# A Risk Analysis Methodology
## for
# Securing Teleworking

### A survey within the Dutch national government

**December 2006**


**Master thesis**
Informatics and Economics
Erasmus University of Rotterdam

**Author**
Lars Hoogendijk
(275959ch)

**Supervisors**
Dr. Ir. Jan van den Berg
and
Ing. Peter Groen MBA RE CISA



**Supported by**
PricewaterhouseCoopers

# Acknowledgements

The completion of this master thesis did not go without some difficult moments. Fortunately I could rely on a number of people whose support ultimately enabled me to complete my studies. These people should not be left unmentioned.

First of all I would like to thank both my supervisors Jan van den Berg and Peter Groen for their unremitting patience and confidence. I would also like to thank all the people who I have interviewed and everybody at PricewaterhouseCoopers who was prepared to comment on my research.

On a more personal level I would like to thank all my friends for frequently offering the necessary distraction from the daily routine of working on my thesis. I would also like to thank my family in New-Zealand who has made my time there unforgettable. In particular my aunty Annie Ruiterman whose strength and life spirit will always be a great example for me.

Last but not least, I would like to thank my parents and my sister for always being there for me. I would never have been where I am now without their love and caring.

# Management summary

## Context

Ever since the advance of teleworking in the 1970s, there has been debate over telework definitions. Many different project-specific telework definitions are currently used in practice, but in the abstract the phenomenon can be defined as ‘working independent of time and place with the help of information and communication technology (ICT)’.

The number of teleworkers in the Netherlands is clearly increasing and the role teleworking plays within the Dutch national government is also likely to become more and more prominent, because the modern national government actively makes use of the possibilities provided by ICT.

Recently however, the national government has been involved in a number of information security incidents associated with teleworking. As a result of these incidents, sensitive government information came in the hands of third parties. A well-known example is the Tonino incident of 2004 whereby sensitive judicial information became publicly available after public prosecutor Joost Tonino had put his old personal computer out with the trash.

The recent security incidents indicate that national government agencies do not always adequately enable information security in relation to teleworking. Therefore we decided to develop a risk analysis methodology that can be used by national government agencies to assess the security risks associated with teleworking and to identify the security controls required to keep the risks within acceptable limits.

## RAMST

We named the risk analysis methodology we have developed the ‘Risk Analysis Methodology for Securing Teleworking’ (RAMST). RAMST is based on a field survey amongst ten national government agencies and relevant literature on information security and teleworking. We have aimed to safeguard the quality of RAMST by means of a validation session with a focus group that consisted of eight security experts.

### Scope of RAMST

Due to the breadth of the concepts of ‘teleworking’ and ‘information security’ on the one hand and time constraints on the other, we have restricted the scope of RAMST. First of all RAMST primarily covers security risks that may have a direct impact on the confidentiality, integrity and available of the ‘asset’ information. Besides that, RAMST is aimed at the security risks associated with the two telework typologies (T1 and T2) we have derived from the way teleworking takes place at the national government agencies included in our field survey. These two telework typologies are described below:

| | |
|---|---|
| **T1** | Teleworking with a 'stand-alone' computer. Information is **stored** and **processed locally**.[1] |
| **T2** | Teleworking with a computer that is connected to central servers by means of a Citrix server based computing architecture. Information is **stored** and **processed centrally**.<br><br>Only user interfaces, keystrokes and mouse clicks are communicated between the computer and the central servers. Communication takes place over the Internet. The computer only generates application screens. |

**Definition 1: Two telework typologies**

## Phases of RAMST

A RAMST review is carried out in four consecutive phases. Each phase consists of several steps that should successively be performed in order to complete the phase (see appendix C). The table below described the objectives of each phase:

| | |
|---|---|
| **Phase 1** | **Set the scene**<br>In this phase a review group is established and the scope of the risk analysis is determined. The latter is done by choosing a telework typology (T1 or T2) and by determining which information is used by the teleworkers under review. |
| **Phase 2** | **Assess business risks**<br>In this phase the information that is used by teleworkers is classified in terms of its importance to the agency and hence the level of protection needed. |
| **Phase 3** | **Assess threats, vulnerabilities and controls**<br>In this phase the key threats and vulnerabilities associated with the chosen telework typology are determined as well as the controls required to keep the risks within acceptable limits. |
| **Phase 4** | **Produce agreed action plan**<br>In this phase a plan of action for implementing controls is agreed. |

**Table 1: The four phases of RAMST**

The third phase is supported by three key documents, namely:

- The 'Directory of Threats' which contains a the main security threats associated with the two telework typologies (see appendix J);
- The 'Directory of Controls' which contains the common controls that can be used to reduce the threats included in the 'Directory of Threats' (see appendix K) and
- The 'Threat/Control Matrix' which indicates the strongest relationships between the threats and controls included in respectively the 'Directory of Threats' and the 'Directory of Controls' (see appendix L).

[1] The protection of information that is transported between the stand-alone telework computer and other computers (e.g. via email or portable data carriers) is outside the scope of this research.

## Use of RAMST

In RAMST the information that is used by teleworkers determines the required level of protection and with that the amount and nature of security controls that need to be implemented. In order to prevent under- or overprotection it is best to conduct RAMST for groups of teleworkers with homogenous information needs.

In case many of such groups can be identified it may be feasible to establish a security baseline. The security baseline contains the security controls that should be implemented in order to achieve a desired minimum level of security for teleworking and is sufficient for all information that requires the same or a lower level of protection than the level of protection offered by the baseline.

The figure below illustrates how the security baseline can be used in practice. By performing steps 1 and 2 of RAMST it can be determined what the required level of protection of the information used by the teleworkers under review is. In case the level of protection required for this information is lower than or equal to the level of protection offered by the baseline, the security controls included in the baseline can be implemented. Otherwise phase 3 and 4 of the RAMST review should also be conducted to identify which additional security controls need to be implemented.

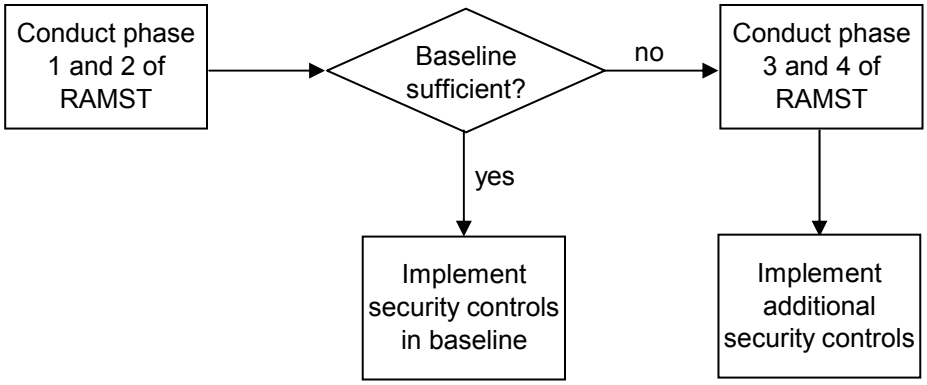


**Figure 1: Baseline or complete RAMST review?**

# Table of contents

# Chapter 1: Introduction

## 1.1 Context

This chapter serves as an introduction to the thesis 'A Risk Analysis Methodology for Securing Teleworking'. First the phenomenon teleworking and the relevance of information security are briefly described. Subsequently we explain what made us start this research. We conclude this chapter with the formulation of the research problem and a description of the research methodology. An outline of the remainder of this thesis is included at the end of this chapter.

### 1.1.1 The rise of teleworking

Much of the recent academic and media interest in work that is performed at home, or at other locations away from the centralised, traditional workplace has focused on the phenomenon telework. Although many different telework definitions are used in practice, there is a growing consensus that telework is remote work that involves the use of information and communications technologies (ICTs). [SULL2003]

Many studies indicate that the Netherlands take a leading role in teleworking [EUCO2005] [SIBI2003] [ECAT2000]. According to the latest estimates of the European Commission [EUCO2005] there are about 1 million teleworkers in the Netherlands, compared to 80,000 in 1995[2]. The director of the Dutch Telework Forum, Philip Todd, is of the opinion that this number can be doubled in the next five years due to technological developments and some significant advantages associated with teleworking such as reductions of traffic and increased employee productivity.

The role teleworking plays in the Dutch national government is also likely become more and more prominent, because the modern national government actively makes use of the possibilities provided by ICT [BZK2001].

### 1.1.2 The need for information security

In order to perform their work activities, teleworkers may need access to an organization's proprietary information. Consequently such information is exposed to various security risks associated with teleworking. These risks can potentially harm the information's quality which – in the field of information security – is usually expressed in terms of its confidentiality[3], integrity[4] and availability[5]. This in turn may result in various forms of damage to the organization, such as reputation loss, loss of public confidence or financial damage.

Security risks can be reduced by implementing security controls. At first sight it seems obvious to implement as many security controls as possible, but security controls also have a downside: they are expensive and generally restrict the functionality of the systems they protect. Therefore it is best not to secure the information that is used by teleworkers any heavier or any lighter than necessary.

[2] These estimates are only intended to give a *global* impression of the scale and growth of the teleworking, because it is unclear exactly how the phenomenon teleworking has been defined and measured in [EUCO2005].
[3] The extent in which access to and inspection of information is restricted to a defined group of authorized persons.
[4] The extent to which information is errorless.
[5] The extent to which information is available at the moment it is needed.

Risk analysis supports the search for a well-balanced and coherent set of security controls that optimally protects information. [OVER2000] As such risk analysis plays a central role in the information security process.

### 1.1.3 Security incidents

Recently a number of telework security incidents whereby sensitive government information came into the hands of third parties made the news (see below). These incidents indicate that national government agencies do not always adequately enable information security with respect to teleworking. The incidents led to considerable public commotion.

- Public Prosecution Office (October 2004)
  Leading public prosecutor Joost Tonino puts his old personal computer out with the trash. The hard disk, which should have been destroyed, contains hundreds of pages of confidential information about high profile cases, as well as Tonino's credit card number, social security number and personal tax files. The personal computer is discovered and the information is sold to TV crime reporter Peter R. de Vries who reveals on television what is on the hard disk. [LIBB2004]
- Regional Intelligence Agency (December 2004)
  Two diskettes are found in a leased car that was used by an employee of the regional intelligence agency (RID). The diskettes contain confidential documents including reports about prominent politicians. Once again the information comes into the hands of TV crime reporter Peter R. de Vries. [ELSE2005]
- Land forces (February 2006)
  A captain of the land forces loses a memory stick by leaving it behind in a rental car. The stick contains sensitive information on Dutch troops in Afghanistan and the personal security of minister Kamp (Defence). The memory stick is found and properly returned to its owner, but the data on it is copied and later on distributed to several news broadcasters. [NUNL2006] [PLAN2006]
- Ministry of Interior and Kingdom Relations (February 2006)
  Equipment is stolen out of two police cars including a laptop and a PDA. The data on the laptop is encrypted, but both the laptop and PDA are not recovered. [ELSE2006a]
- Ministry of Defence (April 2006)
  An official accidentally makes sensitive documents concerning the Royal House and the ministry publicly available via file sharing program Limewire. A student who is connected to the Limewire network discovers the documents and delivers them to a popular newspaper (i.e. *De Telegraaf*). [ELSE2006b]

Since the number of security incidents that made the news probably is only a small tip of the iceberg, the security problem may be considerable. This is further underlined by a survey on the security of mobile workplaces (e.g. notebooks) conducted by 'Control Break International' in 2004 [VNUN2004].

Respondents from various sectors could choose between six different ways in which they secured mobile workplaces (e.g. policy, encryption, tokens) or they could indicate that they did not implement any security controls at all. As much as 61 percent of more than a hundred government employees indicated that they did not take any security measures to protect mobile workplaces.

## 1.2 Research problem

### 1.2.1 Research objective

If national government agencies enable information security with respect to teleworking in a well-structured manner, security incidents like the ones described above may be prevented in the future. Proper information security becomes even more important if the scale on which teleworking takes place increases.

A risk analysis methodology that can help (1) to identify security risks associated with teleworking and (2) to agree on what security controls are worthwhile to reduce the level of risk, can be a valuable tool to enable an adequate level of information security. The objective of our research is derived from this observation and can be defined as follows:

> **To develop a risk analysis methodology that can be used by national government agencies to assess the *security risks* associated with teleworking and to identify the security controls required to keep the risks within acceptable limits.**

**Definition 1.1: Research objective**

### 1.2.2 Research demarcation

Since the security incidents described above all involve information, we would like the risk analysis methodology to be primarily aimed at protecting the asset 'information'. Hence, for this research, the protection of other assets – such as people and computing assets – is considered to be less important than the protection of information.

Teleworking is a very broad and complex phenomenon with enormous potential for variation in terms of, for example work location, work times, and ICT use. In order to operationalise teleworking for this research we create our own specific conceptualization of the phenomenon.

Consequently the security risks mentioned in the research objective involve those risks that (1) have a direct impact on the quality of information and (2) are associated with our conceptualization of teleworking.

### 1.2.3 Research methodology

Our risk analysis methodology should be practically usable by national government agencies. Therefore we conduct a field survey amongst a number of those agencies. The main purposes of this field survey are to learn in which ways teleworking takes place in practice and how corresponding information security is enabled.

Since both teleworking and information security are not new research areas we also use relevant literature on these subjects. We use the literature on teleworking in combination with the survey results to develop a conceptualization of the phenomenon teleworking that corresponds to the way it takes place in practice. The literature on information security (as well as some of the survey results) is utilized to develop a concept version of a risk analysis methodology that can be used to enable adequate information security in relation this conceptualization of teleworking.

The concept version of the risk analysis methodology is then discussed in a focus group that consists of a number of security experts. Their feedback is processed into our final risk analysis methodology. This way we hope to assure that the ultimate methodology is of sufficient quality.

The research methodology is visualized in the figure below:

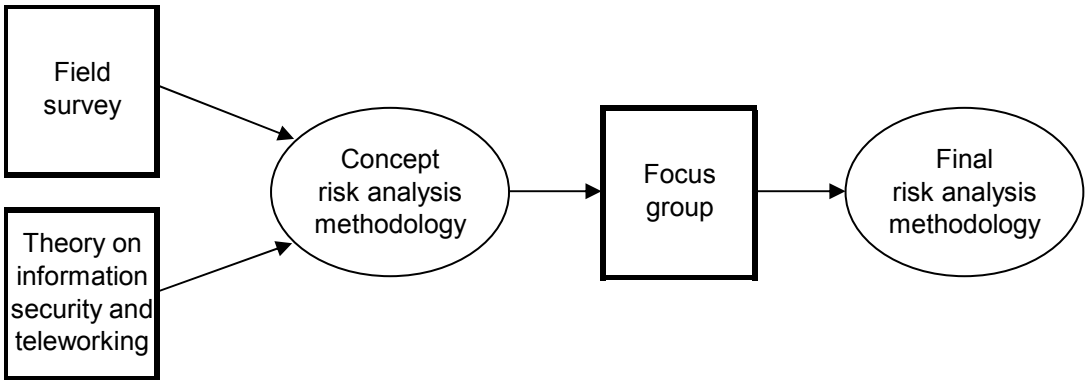


**Figure 1.1: Research methodology**

## 1.3 Reading guide

This thesis is organized into six main chapters (chapter 2 to 7 inclusive) and a concluding chapter (chapter 8). Hereunder a brief description of the contents of these chapters is given. This serves as a reading guide.

**Chapter 2: Teleworking**
In this chapter we introduce the concept of 'teleworking'. For this purpose we give an overview of the history of teleworking, shed light on the debate over telework definitions and present some telework statistics. We also describe the decree '*Raamregeling telewerken*' which contains guidelines for teleworkers within the national government.

**Chapter 3: Information security**
In this chapter we explain the role information and information systems play in organizations and stress the importance of protecting their quality. We also introduce some important concepts in the field of information security and describe two decrees that regulate information security within the national government.

**Chapter 4: Field survey**
In this chapter we describe the set-up and results of a field survey we have conducted at a number of national government agencies. The objective of this field survey is to determine how information security in relation to teleworking is enabled within the national government.

**Chapter 5: A conceptualization of teleworking**
In this chapter we develop a conceptualization of teleworking that corresponds to the way it takes place in practice. We first develop a general definition of teleworking. Subsequently we define two telework typologies based on the ICT used for teleworking by the agencies in our field survey.

**Chapter 6: The Risk Analysis Methodology for Securing Teleworking**
In this chapter we present the final version of the Risk Analysis Methodology for Securing Teleworking (RAMST). The two telework typologies defined in chapter 5 lie at the basis of this methodology. We explain the scope of RAMST, its contents and how it can be effectively used in practice.

**Chapter 7: Development and validation of RAMST**
In this chapter we first explain the development process that led to the concept version of RAMST. Thereafter we describe the set-up and results of the validation session with a focus group. This validation session led to the final version of RAMST as described in chapter 6.

**Chapter 8: Conclusions and further research**
In this chapter we present the main conclusions of our research followed by some recommendations for further research.

# Chapter 2: Teleworking

## 2.1 Introduction

In this chapter we introduce the concept of teleworking. We start with a brief overview of the history of teleworking. Thereafter we shed light on the debate over telework definitions. Subsequently we outline which jobs may be suitable for teleworking and what the main benefits and challenges of teleworking are. We end this chapter with some telework statistics and a description of the decree *'Raamregeling telewerken'* which applies to the whole national government.

## 2.2 A little history

The concept of teleworking is far from novel. As early as in the 1950s, the literature on technological new inventions in electronics and communication systems led to the idea that telecommunications, combined with computing technology, could enable work to be relocated from the traditional office. [BARU2001]

Widespread interest in teleworking however, did not start until the 1970s – the era of the oil crisis – when western nations were forced to cut down on their energy consumption. At that time US academic and consultant Jack Nilles popularised the term telecommuting in a now classic study *The Telecommunications-Transportation trade-off* (1976), in which satellite offices – and to a lesser extent home-based teleworking – were proposed as a potential way of saving energy costs [PYÖR2003].

The late 1970s saw the first wave of experiments with teleworking in most countries of the western world. Many of these projects, however, were to enjoy only a short life, while others publicly proclaimed in loud terms were never even to see the light of day. In the 1980s and 1990s several factors helped to revive interest in teleworking, namely structural factors, economy-related factors, technological change and geographical imbalance. [MARO2001] These factors are described in the table below.

| **Structural factors** | **Economy-related factors** |
|---|---|
| In the 1980s and 1990s the orientation of the traditional industrial economy towards a service-based economy increased in intensity. Teleworking as a means of rationalizing work helped improving the competitiveness of the tertiary activities of business firms. | In the industrialised countries, the 1980s decade was one of economic recession and intensifying competition. In this context, both public authorities and business firms looked on teleworking as a new opportunity that would allow them to reduce overheads (e.g. property fees), maintain local employment, relocate or outsource activities, and increase productivity. |

| | |
|---|---|
| **Technological change**<br>In the 1980s the technical obstacles to the development of teleworking tumbled on after the other due to for example the growth in networks, falling component costs and miniaturisation of equipment. Moreover the use of tools such as the fax, PCs and e-mail began to become commonplace in the course of the decade. Teleworking was further technically enabled by the boom in cell phones and the beginning of the exponential spread of the Internet at the end of the 1990s. | **Geographical imbalance**<br>In the 1990s problems with respect to urbanization (e.g. delinquency, social exclusion, insecurity etc.), deterioration of the environment, loss of attractiveness of peripheral geographical zones and saturation of the transport infrastructure became more and more imminent in Europe. Teleworking potentially is a major means for the de-concentration of the population and geographical re-distribution of economic activity. |

**Table 2.1: Four factors that helped to revive interest in teleworking in the 1980s and 1990s**

## 2.3 What is teleworking?

Although teleworking has been discussed for some years, a universal definition is still not in place. There is not even an agreed term: ‘teleworking’ or ‘eWorking’ (common in European literature), ‘telecommuting’ (common in American literature), ‘home-working’, working-at-a-distance’, ‘off-site workers’ or ‘remote workers – all these terms have similar meanings and are used exchangeably. [BARU2001]

### 2.3.1 General versus project-specific definitions

The lack of a universally accepted definition of teleworking causes problems: for example, academically it hinders the ability to compare findings from different sources and from a legal perspective the lack of an accepted definition causes contractual uncertainty. It also makes it almost impossible to find out how many people and organizations practice teleworking [BARU2001]. Therefore some people assert that a single definition should be used by all research.

Teleworking however, is a broad field of study that attracts attention from a large number of different disciplines ranging from transportation and urban planning to ethics, law, sociology, and organizational studies. Since researchers generally use definitions through which they can best meet the aims of their specific research, it seems inevitable that a wide range of project-specific telework definitions are used in practice. [SULL2003]

Even though studies based on different project-specific telework definitions may not be directly comparably, the findings of various studies together may very well be a useful body of knowledge. Besides that, project-specific definitions can be useful in exploratory studies that deal with concepts where there is debate about conceptualisations and definitions, because they can help to refine future, and possibly more general, definitions.

### 2.3.2 Dimensions of teleworking

So what is teleworking? The common denominator for most definitions is first, that the office is not the only place where work can be conducted, and secondly, that ICT is the vehicle allowing this to happen [BARU2001]. In the abstract teleworking can be defined as follows:

> **Teleworking is working independent of *time* and *place* (with the help of *information and communication technology*).**

**Definition 2.1: Abstract definition of teleworking**

This abstract definition contains at least three dimensions that may be involved in any project-specific definition of teleworking, namely: time, place and – optionally – information and communication technology. The extent to which each of these dimensions is critical to any piece of research will depend upon the specific questions addressed by that research.

**Time**

The amount or proportion of work time spent working remotely is a common criterion for defining teleworking. The cut-off point that is used tends to vary a great deal in different research. [SULL2003]

Some studies group teleworkers into subsets according to the intensity of teleworking: for instance, 'supplementary', 'alternating' and 'permanent', defined respectively as teleworking less than one day a week, teleworking at least one day per week, and teleworking most of the time. 'Overspill work' or 'overtime', which is additional to office hours, is not normally included in definitions of telework [HADD2005]

**Place**

Another key element in arguments about definitions of teleworking is location. Some commentators and researchers have defined telework as work at home, but generally the definition of telework now includes a variety of locations and emphasises is on the remoteness. [SULL2003]

The location in which remote work is carried out may give rise to sub-types of remote work, such as home-based telework (employees work at home), mobile telework (employees are frequently on the move) or satellite offices (employees work in a location convenient to the employees and/or customers). In some cases tele-cooperation – i.e. interacting remotely with others electronically from an office – is also considered to be a form of teleworking.

**Information and communication technology (ICT)**

In the general definition of teleworking presented above, the constituent 'with the help of information and communication technology' is put in brackets, because there is some debate on the degree to which ICT forms a substantial, strategic or necessary part of teleworking.

Some of the earliest studies did not require the element ICT. Telework looked like a new phenomenon because of the content of the work being done at home – now called knowledge work – and this was different from the routine, low paid labour often associated with homeworking. Yet by the late 1980s there were suggestions that the label 'telework' should be reserved for those homeworkers who use new technology. [HADD2005]

In most contemporary research, technology is a crucial element in the distinction between telework and other forms of decentralized work and work at home [SULL2003]. There is however, a problem in determining the role of ICT. For example, people might make incidental use of ICT in the course of their work and the kinds of ICT they use may differ. Some teleworking may be accomplished effectively with only a telephone and facsimile as the relevant technologies, while other teleworking may require more sophisticated technologies like personal computers, email, remote access to corporate databases or technology-mediated meetings. [PÉRE2005]

Sullivan [SULL2003] therefore recommends measuring the level of ICT use. This makes sense, although it is not certain how 'levels' themselves should be defined (by time, intensity, technological complexity?). A possible approach is to acknowledge technology as shaping part of the contours of teleworking practices, and then to differentiate users of different types of ICT. This takes the view that no specific technology defines a teleworker. Specific technologies may define different forms of telework. [HADD2005]

## 2.4 Jobs suitable for teleworking

Not all jobs are suitable to be carried out at a remote location. As a general guide, any job that does not involve physical production, extensive face-to-face customer or team contacts or expensive specialist equipment can be teleworked. Often a job which may not seem to have the potential for teleworking can contain a number of sub-tasks that can be clumped together and carried out through teleworking, even though other tasks must be carried out at the conventional office. [DENB2000]

Other tasks suitable for teleworkers include those where the work can be easily measured, those that involve mental rather than physical effort, and those that do not require extensive hands-on management. Typical telework categories include [DENB2000]:

- *Professionals and managers*: architects, accountants, management, marketing, public relations, human resources, project managers, account managers, finance, financial analysts and brokers.
- *Support workers*: bookkeepers, translators, quality managers, trainers, proofreaders, indexers, researchers, administrators and web designers.
- *Mobile or field workers*: company representatives, surveyors, engineers, inspectors, estate agents, auditors, journalists, insurance brokers and landscapers.
- *Information technology specialists*: system analysts, software programmers, technical support, software localisation engineers and some hardware engineers.
- *Clerical workers*: data-entry staff, secretaries and call-centre agents.

## 2.5 Benefits and challenges

In literature on teleworking – e.g. [KURL1999] [HARP2002] [DENB2003] [MORG2004] [EUCO2005] – various generic telework benefits and challenges have been distinguished. These benefits and challenges are normally grouped under the individual, the organization and/or the society at large.

Key benefits to *individuals* are a better balance between work and social life, the ability to combine work with family care, increased autonomy, flexible working hours, less distraction of colleagues and savings in travel time and expenses. Key challenges are feelings of isolation, no separation between spheres of work and home, limited career advancement, problems with self-discipline and lack of professional support.

For *organizations* teleworking generally leads to better motivated personnel with less sickness and leave, increased flexibility of personnel, access to focus-groups like women and disabled people, higher productivity and savings on the costs for office space, travel and parking. Furthermore it gives them the experience with new ways of working and an innovative and environment-friendly image. Common organizational challenges are related to managing and supervising teleworkers, changing existing work methods, the costs of telework equipment and security risks.

The main *social* advantages are a decrease of commuter travel, a reduction of air and noise pollution, creation of possibilities for women and disabled persons, stimulation of local economies and savings in infrastructure and energy. A major downside is that teleworking may lead to a detached society where individuals are cut off and isolated from one another and from public institutions.

## 2.6 Statistics

Teleworking in the Netherlands is clearly increasing, but there is little consensus on how much Dutch teleworkers there are. The problem with counting teleworkers is that there has been little general agreement on what constitutes a teleworker, or on how to measure teleworking – e.g. whether teleworkers are employed, self-employed, part-time or full-time, what sort of ICT equipment they use or where they are located [DENB2000].

From January 2001 to September 2003 the European Commission sponsored the SIBIS[6] project [SIBI2003] [EUCO2003]. During this period SIBIS publicized extensive statistics on teleworking in Europe.

SIBIS distinguishes three main telework forms, namely home-based teleworking, mobile teleworking and teleworking by self-employed who work from SOHOs, i.e. small offices in their home. These are defined as depicted in the figure below.

[6] Statistical Indicators Benchmarking the Information Society

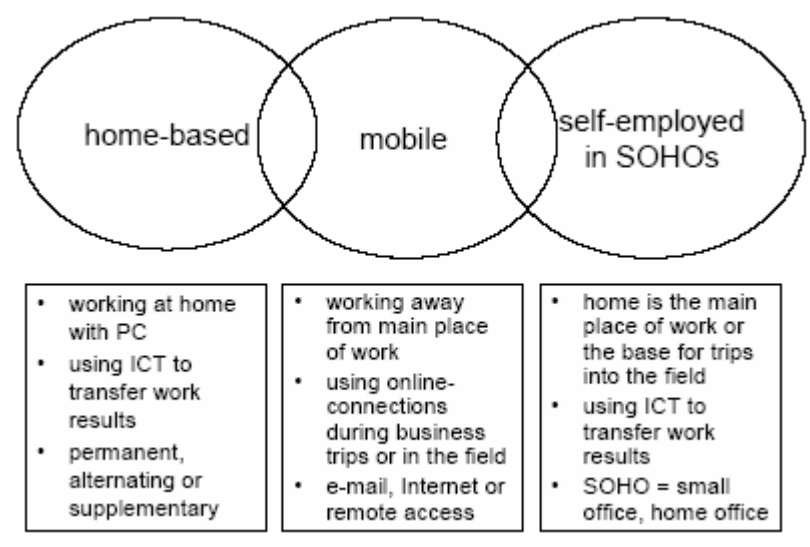


**Figure 2.1: SIBIS definitions and interrelations of teleworking**

According to the last SIBIS report (2003), 13% of the working population in 15 EU member states[7] could be classified as teleworkers (all forms of teleworking included). Between 1999 and 2003 the penetration of teleworking in the EU more than doubled. In 1999 only 6% of all persons employed in the EU were teleworking.

In 2003 the share of teleworkers in Europe was considerable lower than in the US. In the country where the telework idea was born, every fourth worker had some type of teleworkplace (25%).

The Netherlands were the only country included in the SIBIS survey with a higher penetration of teleworking than the US. In 2003 26.4% of the Dutch working population were actively teleworking. The Netherlands were directly followed by the three Scandinavian countries: Finland (21.8%), Denmark (21.5%) and Sweden (18.7%). Below average shares of teleworkers were found in the countries of Southern Europe, namely Italy (9.5%), France (6.3%) and Spain (4.9%).

Several factors have contributed to the leading role that the Netherlands have in teleworking. [EUCO2005] First of all use of ICT has become naturalized in many Dutch households. There is a high penetration of personal computers at home – thanks to the Dutch PC-private project that gave companies the possibility to provide their workers a PC for use at home – and many households have a broadband connection which makes high-speed access to Internet and email possible. Secondly the type of work and the Dutch organization culture and way of managing have contributed to the growth of teleworking. Many Dutch workers work in the service business and Dutch organizations are characterized by horizontal and functional relations. Lastly the Dutch government has actively stimulated teleworking in the last few years.

[7] Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden and the United Kingdom

## 2.7 Teleworking within the national government

In the modern national government that actively makes use of the possibilities provided by ICT, the role teleworking plays is becoming more and more prominent. Therefore the minister of the Interior and Kingdom Relations and the cooperative body of civil servants established the decree *'Raamregeling telewerken'* [BZK2001] which came into effect in June 2001.

The decree contains guidelines for teleworkers who work at home, but leaves it up to the manager and the employee to decide if teleworking is desirable. The decree starts with definitions of relevant concepts. Subsequently it prescribes the way in which agreements between the teleworker and employer are made and recorded. This concerns, amongst other things, the organization of the workplace, the issuance of telework equipment, the number of days on which the teleworking takes place and some information security issues. The decree concludes with guidelines on financial compensations for teleworkers.

## 2.8 Conclusion

In this chapter we introduced the concept 'teleworking'. We started with an overview of the history of teleworking. Thereafter we explained the problems associated defining teleworking. We gave an abstract definition of teleworking which contains three dimensions – time, place and ICT – that may be involved in any specific definition of teleworking. We argued that the extent to which each of these dimensions is critical to any piece of research depends upon the specific questions addressed by that research.

We continued with a description of the kind of jobs that can be teleworked and elaborated on the key benefits and challenges of teleworking for the individual, the organization and the society as a whole. Subsequently we presented some telework statistics which indicate that the Netherlands had the highest penetration of teleworking in Europe in the year 2003. We concluded this chapter with describing the contents of the decree *'Raamregeling telewerken'* which contains guidelines for teleworking and applies to the whole national government.

# Chapter 3: Information security

## 3.1 Introduction

Information security is aimed at the protection of information systems and the information they contain. In this chapter we first introduce some important concepts in the field of information security. Thereafter we explain the information security process and the role risk analysis plays. We end this chapter by describing the decree VIR and the decree VIR-BI which regulate information security within the national government.

## 3.2 Information and information systems

Working with information plays a crucial role in every organization. Organizations do not only deliver information as a product, they also need information to make decisions before, during and after the production process. Many different kinds of information are used in organizations (e.g. plans and procedures, correspondence and archives) and this information takes many forms (e.g. stored on computers, transmitted across networks and spoken in conversations).

The protection of information in whatever form or media is the domain of 'information security'. Strictly speaking it is better to use the terms 'data security' or 'data protection', because only data that reach the consciousness of a human being and contribute to his knowledge are called information. Data as concrete objects can be protected as opposed to information as abstract notion and intangible object. [VRIE2002] The term information security however, expresses more clearly that not only the protection of data is important, but rather the protection of the quality of information systems used to capture and process that data.

Organizations use numerous information systems to support their activities. Since information and information systems play such an important role in organizations it is important to safeguard their quality. In the field of information security three quality aspects are commonly distinguished, namely confidentiality, integrity and availability. The decree VIR [BIZA1994] defines these quality aspects – or security attributes – as follows:

**Confidentiality**[8]: the extent in which access to and inspection of an information system and the information it contains is restricted to a defined group of authorized persons.
**Integrity**: the extent in which an information system is errorless.
**Availability**: the extent in which an information system is in operation at the moment the organization needs it.

**Definition 3.1: Quality aspects of information and information systems**

[8] The decree VIR actually uses the term exclusiveness instead of confidentiality. Nevertheless we employ the term confidentiality because this term is most commonly used in (Anglo-Saxon) literature on information security.

## 3.3 Security risks

The quality of information systems is exposed to various security threats. A security threat is an event or process which could compromise quality of an object. With respect to an information system this concerns the objects hardware, software, data, procedures and people. The source of security threats may be human or non-human [OVER2000]:

- Human threats:
  - Unintentional wrongdoing, by users, system operators, guests or external personnel;
  - Misuse and criminality, such as theft, burglary, hacking, sabotage or fraud.
- Non-human treats:
  - External threats, such as earthquake, storm, lightening, flooding or fire;
  - Interruptions in the basis infrastructure, such as power or air-conditioning failure;
  - Interruptions in apparatus, software or data files.

A security breach arises if a security threat exploits one or more vulnerabilities of an object. The vulnerability of an object with respect to a threat is the extent in which the object is susceptible to that threat. This susceptibility arises if one or more characteristics of the object allow a threat to have a negative influence on the object. Hardware for example, is sensitive to physical violence while software is sensitive to digital violence. [OVER2000]

A security risk is a function of the magnitude of possible damage which would arise as a result of a security breach and the likelihood of harm being suffered. This damage may be direct or indirect. Especially the indirect consequential damage, such as reputation loss or loss of public confidence, is hard to quantify. Therefore risks can be estimated, but not precisely calculated. This explains why risk analyses are often subjective in nature. [VRIE2002]

## 3.4 Security controls

Security controls can be introduced to reduce the risk of security breaches and to minimise the harm they cause [ISF1997a]. At first sight it seems obvious to reduce risks by implementing as many controls as possible, but security controls also have a downside: they are expensive and generally restrict the functionality of the systems they protect. Therefore it is best not to secure any heavier or any lighter than necessary. [OVER2000] In order to understand risks and to determine what measures need to be taken to control them, a risk analysis can be performed.

According to Overbeek [OVER2000] security controls can be classified in three different ways:

- Classification based on the event cycle;
- Classification based on the way security controls are realized and
- Classification based on the quality aspects security controls help protect.

**Classification based on the event cycle**
The event cycle describes the steps that take place around the manifestation of a security breach. These steps are subsequently: (1) a threat – something that could happen –, (2) a breach – the manifestation of a threat –, (3) damage – the consequences of a breach – and (4) recovery – the recovery of damage –. This is illustrated in the figure below.

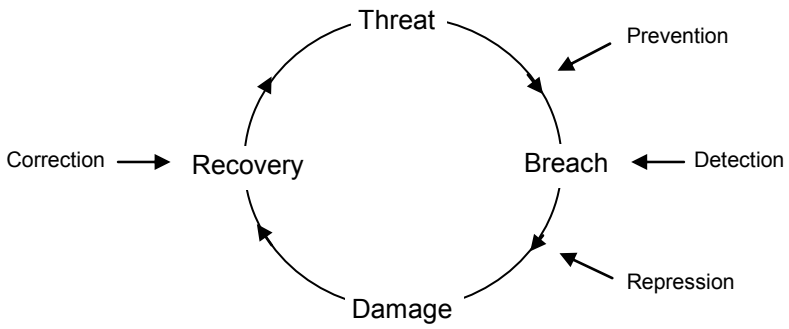


**Figure 3.1: The event cycle and security controls**

Security controls are aimed at a certain moment in the event cycle. From this perspective, security controls can be distinguished into:

- Prevention controls. These controls provide a first line of defence. Their purpose is to prevent a threat from causing a security breach. Prevention controls are distinguished into permanent controls and triggered controls. Permanent controls provide continuous protection (e.g. incombustible floor covering) while triggered controls only offer protection after they are put into action (e.g. uninterruptible power supply).
- Detection controls. These controls are not effective on their own. Detection controls can only be effective in combination with one or more triggered prevention or repression controls. Therefore detection controls are sometimes considered to be part of the prevention and repression controls they support (e.g. smoke detectors).
- Repression controls. These are second-line controls. Repression controls are aimed at reducing the negative influence of a security breach in case the prevention controls could not prevent it (e.g. data back-up or contingency arrangements).
- Correction controls. These controls are aimed at the recovery of objects that have been damaged as a result of a security breach. In fact these controls are maintenance controls instead of security controls.

**Classification based on the way security controls are realized**
Besides the classification based on the security cycle, controls can also be classified according to the way they are realized. From this perspective the following controls can be distinguished:

- Organizational controls. These controls concern the organization as a whole. Organizational controls include the formulation of the security policy, guidelines and procedures.
- Logical controls. These controls are programmed into software. Examples are logical access control and encryption software.
- Physical controls. These controls are based on hardware and other material things. Examples are fire extinguishers and uninterruptible power supply.

**Classification based on the quality aspects security controls help protect**
Information security is essentially about protecting the confidentiality, integrity and availability of information systems. Therefore every security control can be related to one or more of these quality aspects.

## 3.5 The information security process

Although we have already explained some important concepts in the field of information security, we have not yet given a formal definition of information security. The decree VIR [BIZA1994] defines information security as follows:

> **Information security is implementing and maintaining a coherent set of security controls in order to safeguard the confidentiality, integrity and availability of an information system and with that of the information therein.**

**Definition 3.2: The decree VIR's definition of information security**

The words 'implementing' and 'maintaining' included in this definition indicate that information security is not a once-only event. Instead, it often considered to be a cyclical and iterative process. According to Overbeek [OVER2000] this process consists of six steps:

1. Formulating an information security policy and establishing the organization that is responsible for information security;
2. Finding unacceptable risks and searching for security controls which can reduce those risks;
3. Selecting a set of security controls;
4. Implementing a set of security controls;
5. Monitoring the compliance with implemented security controls and
6. Evaluating the effect achieved with the implemented security controls.

Organizations and their environment are continuously changing. Therefore risks will also change as well as the requirements organizations put on information security. This in turn has consequences for the extent in which implemented security controls satisfy these requirements. In order to ensure that an adequate level of information security is maintained, the information security process has to be repeatedly executed.

## 3.6 Risk analysis

Step 2 of the information security process can be put into practice by means of a risk analysis. Risk analysis is a process for understanding risks and determining what measures need to be taken to control them [ISF1997]. It supports the search for a well-balanced and coherent set of security controls to optimally protect information systems. A risk analysis is usually carried out by the person who is responsible for the subject of the analysis (e.g. a manager).

There are various forms of risk analysis which can be roughly distinguished into two groups [OVER2000] namely: (1) standardized and (2) made-to-measure risk analyses.

**Standardized risk analyses**
Standardized risk analyses are often based on checklists that contain standard security controls. Together these standard controls constitute the security norm pursued by the checklist. Checklists vary in breadth and depth. The simplest form is the quick scan whereby some external norm is pursued. A more complex form is the baseline checklist whereby an internal norm is pursued. The baseline checklist may be based on one or more external norms.

Advantages standardized risk analyses are:
- Checklists are easy to apply and relatively inexpensive and
- Checklists can be used as a frame of reference.

Disadvantages are:
- One size does not fit all: checklists cannot be applied in every situation;
- Checklists soon get out of date due to continuous developments in ICT.
- Checklists may provide hackers with information on which security controls they have to circumvent.

**Made-to-measure risk analyses**
Made-to-measure risk analyses are not based on standard checklists. Instead, security controls are identified by means of a thorough analysis of the importance of objects (e.g. information systems) and the threats to which they are exposed.

The qualitative risk analysis is the simplest made-to-measure risk analysis. Hereby risks are roughly estimated. A more complex form is the quantitative risk analysis. Hereby risks are quantified in measurable units (where possible), such as money.

Major advantages of a made-to-measure risk analyses is:
- An accurate assessment of risks is possible.
- Made-to-measure risk analyses stay up-to-date because they do not contain specific (time-dependent) security controls.

Disadvantages are:
- Made-to-measure risk analyses are complex, expensive and time consuming;
- Made-to-measure risk analyses can lead to an information overload, which complicates decision-making.

**Focus of the risk analysis**
Risk analysis can be performed in different ways, on different levels of abstraction and on different objects. Some risk analysis focus on business processes while other risk analysis focus on the technique itself. Examples of objects that can be subjected to a risk analysis are the organization, the business process, the information system and the application.

## 3.7 Information security within the national government

The national government has the duty to organize and maintain its own information security [EXPE2002]. Hereto the decree '*Voorschrift informatiebeveiliging rijksdienst*' (abbreviated to VIR) and the decree '*Voorschrift informatiebeveiliging rijksdienst – bijzondere informatie*' (abbreviated to VIR-BI) are effective. In this paragraph we shortly describe both decrees.

### 3.7.1 The decree VIR

In 1994 the decree VIR [BIZA1994] came into affect. The decree VIR contains six articles in which the organization and approach of information security within the national government is worked out. The decree is made to last and therefore global in nature.

In the decree VIR article 1 deals with definitions of concepts and article 2 focuses on inter-organizational aspects and the allocation of responsibilities. Article 3 subsequently centres on the information security policy and the associated policy document. The risk analysis methodology with which a well-balanced coherent set of information security controls can be chosen is described in article 4, while article 5 is focused on the way these security controls are realized. Finally article 6 contains concluding statements. [BRUI1995]

### 3.7.2 The decree VIR-BI

In 2004 – ten years after the decree VIR – the decree VIR-BI [BZK2004] came into effect. The decree VIR-BI gives rules for the protection of the confidentiality of *special* information. In addition to this it describes who is responsible for the security of special information and how the classification of special information is organized (e.g. classes of special information, duration, termination etc.). The decree VIR-BI supplements the decree VIR.

Special information is information for which inspection by unauthorized parties can have serious consequences for the interests of the State, its allies or one or more ministries. There are various classes of special information. This is illustrated in the figure below.

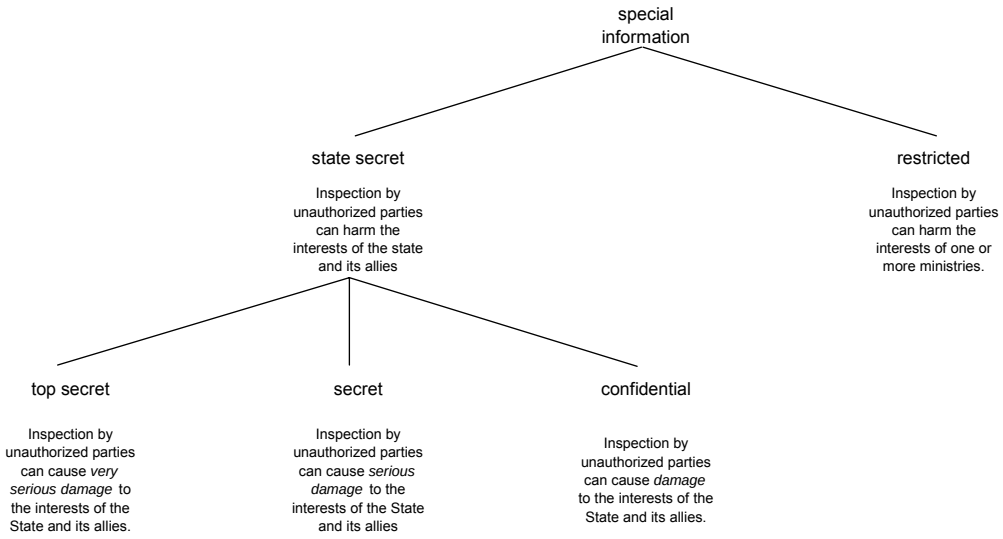


**Figure 3.2: Classes of special information**

Article 12 of the decree VIR-BI contains two general security requirements with respect to the confidentiality of special information. Special information needs to be secured in such a way that (1) only authorized persons can handle or inspect special information for as far as this is necessary for the proper fulfilment of their tasks and (2) that security breaches are detected and a proper investigation for (possible) breaches is possible.

These general security requirements are further specified in appendix 3 of the decree. This appendix contains a matrix with a large number of detailed confidentiality requirements grouped under nine categories. Every confidentiality requirement included in this matrix may concern different classifications of special information (e.g. top secret, secret etc.). This is illustrated in the table below. Some confidentiality requirements must be satisfied while others are optional.

| **LOGICAL ACCESS CONTROL** | | | | | |
|---|---|---|---|---|---|
| **Identification and authentication** | | **Top secret** | **Secret** | **Confi-dential** | **Restric-ted** |
| C | Users are identified and authorized in advance | **V** | **V** | **V** | **V** |
| D | The identity of a user is determined by means of a token or biometrics | **V** | **V** | | |

**Table 3.1: Example of two confidentiality requirements included in VIR-BI**

## 3.8 Conclusion

In this chapter we explained that information and information system play a crucial role in every organization. Therefore it is important to protect their quality, expressed in terms of confidentiality, integrity and availability. We subsequently explained that this quality is exposed to various security threats and that there is a security risk that these threats cause a security breach which leads to damage.

Security controls can be introduced to reduce the risk of security breaches and minimize the harm they cause. Information security is a cyclical and iterative process for implementing and maintaining a coherent set of security controls in order to safeguard the confidentiality, integrity and availability of an information system and with that of the information therein. The risk analysis – which is a process for understanding risks and determining what measures need to be taken to control them – plays a crucial role in the information security process.

At the end of this chapter we described the decree VIR and the decree VIR-BI which regulate information security within the national government. VIR deals with information security in general, while VIR-BI is aimed at protecting a certain class of information, namely *special* information.

# Chapter 4: Field survey

## 4.1 Introduction

In the previous two chapters we have introduced the concepts of 'teleworking' and 'information security'. In order to find out how information security in relation to teleworking is enabled within the Dutch national government, we have conducted a field survey at a number of national government agencies. We start this chapter by explaining the field survey's objectives and how it was conducted. Thereafter we describe the main survey results.

In the next chapter the field survey results are used to develop a conceptualization of teleworking that corresponds to the way it takes place at the agencies included in our field survey. The survey results are also used for the development of the concept risk analysis methodology (see chapter 7).

## 4.2 Field survey set-up

The main objective of our field survey is to determine how information security in relation to teleworking is enabled within the Dutch national government. To achieve this objective we have investigated at a number of national government agencies:

- What teleworking is and at what scale it takes place;
- In which way(s) teleworking takes place (i.e. location and technology) and
- Which security controls are employed to realize information security in relation to teleworking and on which grounds these security controls are chosen.

### 4.2.2 Field survey group

The national government consists of many agencies such as ministries (e.g. the Ministry of Justice), their divisions (e.g. the Public Prosecution Office) and various executive agencies (e.g. the Tax and Customs Administration or the National Service for Archaeology, Cultural Landscape and Built Heritage). Ideally all these agencies should be included in our field survey, but that would be impracticable given the time available for this research.

Therefore we have restricted the survey group to a manageable total of ten national government agencies i.e. seven ministries, one ministerial division and two executive agencies. The names of these agencies are not publicized, because we formally agreed to make sure that survey results cannot be related to individual agencies[9].

[9] Some interviewees requested and received a written confirmation that the interview results would be kept confidential.

### 4.3.3 Interviews

In order to achieve our field survey objective we have conducted an interview with one or more security experts at every agency included in our field survey. The interviews were conducted in the months June and July of 2005.

All interviewees received the same standard questionnaire so that we could easily compare the interview results. The questionnaires were sent to the interviewees some time in advance, to make sure they had enough time to prepare for the interview. An example of a questionnaire is included in appendix A.

An interview normally took between two and three hours, which was enough to discuss the matter in sufficient depth. The results of every interview have been detailedly recorded in interview reports. Most of these reports have been submitted to the interviewees for verification. If necessary, adjustments have been made. In some cases the interviewees provided us with supportive material, such as policies and guidelines.

## 4.3 Summary of the survey results

### 4.3.1 The concept of teleworking

The interviewees have different notions of the concept of teleworking with respect to work locations, work times and ICT use. Most interviewees however, agree that teleworking takes place at a remote location and that it involves the use of ICT. In the next chapter we use some of the telework definitions given by the interviewees in order to develop our own conceptualization of teleworking.

The scale in which teleworking takes place within the agencies in our survey varies considerably, but at most agencies teleworking – in broad sense – is a common phenomenon. This assertion is based on estimates of the number of teleworkers given by interviewees. Although these estimates provide a reliable global image of the proportions of teleworking it would be misleading to include any numbers here. Their accuracy is questionable and it is often unclear exactly on which definition of teleworking they are based.

Usually teleworking takes place on the initiative of the employee. In that case the employee submits a request for teleworking to his manager who decides if the employee is allowed to telework. Teleworking may also be inherent certain functions (e.g. inspectors).

### 4.3.2 Work locations and work times

The telework location is usually the home of the employee, but it may also be that teleworkers do not have a fixed working location. A few agencies have some teleworkers working from satellite offices. Such offices typically house various employees of the same agency.

Some interviewees make a distinction between incidental teleworking (e.g. teleworking less than one workday per week) and structural teleworking (e.g. teleworking at least one workday per week). Besides that, some interviewees are of

the opinion that teleworking mainly takes place during office hours, while others state that it primarily concerns 'overspill work'.

### 4.3.3 Information and communication technology

All agencies in our survey issue laptop computers to at least a part of their teleworking workforce. A few agencies also issue PDAs, be it on a small scale. Computing devices that are not provided by the agency may also be used for teleworking. In theory such devices can be anything that satisfies relevant technical requirements for teleworking. Most interviewees however, claim that teleworkers who do not have a computer issued by the agency at their disposal, mainly use privately owned desktop computers.

Our field survey shows that information exchange between the telework computer and other computers can for example take place via email, portable data carriers or network access points at the office. Not all interviewees however, associate (all of these forms of) information exchange with teleworking.

Almost all agencies in our survey allow at least a part of their teleworkers to access agency information and applications across an external telecommunications service. For this purpose all but one of these agencies employ a server based computing solution developed by Citrix Systems[10].

The characteristic of server based computing is that all applications and databases are completely installed and processed on central servers. In case of Citrix only user interfaces, key strokes and mouse movements are transferred between the central servers and the client computer. This is done by means of the ICA protocol[11]. Almost all agencies employ the Internet as the telecommunications service[12].

A client computer that is part of a server based computing architecture only has to generate the application screens. To enable such a computer to communicate with the central servers it needs to run a small software application. Hereto Citrix makes use of the so-called ICA-client-application[13]. In principle it does not matter where the client computer is located or what it consists of (type of hardware or operating system), as long as it has the ability to run the ICA-client-application and establish a connection with the Internet.

### 4.3.4 Information security

**Security threats**

When asked about the most important security threats related to teleworking, the interviewees did not mention any specific security threats. Instead they indicated which quality aspects of information (i.e. confidentiality, integrity or availability) they considered to be most important.

[10] One agency uses a server based computing solution based on 'Terminal Services' instead of Citrix. Both solutions are conceptually the same.
[11] The Independent Computing Architecture (ICA) protocol is flexible in nature and can work with many protocols (e.g. TCP/IP and PPP) and associated transport means (e.g. modems, ISDN and ADSL) [BRUI2004].
[12] One agency uses a call-in protocol whereby a teleworker 'calls into' a server by means of a telephone line or ISDN connection.
[13] The ICA-client-application is available for nearly every operating system so that applications can be used on for example SUN workstations, HP workstations and UNIX variants, but also on PDAs, DOS, Macintosh or other workplaces and via webclients with JAVA or plug-ins for Netscape Navigator or ActiveX-controls for Microsoft Internet Explorer [BRUI2004].

Most interviewees argued that a loss of information confidentiality would be most damaging, but some interviewees also stressed the importance of the integrity of information. The availability of information generally seems to be less of an issue. Which one of these three aspects is most important seems to primarily depend on the nature of the information used by teleworkers i.e. the extent to which it is sensitive and/or critical.

**Security controls**
On our request the interviewees listed the security controls associated with teleworking implemented at their agencies. Hereunder we broadly describe these controls. We have distinguished organizational from technical controls. Technical controls encompass both logical and physical controls.

*Organizational security controls*
The general information security policy usually contains some security guidelines that are relevant for teleworking, such as guidelines for Internet and email usage. None of the agencies however, paid specific attention to teleworking in their security policy. At one agency a *telework* security policy was about to be implemented.

Normally procedures are described and implemented for the allocation and withdrawal of authorizations of teleworkers and the provision and recollection of telework equipment such as tokens and computers.

Employees who formally telework, are required to sign a 'telework agreement'. At some agencies information security related issues are explicitly mentioned in the telework agreement. By signing such an agreement the teleworker agrees to conduct responsible behaviour in relation to teleworking and information security for example by implementing certain security measures.

One agency developed a code of conduct for teleworking which contains guidelines that indicate how teleworkers should realize adequate information security in relation to teleworking. Another agency implemented a protocol for home working in which some attention is paid to information security related issues.

Most agencies periodically organize security awareness meetings. Although certain topics addressed in these meetings may be relevant for teleworking, security awareness meetings are usually not specifically aimed at teleworking.

Some agencies offer security software, such as anti-virus scanners and personal firewalls (free of charge), in order to enable employees to secure their private computer.

*Technical security controls*
Laptop computers that are issued by the agency are usually preconfigured and user access rights are restricted. Such laptops are normally equipped with antivirus software and a personal firewall. Important security updates and patches are automatically downloaded and installed when the laptop is connected to the Internet.

Logical access control on an agency laptop is normally in place at the operating system level and sometimes pre-boot authentication[14] is also implemented. Authentication is usually based on only one factor, namely 'what the user knows'. This can for example be a combination of a username and password. All data on the laptop's hard disk are automatically encrypted.

[14] In this case access control takes place before the operating system starts.

In addition to this some agencies do *not* equip their laptops with CD or floppy drives and restrict the physical availability of hardware ports to prevent the use of unauthorized peripheral equipment such as CDs, memory sticks or modems. Sometimes device lock software and URL filters are also implemented to respectively control the use of external devices and the Internet.

At all agencies that facilitate teleworking across an external telecommunications service, logical access control for access to applications and information available on central servers is in place. The number of factors required for authentication varies per agency and may be based on one, or a combination, of the following factors:

1. Something the user knows, such as a username or password;
2. Something the user has, such as a token or certificate;
3. Something that is part of the user i.e. a biometrical characteristic, such as a fingerprint.

Additionally some agencies restrict access to central servers to authorized telework computers only. This can for example be done by means of ActiveX applications that run on the telework computer to check if the correct software versions are installed and which applications are or are not running.

At some agencies the number of allowed log-on attempts on central servers is restricted. In case the maximum number of log-on attempts is exceeded, the user account is usually blocked. If the log-on is successful, only the applications to which the user is authorized are available to him. At most agencies certain activities of teleworkers on the central servers are logged.

The data that is exchanged between the telework computer and the central servers is normally encrypted. At some agencies open connections are automatically terminated. This may be done periodically (e.g. every 24 hours), or if a connection has not been used for a certain time.

The physical security of the remote location was seldom explicitly mentioned in relation to teleworking. Only one agency secured home offices by means of for example burglar alarms, locks and safes.

**Choosing security controls**

Within only a few agencies a formal risk analysis has been carried out in order to secure teleworking. In those cases a dependency and vulnerability analysis was used to choose the necessary security controls. The interviews did not shed light on exactly how those risk analyses have been conducted. None of the interviewees showed us a document in which the risk analysis has been put in writing.

The majority of agencies did not conduct any formal risk analysis to secure teleworking. At some of these agencies security measures were chosen on the basis of how similar organizations secured teleworking. At other agencies the ‘common sense’ of security experts or existing security baselines were used.

## 4.4 Conclusion

We started this chapter with describing the objective of our field survey, namely: to determine how information security in relation to teleworking is enabled within the Dutch national government. We then explained that we have conducted interviews with security experts at ten national government agencies in order to achieve this objective.

Thereafter we described the main results of our field survey. We first elaborated on how interviewees perceived the concept of teleworking in relation to the locations from which teleworking takes place, the telework times and the technology used for teleworking. We subsequently described which security controls the agencies have implemented in order to enable information security. Notably it is often unclear exactly on which grounds the agencies in our field survey have chosen their security controls for teleworking.

In the next chapter we use the (some of the) results of our field survey to develop a conceptualization of teleworking that corresponds to the way it takes place at the agencies in our field survey.

# Chapter 5: A conceptualization of teleworking

## 5.1 Introduction

In this chapter we develop a conceptualization of teleworking that corresponds to the way it takes place in practice. We start with formulating a general definition of teleworking based on the decree *'Raamregeling telewerken'* and some definitions of teleworking given by interviewees.

This general definition contains the broad term 'ICT'. From the ICT used for teleworking by the agencies included in our field survey – as described in the previous chapter – we derive two telework typologies. These typologies lie at the basis of the risk analysis methodology for securing teleworking described in the next chapter.

## 5.2 A general definition of teleworking

Teleworking is a very broad and complex phenomenon that has been the subject of a wide field of study. Although there is a growing consensus that – in general terms – teleworking is remote work and that it involves the use of ICT, a broad range of telework definitions are being used in practice. This causes problems: for example, academically it hinders the ability to compare findings from different sources.

This incomparability can sometimes be disadvantageous, but according to Sullivan [SULL2003] it is inevitable that researchers will use definitions through which they can best meet the aims of their specific research.

Sullivan argues that every research should be based on a precise project-specific definition, based on meaningful reasons and a clear rationale. In accordance with this view we formulate a general definition of teleworking in this paragraph and distinguish two telework typologies in the next paragraph.

### 5.2.1 Definition from the *'Raamregeling telewerken'*

The starting point of the development of our general definition of teleworking is the decree '*Raamregeling telewerken*' [BZK2001], which contains teleworking guidelines for the whole Dutch national government. In this decree teleworking is defined as follows:

> *Teleworking is performing work activities in behalf of the agency, at the civil servant's home, using information and (tele)communication technology.*

The decree further states that the person involved in teleworking is:

a. *The civil servant who is obliged to telework due to his function or*
b. *The civil servant who teleworks one or more workdays per week on a voluntary basis.*

With respect to this conceptualization of teleworking the following three points are worth noticing:

- Teleworking involves the use of ICT, which is in line with the growing consensus in literature on teleworking [SULL2003];
- Teleworking is place-dependent, since it has to take place at the home of the civil servant and
- Teleworking is time-dependent if it occurs on a voluntary basis. In that case the civil servant teleworks at least one workday per weak.

### 5.2.2 Definitions from the interviews

Despite this general government-wide conceptualization, the interviewees gave ambiguous answers when they were asked to define teleworking. Within some agencies there was no formal agency-wide notion of the concept. In those cases the interviewees made up their own definition.

Hereunder we have enumerated some of the definitions of teleworking brought up by interviewees.

**Teleworking is …**

1. *… working from a location that is not a standard agency location. This can be done by employees who either can or cannot make a connection with the agency's network.*
2. *… working from another location than the agency's location by means of a laptop (provided by the agency), whereby electronic access to the agency's network can be gained.*
3. *… connecting to the agency's network from a distance, whereby offered applications and email facilities can be used.*
4. *… 'home working' by means of ICT, whereby electronic data communication takes place between the teleworker and the agency.*
5. *… working from the home location on a structural basis and on a fixed time in the week using ICT and with a connection to the agency's network.*

Obviously the five above mentioned definitions vary in strictness; the first definition is the most general and the last definition is the most specific. It is remarkable that none of these definitions matches the conceptualization of the *'Raamregeling telewerken'*. It can be argued that the strictest definition, which is number five, comes closest. Next we shortly comment on all five definitions.

The first definition is very broad and does not prescribe the use of ICT for teleworking. Using hardcopy documents outside the office is therefore also a form of teleworking. This contradicts most of the existing literature on the subject and almost all other definitions mentioned by interviewees.

The second definition is more specific and broadly prescribes the use of certain technologies for teleworking, namely a laptop and electronic access to a network, whereas the third definition restricts the range of applications that can be used remotely. The first three definitions are time-and-place[15]-*in*dependent.

[15] Strictly speaking the first two definitions are place-independent insofar teleworking takes place outside the agency's location.

The fourth definition is place-dependent, since it prescribes that teleworking should take place from the teleworker's home. For the majority of agencies in our survey, teleworking primarily takes place from the home of the teleworker. In just a few cases however, this is claimed to be the only form of teleworking. Usually a smaller part of the teleworking workforce does not have a fixed work location or, in some cases, works from a satellite office.

In the fifth definition teleworking is not only place-, but also time-dependent since it prescribes that teleworking should take place on a structural basis and on a fixed time in the week. Time also plays a role in two other definitions mentioned by interviewees. In those definitions a distinction is made between occasional (e.g. less than one day a week) and structural teleworking (e.g. at least one day a week). Generally however, the amount of time an employee teleworks is not considered to be very relevant. Most interviewees do make a distinction between structural teleworkers and incidental teleworkers.

### 5.2.3 General definition of teleworking

From the definition from the *'Raamregeling telewerken'* and the definitions given by interviews we will now deduct the general definition of teleworking. The following two considerations lie at the basis of this process:

1. We wish to conform to the *Raamregeling telewerken*, because this decree contains the formal government-wide conceptualization and
2. We wish to include all notions of teleworking used by the agencies in our survey, because we would like our research to fit the practice.

Unfortunately these two considerations seem to be contradictory, because the decree's conceptualization is so specific that it does not match any of the definitions used in practice.

There is however, considerable consensus amongst interviewees that teleworking involves the use of ICT and therefore we follow the decree on this point. This choice complies with consideration one, while it only mildly conflicts with consideration two.

The time[16]-and-place-dependency of the decree's conceptualization is not in accordance with the majority of practiced telework definitions. We consider this undesirable as it is seriously in conflict with consideration two. Therefore we strip the decree's conceptualization from time-and-place-dependency, even though it conflicts with consideration one. What remains is the following general definition of teleworking:

**Teleworking is working from another location than the agency's location, by a civil servant in behalf of that agency, using information and communication technology (ICT).**

**Definition 5.1: General definition of teleworking**

It can be argued that this definition is based on meaningful reasons and a clear rationale conform Sullivan's view outlined at the beginning of this paragraph. Still the definition is not very project-specific, because it is very similar to the general consensus that teleworking is remote work which involves the use of ICT. For this research the project specificity is however enclosed in the definition's last term: ICT.

[16] Actually it follows from the decree that teleworking is only time-dependent if it is not inherent to a certain function.

## 5.3 Two telework typologies

According to Aad Kranendonk (KPMG), *information (and communication) technology* is the technology to gather, record and store, process, transport and/or provide data (information), including the knowledge about the appliance of that technology [JACO2000]. ICT is an umbrella term that can encompass not only today's technology, but also the technology of the future. Practical examples of ICT in use today are radio, television, cellular phones, computer and network hardware and software [SWS2004].

Since ICT is such a broad term and different forms of ICT generally require different security approaches it is impractical to include all forms of ICT into this research. Hence Kranendonk's abstract notion of ICT needs to be made more concrete. Therefore we focus on the ICT that is used for teleworking within the agencies in our survey.

In the previous chapter we have described that teleworkers generally use laptops (and sometimes PDAs) issued by the agency or other computing devices that satisfy relevant technical requirements for teleworking (e.g. privately owned desktop computers). In practice teleworkers use their computer:

1. 'Stand-alone' i.e. *not* as a part of the Citrix server based computing architecture or
2. As a part of the Citrix server based computing architecture.

Based on the way teleworkers use their computer, two telework typologies – T1 and T2 – can be distinguished.

| | |
|---|---|
| **T1** | Teleworking with a 'stand-alone' computer. Information is **stored** and **processed locally**. |
| **T2** | Teleworking with a computer that is connected to central servers by means of a Citrix server based computing architecture. Information is **stored** and **processed centrally**.<br><br>Only user interfaces, keystrokes and mouse clicks are communicated between the computer and the central servers. Communication takes place over the Internet. The computer only generates application screens. |

**Definition 5.2: Two telework typologies**

Information stored on central servers (T2) can sometimes be downloaded to local computers, for example via the 'safe as'-functionality in applications or via email. We would like to be able to methodologically strictly distinguish both typologies. Therefore we assume that information stored on central servers remains centrally stored.

In practice locally stored information (T1) may be exchanged between the stand-alone telework computer and various other computers. This can be done in different ways, for example by means of portable data carriers or email. The security approach required for different kinds of data exchange may vary considerably. Due to time constraints we leave the protection of information during transport outside the scope of our research.

Further information about the security of email can for example be found in [ISF2003] and [BZK1999]. The security of portable data carriers is discussed in the articles [GORG2005] and [MEAR2006].

## 5.4 Conclusion

In this chapter we have created a conceptualization of teleworking. First we formulated a time-and-place-independent definition of teleworking based on the decree '*Raamregeling telewerken*' and some of the definitions given by interviewees at the agencies in our field survey. This general definition is: 'Teleworking is working from another location than the agency's location, by a civil servant in behalf of that agency, using information and communication technology (ICT)'.

Since ICT is a broad term and it would be impractical to include all forms of ICT into our research we have subsequently defined two telework typologies T1 and T2 (see definition 5.2, paragraph 5.3) based on the ICT used for teleworking within the agencies in our field survey. These two telework typologies lie at the basis of the risk analysis methodology for securing teleworking described in the next chapter.

# Chapter 6: The Risk Analysis Methodology for Securing Teleworking

## 6.1 Introduction

In this chapter we present the final version of the Risk Analysis Methodology for Securing Teleworking (abbreviated to RAMST). RAMST is the end-product of our research and as such it meets the research objective defined in chapter 1.

This chapter consists of two main paragraphs. In the first main paragraph we explain the scope of RAMST in relation to the research demarcation outlined in chapter 1. We also clarify the four phases out of which RAMST consists and give recommendations on how it can be effectively used in practice. In the second main paragraph we describe three key documents included in RAMST, namely the 'Directory of Threats', the 'Directory of Controls' and the 'Threat/Control Matrix'.

In the next chapter we explain both (1) the development process that led to the concept version of RAMST and (2) the validation process that led to its final version as presented in this chapter.

## 6.2 Scope, set-up and use of RAMST

### 6.2.1 Scope of RAMST

In paragraph 1.2.1 we have defined the objective of our research as follows: 'to develop a risk analysis methodology that can be used by national government agencies to assess the security risks associated with teleworking and to identify the security controls required to keep the risks within acceptable limits'.

Teleworking however, is a very broad and complex phenomenon with enormous potential for variation in terms of, for example work location, work times, and ICT use. Information security, in turn, is a many-sided discipline that may be aimed at protecting a variety of assets such as information assets, software assets, physical assets and people.

Due to the breadth of the concepts 'teleworking' and 'information security' on the one hand and time constraints on the other, we were forced to restrict the scope of our research. In paragraph 1.2.2 we already argued that we would like the risk analysis methodology to be primarily aimed at protecting the asset 'information'. In addition to this we indicated that we would develop a specific conceptualization of the phenomenon teleworking that corresponds to the way it takes place in practice. In chapter 5 we have done this by formulating two telework typologies T1 and T2 based on the results of our field survey.

Consequently RAMST is particularly intended to be a tool for assessing the security risks that are (1) associated with the two telework typologies and (2) have a direct impact on the confidentiality, integrity and availability of information. In line with this RAMST primarily helps to identify the controls required to keep this particular group of risks within acceptable limits.

There is also a wide variety of risks that may negatively affect a national government agency without directly having an impact on information. This includes risks associated with a failure to follow regulatory frameworks with teleworking.

Although such risks are outside the scope of our research, we would like to stress that in case of teleworking it is not always possible to satisfy all the requirements included in VIR-BI (see paragraph 3.7.2). Especially the requirements associated with the physical security of locations and buildings are hard to meet.

In case teleworkers use special information (which is subjected to VIR-BI) the overall level of security enabled for teleworking, should be high enough to compensate for the specific VIR-BI requirements that cannot be met. Special information of the classification 'top secret' should not be used by teleworkers at all, because VIR-BI explicitly states that such information should not be taken home or to a foreign country.

### 6.2.2 Set-up of RAMST

A RAMST review is carried out in four successive phases. Hereunder each phase is briefly explained. The steps required to complete each phase are described in detail in appendix C.

**Phase 1: Set the scene**
In this phase a review group that will conduct the risk analysis is first established. The review group consists of a coordinator working in conjunction with a responsible line manager. A coordinator may for example be a specialist in information security or an internal auditor.

Subsequently the scope of the risk analysis is determined. This is done by determining which information is used by the teleworkers under review (hereafter referred to as 'telework information') and by choosing the telework typology (T1 *or* T2) for which the risk analysis will be conducted.

**Phase 2: Assess business risk**
In phase 2 the business risk associated with teleworking is assessed by evaluating the business consequences and impact of a loss of the confidentiality, integrity and availability of telework information.

For each quality aspect of telework information the review group should examine a question list. For each type of consequence on this question list (e.g. fraud, additional costs, or business disruption), the responsible manager should rate what the associated business impact is. For this purpose the following impact ratings can be used: (A) Serious Damage, (B) Significant Damage, (C) Minor Impact and (D) Negligible. Together the individual consequence ratings result in an overall rating for the quality aspect concerned.

The overall ratings of all three quality aspects together classify the telework information in terms of its importance to the business and hence the level of protection needed.

**Phase 3: Assess threats, vulnerabilities and controls**
In phase 3 the key threats and vulnerabilities associated with the chosen telework typology are assessed and the controls required to keep the risks within acceptable limits are identified.

To support the assessment of threats and vulnerabilities, RAMST includes a 'Directory of Threats' (see paragraph 6.3.2) which contains common threats associated with the two telework typologies. The review group should discuss how vulnerable the agency is to each threat that is relevant for the chosen telework typology. Subsequently a vulnerability rating should be assigned according to the likelihood of the threat materializing. For this purpose the following ratings can be used: (A) Highly Possible, (B) Possible, (C) Unlikely or (D) Impossible.

Thereafter the review group should identify the controls required to reduce the vulnerability associated with each relevant threat. This is done by taking into consideration the required level of protection for the quality aspects (as identified in the previous phase), the relevance of the threat for these quality aspects and the vulnerability to the specific threat (as identified above).

To support the identification of controls RAMST includes a 'Directory of Controls' and a 'Threat/Control Matrix'. The 'Directory of Controls' (see paragraph 6.3.3) contains common controls that can be used to reduce the threats included in the 'Directory of Threats'. The 'Threat/Control Matrix' (see paragraph 6.3.4) indicates the strongest relationship between these threats and controls.

**Phase 4: Produce agreed action plan**
In the fourth and last phase the review group should agree on an action plan for controls, designed to keep risks within acceptable limits.

In the action plan the security controls are prioritized by taking into consideration the effectiveness of the controls with respect to safeguarding the quality of telework information, the cost-effectiveness of the controls and the ease with which the controls can be implemented. The action plan also specifies who is responsible for implementing controls and what the implementation dates are.

### 6.2.3 Use of RAMST

In RAMST the nature of telework information (e.g. its sensitivity or criticalness) determines the required level of protection and hence the amount and character of the security controls that need to be implemented. To prevent under- or overprotection it is best to conduct a RAMST review for groups of teleworkers with homogenous information needs (e.g. teleworkers who work at the same division or on the same business process).

In practice the information needs of an agency's teleworkers may vary considerably. Consequently it may be that many different groups of teleworkers with homogenous information needs can be distinguished. In that case it may be infeasible to conduct a complete RAMST review for every single group of teleworkers.

In this situation it may be more efficient to establish a security baseline which enumerates the security controls that should be implemented in order achieve a desired minimum level of security for teleworking. This can be done by performing a RAMST review for the information that is commonly used by the majority of all teleworkers. This security baseline should offer sufficient protection for all information that has the same or a lower classification than this 'commonly used information' in terms of its importance to the business.

The figure below illustrates how the security baseline can be used in practice. For each group of teleworkers phase 1 and 2 of the RAMST review should be carried out in order to classify the information used by those teleworkers. In case the level of protection required for this information is lower than or equal to the level of protection offered by the baseline, the security controls included in the baseline can be implemented. Otherwise phase 3 and 4 of the RAMST review should also be conducted to identify which additional security controls need to be implemented.

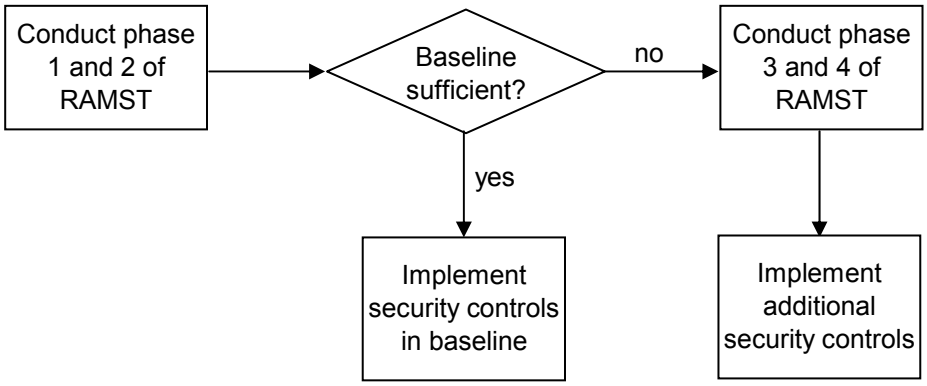


**Figure 6.1: Baseline or complete RAMST review?**

## 6.3 Threats, controls and their relationship

### 6.3.1 The telework service

For a proper understanding of the set-up of the 'Directory of Threats', the 'Directory of Controls' and the 'Threat/Control Matrix', insight into the conceptual 'telework service' is first required. As illustrated in the figure below this telework service consists of five interacting components, namely: the teleworker, the telework location, the telework computer, the Internet connection and the remote access farm.

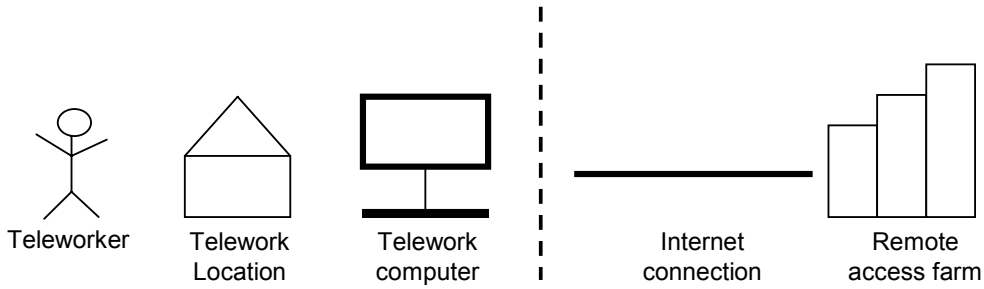


**Figure 6.2: The telework service**

The threats included in the 'Directory of Threats' and most controls included in the 'Directory of Controls' are related to one of the five interacting components of the telework service. For typology T1 (stand-alone teleworking) only the three components on the left-hand side of the dotted vertical line are relevant. For typology T2 (teleworking with a connection to central servers) all five components are relevant. The components are described in more detail in the table below.

| **The teleworker** |
|---|
| The teleworker is an employee of a national government agency who performs his work activities at a remote location. A teleworker makes use of his telework computer and possibly the remote access farm to perform his work activities. |
| **The location** |
| The telework location is the place where teleworkers perform their work activities. In practice teleworking mainly takes place from the teleworker's home, but sometimes teleworkers do not have a fixed location. In the latter case they may work from various locations such as hotels, public facilities or cars. Sporadically teleworking takes place from a satellite office. Such offices only house teleworkers from a single organization. |
| **The telework computer** |
| A telework computer is a computing device that is used for teleworking. Telework computers issued by agencies are primarily laptops. PDAs are only issued on a very small scale. A telework computer that is not issued by an agency can be anything that satisfies relevant technical requirements for teleworking (e.g. desktops). |
| **The Internet connection** |
| The Internet is used to establish a connection between the telework computer and the remote access farm. Only user interfaces, key strokes and mouse clicks are communicated once a connection has been established. |
| **The remote access farm** |
| The remote access farm is a collection of computer servers, typically housed inside the agency's buildings, that facilitates remote access to certain applications in behalf of teleworkers. |

**Table 6.1: Description of the components of the telework service**

### 6.3.2 The Directory of Threats

The 'Directory of Threats' (see appendix J) contains the various security threats associated with the two telework typologies. Every threat included in this directory is grouped under one of the five components of the telework service.

Figure 6.3 shows a part of the index of the 'Directory of Threats', in this case 'Component A: the teleworker'. The index contains the unique references and titles of all threats included in the directory. For every quality aspect – confidentiality, integrity and availability – of telework information an indication is given of the relevance of the threat for that quality aspect by means of the symbols '+', '-' and 'X'. These symbols respectively express 'high relevance', 'low relevance' and 'not relevant'. The same symbols are used to indicate the relevance of a threat for the two different telework typologies T1 and T2.

The unique threat reference included in the index of the 'Directory of Threats' can be used to find the associated 'threat box' which contains additional information about the threat. As illustrated by figure 6.4 a threat box contains the information included in the index plus a high-level description and more detailed 'supporting information'. If necessary the threat box also contains a description of the relevance of the threat for the two different telework typologies T1 and T2.

Note that the threat references included in the 'Directory of Threats' are hyperlinks. In the digital version of this thesis, these hyperlinks can be used to navigate between the index of the 'Directory of Threats' and the individual threat boxes. For example: by clicking on the reference A1.1 in the index of the 'Directory of Threats', the threat box of the threat 'Disclosure of log-on information' appears. By subsequently clicking on the letter 'A' of the reference A1.1 included in the threat box, the index of the 'Directory of Threats' appears again.

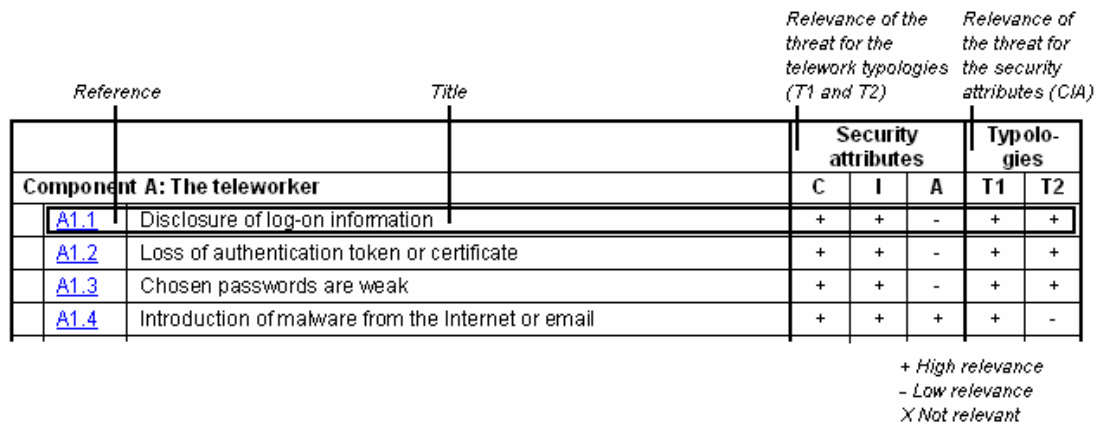


**Figure 6.3: Part of the index of the 'Directory of Threats'**

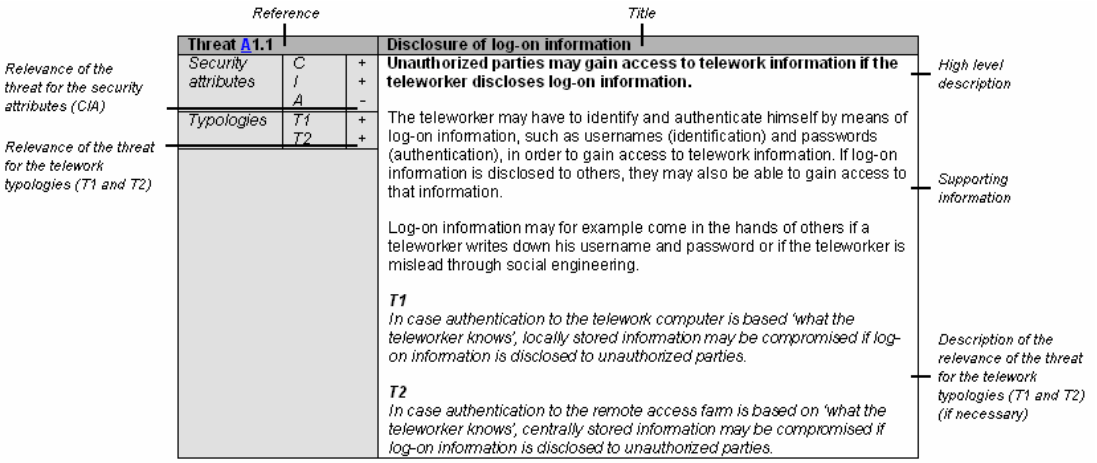


**Figure 6.4: The threat box of the threat 'Disclosure of log-on information'**

### 6.3.3 The Directory of Controls

The 'Directory of Controls' (see appendix K) contains the common controls that can be used to reduce the threats included in the 'Directory of Threats'. Most controls in the 'Directory of Controls' are grouped under one of the five components of the telework service. A few controls however, cannot be easily related to individual components of the telework service. These controls are included in a separate group named 'general controls'.

Figure 6.5 shows a part of the index of the 'Directory of Controls', in this case 'Group D: Controls telework computer'. The index contains the unique references and titles of all controls included in the directory. For every control an indication is given of the (1) relevant security attributes (why) – confidentiality, integrity and availability –, (2) the place in the event cycle (when) – prevention, detection and repression – and (3) the sphere of action (what) – organizational, logical and physical. This is done by placing a marking ('V') under the relevant aspects associated with 'why', 'when' and 'what'.

The unique control reference included in the index of the 'Directory of Controls' can be used to find the associated 'control box'. As illustrated by figure 6.6 a control box contains the information included in the 'index' plus a more detailed description of the control. If applicable, a control box also includes a description of requirements from the decree '*Raamregeling telewerken*' or the decree VIR-BI.

Note that the control references included in the 'Directory of Controls' are hyperlinks. In the digital version of this thesis, these hyperlinks can be used to navigate between the index of the 'Directory of Controls' and the individual control boxes. For example: by clicking on the reference D2.11 in the index of the 'Directory of Controls', the control box of the control 'Automatically encrypt data on the hard disk' appears. By subsequently clicking on the letter 'D' of the reference D2.11 included in the control box, the index of the 'Directory of Controls' appears again.

| | | *Indication of the:* | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| *Reference* | *Title* | *Relevant security attributes* | | | *Place in the event cycle* | | | *Sphere of action* | | |
| | | **Why** | | | **When** | | | **What** | | |
| **Group D: Controls telework computer (controls aimed at protecting a laptop computer issued by the agency)** | | **C** | **I** | **A** | **P** | **D** | **R** | **O** | **L** | **P** |
| ... | | | | | | | | | | |
| *Category 2: Software controls* | | | | | | | | | | |
| ... | ... | V | V | V | V | V | V | | V | |
| D2.11 | Automatically encrypt data on the hard disk | V | V | | V | | | | V | |
| D2.12 | Implement automatic power-safe | | V | V | V | V | | | V | |
| D2.13 | Implement device lock software | V | V | V | V | V | | | V | |
| D2.14 | Implement an URL filter | V | V | V | V | V | | | V | |
| ... | ... | | | | | | | | | |

**Figure 6.5: Part of the index of the 'Directory of Controls'**

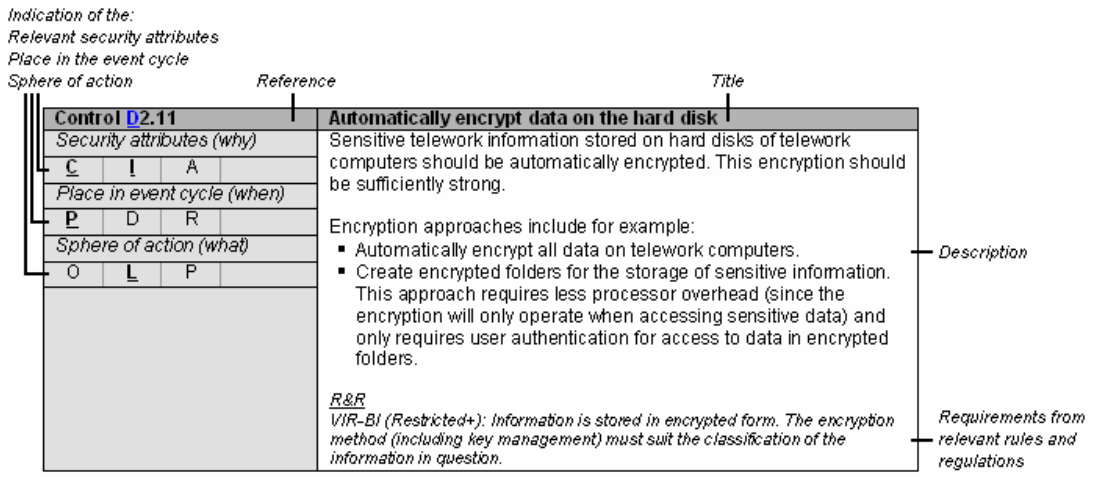


**Figure 6.6: The control box of the control 'Automatically encrypt data on the hard disk'**

### 6.3.4 The Threat/Control Matrix

The ‘Threat/Control Matrix’ (see appendix L) indicates the strongest relationships between the threats and controls included in respectively the ‘Directory of Threats’ and the ‘Directory of Controls’.

The matrix is intended only as a guide as many controls may be required to reduce an individual threat, whilst a number of different threats may be mitigated by a single control. The ‘Threat/Control Matrix’ helps to identify controls that strongly relate to a particular threat or to identify the threats that are affected by particular controls.

Figure 6.7 illustrates a part of the ‘Threat/Control Matrix’. Within the ‘Threat/Control Matrix’, the threat column on the left hand side lists all of the threats from the ‘Directory of Threats’, with each threat-title preceded by its reference. The row along the top shows the controls from the ‘Directory of Controls’, with each control-title preceded by its reference.

By reading across from the threat reference on the left, the set of controls that assist in managing that threat can be found. Details about controls can subsequently be found in the ‘Directory of Controls’. Conversely by looking for a particular control in the matrix, references to the threats that it assists to manage can be found from the list of threats on the left hand side. Details about threats can subsequently be found in the ‘Directory of Threats’.

A ‘threat/control junction’ may be empty or it may contain the letter ‘V’ or ‘G’. The letter ‘V’ is used to indicate that there is a strong relationship between a threat and a control. A ‘G’ indicates that the control in question is a general control. General controls cannot be easily mapped to specific threats. They should be evaluated individually, independent of relevant threats.

Note that the threat and control references included in the ‘Threat/Control Matrix’ are hyperlinks. In the digital version of this thesis, these hyperlinks can be used to evoke the individual threat and control boxes. For example: by clicking on the reference A1.1 in the threat column, the threat box of the threat ‘Disclosure of log-on information’ appears and by clicking on the reference D2.11 in the control row, the control box of the control ‘Automatically encrypt data on the hard disk’ appears.

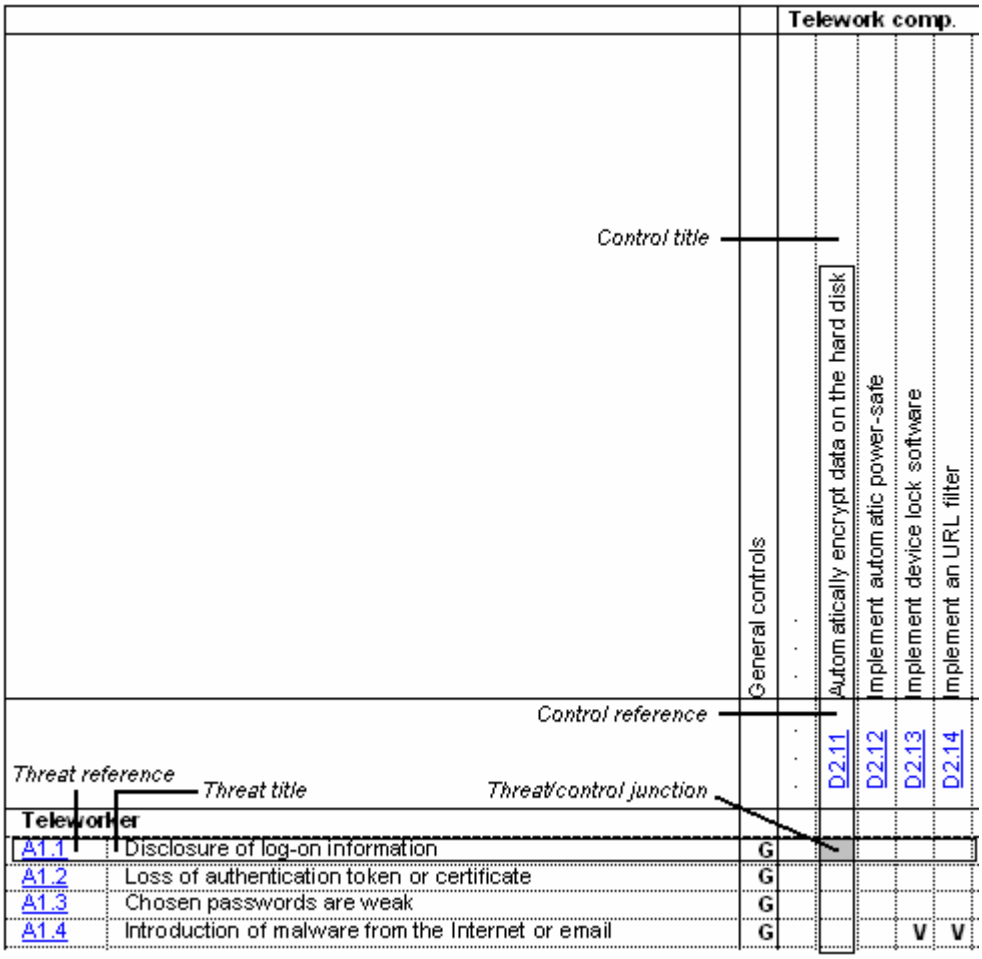


**Figure 6.7: Part of the Threat/Control Matrix**

## 6.4 Conclusion

In this chapter we have presented the final version of RAMST. The chapter consists of two main paragraphs. In the first main paragraph we have described the scope, set-up and use of RAMST. We first indicated that RAMST is a tool that can be used by national government agencies to assess the security risks – that are (1) associated with the two telework typologies (T1 and T2) and (2) have a direct impact on the confidentiality, integrity and availability of information – and to identify the controls required to keep this particular group of risks within acceptable limits. Thereafter we explained the four phases out of which RAMST consist and described how the methodology can be effectively used in practice.

We started the second main paragraph with a description of the conceptual telework service that consists of five interacting components. Thereafter we described three key documents included in RAMST, namely:

- The 'Directory of Threats' which contains the various security threats associated with the two telework typologies (T1 and T2). Every threat is grouped under one of the five components of the telework service.
- The 'Directory of Controls' which contains the common controls that can be used to reduce the threats included in the 'Directory of Threats'. Most controls are grouped under one of the five components of the telework service.
- The 'Threat/Control Matrix' which indicates the strongest relationships between the threats and controls included in respectively the 'Directory of Threats' and the 'Directory of Controls'.

In the next chapter we explain (1) the development process that led to the concept version of RAMST and (2) the validation session that led to its final version as presented in this chapter.

# Chapter 7: Development and Validation of RAMST

## 7.1 Introduction

In the previous chapter we have described the final version of the Risk Analysis Methodology for Securing Teleworking (RAMST). In this chapter we describe the development process that led to the concept version of RAMST as well as the validation session with a focus group that led to its final version.

We first explain which existing risk analysis methodology lies at the basis of RAMST and which adjustments we have made in order to make this methodology better suit the purposes of our research. Subsequently we describe how we have developed the 'Directory of Threats', the 'Directory of Controls' and the 'Threat/Control Matrix'. Lastly we elaborate on the validation session we have performed in order to test the quality of RAMST.

## 7.2 Choosing a risk analysis methodology

The objective of our research is 'to develop a *risk analysis methodology* that can be used by national government agencies to assess the security risks associated with teleworking and to identify the security controls required to keep the risks within acceptable limits'.

In paragraph 3.6 we have indicated that many different kinds of risk analysis methodologies are already available in the field of information security. These methodologies can be standardized or made-to-measure and may focus on various objects such as the organization, business processes, information systems or applications.

Since such a wide variety of risk analysis methodologies already exists, it would be very inefficient to develop RAMST from scratch. Instead it is more practicable to base RAMST on some existing methodology. This introduces the question which risk analysis methodology that should be. Since the decree VIR outlines the organization and approach of information security within the national government and our research is aimed at the national government, it seems logical to use a risk analysis methodology that corresponds to this decree.

### 7.2.1 The decree VIR and the D&V-analysis

The national government has chosen to use the dependency and vulnerability analysis (D&V-analysis) as the standard risk analysis methodology for enabling adequate information security.

The D&V-analysis is conceptually described in the decree VIR [BIZA1994]. This decree prescribes that a D&V-analysis should be performed for every information system (VIR article 4, sub a) and for every responsibility area[17] (article 4, sub b).

[17] A responsibility area consists of all facilities that are available to one or more information systems and for which the responsibility can univocally be attributed to one organizational unit (e.g. an internal network LAN). [BIZA1994]

A D&V-analysis starts with the common quality requirements and existing security controls which are laid down in the security policy (article 3). The dependency analysis is employed to determine the extent in which business processes depend on the quality of an information system and what the potential damage is in case the information system fails. The dependency analysis results in a set of quality requirements (expressed in terms of confidentiality, integrity and availability) for the information system. The same approach is prescribed for responsibility areas.

The next step is to identify and analyse the relevant threats to the information system or responsibility area (article 4, sub c). Subsequently security controls are chosen in such a way that a vulnerability analysis can prove that the determined quality requirements are met (article 4, sub d). The identified security controls are laid down in an information security plan (article 4, sub e). This is done per information system and per responsibility area. The security plan is periodically evaluated and – if necessary – adjusted to changed circumstances (article 4, sub f).

### 7.2.2 The Guidebook D&V analysis

The decree VIR describes the D&V-analysis in abstract terms. As such it is not directly applicable in practice. A more concrete approach for performing a D&V-analysis is laid down in the Guidebook D&V-analysis *'Handboek A&K-analyse'* [ACIB1998]. This guidebook describes the steps that should be performed in order to analyze dependencies and vulnerabilities in a systematic way. The guidebook is written on behalf of national government agencies such as ministries and their divisions. A description of the guidebook's approach for carrying out a D&V-analysis is included in appendix B.

Unfortunately the guidebook's D&V-analysis is less suitable for our research, because it is notoriously complex and laborious to use. Besides that it is centred on the business process. Since we would like our risk analysis methodology to be primarily aimed at protecting the asset 'information' (see paragraph 1.2.2), it is more practical to base this methodology on some existing methodology that is centred on information (systems) instead. Hence on this point we prefer to deviate from the decree VIR's approach.

### 7.2.3 Suitability of SPRINT for this research

An eye catching risk analysis is the SPRINT[18] methodology [ISF1997] developed by the Information Security Forum (ISF). The SPRINT methodology is designed to analyze information systems. The idea behind SPRINT is that most risk analysis methodologies are useful for securing specific information systems, but that they are hard to understand, produce results of uncertain value and require experienced risk analysis practitioners – who are in short supply – to apply them. In response to this, SPRINT is business oriented and easy to use.

SPRINT's user friendliness and the fact that it centers on information systems instead of business processes, suits our research. Besides that, SPRINT closely corresponds to the approach described in the decree VIR, because it consists of two main parts: a dependency and a vulnerability analysis. Furthermore SPRINT distinguishes the quality aspects of confidentiality, integrity and availability, which is also in line with the decree VIR.

[18] SPRINT stands for 'Simplified Process for Risk Identification'.

For these reasons we have primarily based RAMST on SPRINT. Nevertheless we had to make some significant changes to SPRINT in order to make the methodology better suit the purposes of our research. In the next paragraph we describe SPRINT methodology and explain the changes we have made.

## 7.3 Adjustments to SPRINT

A SPRINT review is carried out in three phases. For the purpose of our research we have made some significant changes to phases 1 and 2. Phase 3 'Produce agreed action plan' largely remained the same. We also added an additional phase 'Set the scene' (see paragraph 6.2.2) that comes before SPRINT's original phase 1. This resulted in the concept version of RAMST.

Hereunder we briefly describe phases 1 and 2 of SPRINT and clarify the relevant changes we have made. For a more detailed description of the complete SPRINT methodology we refer to the 'SPRINT User Guide' [ISF1997a].

### 7.3.1 Phase 1: Assess business risk

**Description**

The first phase of the SPRINT methodology corresponds to the dependency analysis described in the decree VIR. In this phase the business risk associated with the information system is assessed by evaluating the business consequences and impact of a loss of the confidentiality, integrity and availability of the information processed by that information system.

For each quality aspect the review group should examine a question list. For each type of consequence on this question list (e.g. fraud, additional costs, or business disruption), the business manager has to rate what the associated business impact is. For this purpose the following impact ratings can be used: (A) Business Survival Threatened, (B) Serious Damage, (C) Significant Damage, (D) Minor Impact and (E) Negligible. Together the individual consequence ratings result in an overall rating for the quality aspect concerned.

The overall ratings of all three quality aspects together classify the information system as a whole in terms of its importance to the business and hence the level of protection needed.

**Adjustments**

For our research the required level of protection should depend on the information that is used by the teleworkers under review (i.e. telework information) instead of information processed by individual information systems. Therefore we have adjusted the question lists included in SPRINT to make sure that the questions are aimed at telework information.

This operation was quite straightforward. We replaced the word 'information' – in the question lists associated with the quality aspects of confidentiality and integrity – and the word 'application' – in the question list associated with availability – by the words 'telework information'.

Besides that we have removed the question associated with the business consequence '*Direct loss of business*' from the three question lists, because we consider this type of consequence to be less relevant for a non-commercial national

government. Instead of this we adopted the following questions from ACIB's D&V-analysis [ACIB1998]:

- Aspect: *Confidentiality*. Consequence: *Political implications.* Question*: Could publication of telework information lead to social commotion or political turbulence?*
- Aspect: *Integrity*. Consequence: *Personal well-being*. Question: *Could corrupted telework information lead to disasters in relation to the well-being of persons?*
- Aspect: *Availability*. Consequence: *Personal well-being*. Question: *Could unavailable telework information directly lead to life threatening situations or seriously affect the health of persons?*

Furthermore we have not adopted the rating of 'Business Survival Threatened' included in the SPRINT methodology, because it seems unlikely that the existence of a national government agency will be threatened as a result of the loss of the quality of (telework) information. Instead we used the remaining four ratings: (A) Serious Damage, (B) Significant Damage, (C) Minor Impact and (D) Negligible.

### 7.3.2 Phase 2: Assess threats, vulnerabilities and controls

**Description**

The second phase of the SPRINT methodology corresponds to the vulnerability analysis described in the decree VIR. In this phase the key threats and vulnerabilities of an information system are assessed and controls to keep the risks within acceptable limits are identified.

Hereto the SPRINT methodology includes 24 so-called 'threat and vulnerability factors' associated with information systems (e.g. unauthorized access to data by employees, input errors or major disasters). Every 'threat and vulnerability factor' is grouped under one of the three quality aspects.

Per quality aspect the review group should discuss how vulnerable the business is to each of the associated 'threat and vulnerability factors' and subsequently assign a vulnerability rating according to the likelihood of threats materializing. For this purpose the following ratings can be used: (A) Probable, (B) Highly Possible, (C) Possible, (D) Unlikely or (E) Impossible.

Thereafter the review group should identify the controls required to reduce the business risk associated each 'threat and vulnerability factor'. This is done by taking into consideration both the required level of protection for the quality aspect concerned (as identified in phase 1) and the vulnerability to the specific 'threat and vulnerability factor'.

The 'SPRINT Directory of Controls' [ISF1997b] is intended to assist the process of identifying controls. For every 'threat and vulnerability factor' this document presents a number of controls that can be applied to the information system in order to reduce risk.

**Adjustments**
In the SPRINT methodology the threats, vulnerabilities and controls are assessed per quality aspect. This is possible because each 'threat and vulnerability factor' included in SPRINT is grouped under one of the three quality aspects. The main advantage of this approach is that the level of protection associated with the quality aspect (as determined in phase 1) can easily be related to the vulnerability to the specific 'threat and vulnerability factor'. Based on this mapping appropriate security controls can subsequently be selected.

In RAMST we have replaced SPRINT's 'threat and vulnerability factors' by the 'Directory of Threats'. This directory contains threats associated with the two telework typologies (T1 and T2). We have not grouped the threats included in the 'Directory of Threats' under quality aspects. That would be too arbitrary, because most of these threats may have an equal impact on more than one quality aspect.

Consequently in RAMST the threats, vulnerabilities and controls cannot be assessed per quality aspect. Therefore it is harder to relate the level of protection associated with the quality aspects to the vulnerability to the threats included in the 'Directory of Threats'. This mapping is however essential for selecting security controls. Therefore we have given an indication of the relevance of each threat included in the 'Directory of Threats' for each of the three quality aspects using the symbols '+ (relevant) - (less relevant) and X (not relevant)' (see paragraph 6.3.2).

For every 'threat and vulnerability factor' the 'SPRINT Directory of Controls' presents a number of controls that can be applied to an information system in order to reduce risk. Alternatively RAMST incorporates a 'Directory of Controls' that can be used to reduce the risks associated with the two telework typologies and a 'Threat/Control Matrix'. This matrix indicates the strongest relationship between the threats included in the 'Directory of Threats' and the controls included in the 'Directory of Controls'.

Furthermore we have not adopted the rating 'Probable' included in the SPRINT methodology, because we also removed the highest rating in the previous phase and it is methodologically better if both phases have an equal amount of ratings. Therefore in RAMST we used the remaining four ratings: (A) Highly Possible, (B) Possible, (C) Unlikely or (D) Impossible.

## 7.4 Development of the 'Directory of Threats', the 'Directory of Controls' and the 'Threat/Control Matrix'

### 7.4.1 Directory of threats

As described in paragraph 4.3.4, the field survey did not shed much light on which concrete security threats are related to teleworking. Therefore we had to primarily rely on literature to develop our 'Directory of Threats'.

The ISF report 'Securing remote access by staff – Directory of risks and controls' [ISF1999] is the most important information source we have used. This report presents detailed directories of the risks and controls associated with providing a remote access service to staff. The ISF report is very broad in scope and is aimed at a variety of remote access methods (e.g. Citrix) and connections (e.g. the Internet). Furthermore it is not exclusively aimed at safeguarding the quality of information, but also on safeguarding other assets, such as equipment.

The ISF directory of risks contains a description of 112 detailed risks associated with remote access. It also includes a brief description of the possible business consequences (e.g. loss of or damage to equipment, loss or corruption of sensitive data, etc.) associated with each risk. The risks included in the ISF report are grouped under each of the 12 components of the so-called 'remote access service'.

Because of the ISF report's broad scope not all these risks are relevant for the two telework typologies we have identified. Therefore we have carefully selected only those risks we considered to be important. We subsequently reformulated and/or combined some of these risks in order to make them better fit the two typologies in scope. We also added a few new risks based on some of the government related telework security incidents described in chapter 1 (e.g. malfunctioning telework computers in the hands of third parties).

To the resulting risks we added an indication of their relevance for the three security attributes and the two telework typologies. We also mapped each risk to one of the five components of our conceptual telework service (see paragraph 6.3.1). Finally we named the 'risks' 'threats', because they describe the circumstances that are likely to cause that security breach and do not express the damage associated with and/or the likelihood of a security breach occurring. This resulted in the concept version of our 'Directory of Threats'.

### 7.4.2 Directory of controls

The results of our field survey have been the starting point of the development of our 'Directory of Controls'. Most controls mentioned by the interviewees have been included in this directory. We also used supporting material provided by interviewees, such as a code of conduct for information security and teleworking and a protocol for home-working.

Other controls have been adopted from relevant security literature such as the ISF report 'Securing remote access by staff – Directory of risks and controls' [ISF1999], the 'Code of practice for information security management' [ISO2005] the articles 'Securing Teleworker Networks' [PHIF2003] and '*Citrix-omgeving nader bekeken*' [BRUI2004] as well as various articles concerning the security of mobile computers [GREE2002] [ISF2002] [PSTN2003] [POTT2004] [SYMA2005].

To the resulting controls we have added an indication of the (1) relevant security attributes (why) – confidentiality, integrity and availability –, (2) the place in the security cycle (when) – prevention, detection and repression – and (3) the sphere of action (what) – organizational, logical and physical. We also added a description of the relevant rules and regulations such as the decree '*Raamregeling telewerken*' and the decree VIR-BI to a number of controls.

Where possible we have mapped the controls to the five components of the telework service. We found that a few controls could not be easily related to an individual component of the telework service. For these controls we have created a separate group named 'general controls'. This resulted in the concept version of our 'Directory of Controls'.

### 7.4.3 Threat/Control Matrix

The ‘Threat/Control Matrix’ is inspired on the ‘risk/control tables’ included in the ISF report ‘Using email: detailed risks and controls’ [ISF2003]. We have constructed the concept version of the ‘Threat/Control Matrix’ by evaluating per threat – included in the concept version of the ‘Directory of Threats’ – which controls – included in the concept version of the ‘Directory of Controls’ – can be used to reduce that threat. We only mapped those threats and controls that have a strong relationship.

Each threat is mapped to at least one control and each control is mapped to at least one threat. This way we made sure that each threat can be reduced by one or more controls and that there is no surplus of controls. In this process we left the general controls out of consideration, because they cannot be easily mapped to specific threats.

## 7.5 Validation concept version of RAMST

### 7.5.1 Approach

We have validated the concept version of RAMST by discussing it in a focus group. This focus group consisted of eight security experts who work as IT auditors and IT security consultants for PricewaterhouseCoopers.

In order to enable the members of the focus group to prepare for the meeting, we sent them the concept version of the framework considerable time in advance. Since the complete RAMST document is sizeable, we did not ask the focus group members to completely read it. Instead we asked them to go through specific sections which we considered to be important.

After a short presentation in which we explained the objective of our research, we asked the members of the focus group to give their opinion about the:

- Set-up of each phase of the risk analysis methodology;
- The correctness and completeness of the ‘Directory of Threats’ in relation to the two telework typologies;
- The correctness and completeness of the ‘Directory of Controls’ in relation to the threats included in the ‘Directory of Threats’ and
- The correctness of the ‘Threat/Control Matrix’.

### 7.5.2 Results

During the discussion about the set-up of RAMST, some focus group members argued that RAMST is too theoretical. It is for example hard to identify which information is used by teleworkers (phase 1). In addition to this, some of them were of the opinion that the methodology is too laborious and that a baseline approach would be more practical.

In response to this we have included recommendations on the practical use of RAMST in paragraph 6.2.3. Here we have described that RAMST should be performed for groups of teleworkers with similar information needs and that it is more efficient to develop a security baseline if many of such groups can be distinguished. Unlike some focus group members we believe that the managers involved in the RAMST review intuitively know which information is used by their teleworking employees.

The focus group members only had a few comments on the accuracy and completeness the 'Directory of Threats' and the 'Directory of Controls'. For example, in the concept version of RAMST the threats associated with the teleworker are divided into errors in unconscious and errors in conscious behavior. The focus group members justifiably argued that this distinction is hard to make. Therefore we have joint all threats associated with the teleworker together in the final version of RAMST. On advice of the focus group members we also included some additional security controls associated with the remote access farm into the final version of RAMST.

With respect to the 'Threat/Control Matrix' some focus group members noticed some inaccuracies with respect to the numbering of threats and controls. These inaccuracies have been corrected in the final version of RAMST. They also noticed that one threat was not mapped to any security control. This has also been adjusted in the final version of RAMST.

## 7.6 Conclusion

We have started this chapter with a description of the development process that led to the concept version of RAMST. We first explained that we have based RAMST on the SPRINT risk analysis methodology [ISF1997], because SPRINT is relatively easy to use, focuses on information (systems) and largely corresponds to the decree VIR. Subsequently we described the adjustment we made to the original SPRINT methodology to make it better suit the purposes of our research.

Furthermore we elaborated on how we developed the concept versions of 'Directory of Threats', the 'Directory of Controls' and the 'Threat/Control Matrix' included in RAMST. These documents are based on a variety of literature on information security such as the ISF report 'Securing remote access by staff – Directory of risks and controls' [ISF1999].

Lastly we have described the set-up and results of the validation session with a focus group that consisted of eight security experts. The comments of the focus group members have been processed into the final version of RAMST. This final version is described in the previous chapter.

# Chapter 8: Conclusions and further research

## 8.1 Final result of our research

Recently a number of telework security incidents whereby sensitive government information came into the hands of third parties have been in the news. These incidents indicate that national government agencies do not always adequately enable information security with respect to teleworking.

Therefore we decided to develop a risk analysis methodology that can be used by national government agencies to assess the security risks associated with teleworking and to identify the security controls required to keep the risks within acceptable limits. We named this methodology the 'Risk Analysis Methodology for Securing Teleworking' (RAMST).

The security risks covered by RAMST primarily involve those risks that (1) have a direct impact on the confidentiality, integrity and availability of information and (2) are associated with the two telework typologies (T1 and T2) defined in chapter 5. These telework typologies are based on the way in which teleworking takes place at the ten agencies included in our field survey (see chapter 4).

RAMST consists of the following four phases that should be successively completed:

| | |
|---|---|
| **Phase 1** | **Set the scene**<br>In this phase a review group is established and the scope of the risk analysis is determined. The latter is done by choosing a telework typology (T1 or T2) and by determining which information is used by the teleworkers under review. |
| **Phase 2** | **Assess business risks**<br>In this phase the information that is used by teleworkers is classified in terms of its importance to the agency and hence the level of protection needed. |
| **Phase 3** | **Assess threats, vulnerabilities and controls**<br>In this phase the key threats and vulnerabilities associated with the chosen telework typology are determined as well as the controls required to keep the risks within acceptable limits. |
| **Phase 4** | **Produce agreed action plan**<br>In this phase a plan of action for implementing controls is agreed. |

Three key documents support the review group in carrying out phase 3, namely:

- The 'Directory of Threats' which contains the various security threats associated with the two telework typologies;
- The 'Directory of Controls' which contains the common controls that can be used to reduce the threats included in the 'Directory of Threats' and

- The ‘Threat/Control Matrix’ which indicates the strongest relationships between the threats and controls included in respectively the ‘Directory of Threats’ and the ‘Directory of Controls’.

The set-up of RAMST and the supporting documents are described in detail in chapter 6. In this chapter we have also outlined how RAMST can be effectively used in practice.

## 8.2 Development and validation of RAMST

Since many risk analysis methodologies already exist in the field of information security it would be very inefficient to develop RAMST from scratch. Instead we have based RAMST on the SPRINT methodology [ISF1997] developed by the Information Security Forum (ISF). We have used SPRINT because it is relatively easy to use, focuses on information (systems) and largely corresponds to the decree VIR. The latter point is important, because the decree VIR outlines the organization and approach of information security within the national government.

We have made a number of adjustments to the original SPRINT methodology in order to make it better suit the purposes of our research. These adjustments are described in detail in chapter 7. The ‘Directory of Threats’, the ‘Directory of Controls’ and the ‘Threat/Control Matrix’ incorporated in RAMST are based on a variety of literature on information security.

The resulting concept version of RAMST has been validated in a focus group that consisted of eight security experts. Their comments have been used to improve the concept version of RAMST. This led to the final version of RAMST as presented in chapter 6.

## 8.3 Further research

The most obvious opportunity for further research is to include the security risks and controls associated with exchange of locally stored information between the stand-alone telework computer (T1) and various other computers into RAMST (see chapter 5). This should at least concern the security risks and controls associated with email, portable data carriers and/or network access points at the office, because our field survey indicates that these are ways in which such information exchange may take place.

Another interesting option for further research would be to include more national government agencies into the field survey in order to investigate if there are any other ways in which teleworking takes place within the national government and/or to find out if there are any other security risks or controls that need to be included into RAMST.

It would also be useful to further improve the quality of RAMST by performing some additional and more thorough validation sessions. Ideally security experts from national government agencies should also be involved in any further validation of RAMST, because they are directly concerned with the practice.

Finally it would be an interesting option for further research to assess to what extent RAMST is actually useful as a practical risk analysis tool (e.g. in order to carry out IT audits) by actively employing it in practice.

# Bibliography


[ACIB1998] Advies- en Coordinatiepunt InformatieBeveiliging: *Handboek A&K-analyse*. Ministerie van Binnenlandse Zaken, 1998.

[BARU2001] Baruch, Y.: 'The status of research on teleworking and an agenda for future research', in: *International Journal of Management Reviews*, Volume 3, Issue 2 (2001), pp. 113-129.

[BIZA1994] Ministerie van Binnenlandse Zaken: *Besluit voorschrift informatiebeveiliging rijksdienst 1994*. Den Haag, Ministerie van Binnenlandse Zaken, 1994.

[BROU1996] Brouwer, A.: 'De kracht van de kwalitatieve analyse', in: *De EDP-Auditor*, Number 2 (1996), pp. 9-14.

[BRUI1994] Bruijn de, A. and W. van de Garde: 'Besluit Voorschrift Informatiebeveiliging rijksdienst 1994', in: *De EDP-Auditor*, January 1995 pp. 13-20.

[BRUI2004] Bruijn de, R.: 'Citrix-omgeving nader bekeken', in: *De EDP-Auditor*, Number 1 (2004) pp. 20-28.

[BZK1999] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties: *Beveiligde E-mail voor de Rijksoverheid / Communiceren in vertrouwen*. Den Haag, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 1999.

[BZK2001] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties: *Raamregeling Telewerken*. Den Haag, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2001.

[BZK2004] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties: *Besluit voorschrift informatiebeveiliging rijksdienst – bijzondere informatie*. Den Haag, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2004.

[DENB2000] Denbigh, A.: *The teleworking handbook / written on behalf of the Telework Association by Alan Denbigh*. London, Black, 2000.

[ECAT2000] ECaTT: *Benchmarking progress on new ways of working and new forms of business across Europe*. Bonn, Empirica, 2000.

[ELSE2005] Elsevier (December 8, 2005): *Woede over kwijtraken AIVD-diskettes*. Available online via http://www.elsevier.nl/nieuws/nederland/nieuwsbericht/asp/artnr/77062/index.html Accessed on September 27, 2006.

[ELSE2006a] Elsevier (February 8, 2006): *Remkes: Weer politie-informatie op straat*. Available online via http://www.elsevier.nl/nieuws/nederland/nieuwsbericht/asp/artnr/85922/index.html. Accessed on April 3, 2006.

[ELSE2006b] Elsevier (April 1, 2006): *Documenten Koninklijk Huis op straat*. Available online via http://www.elsevier.nl/nieuws/nederland/artikel/asp/artnr/93019/index.html. Accessed on April 1, 2006.

[EUCO2003] European Commission: *Collaboration@Work / The 2003 report on new working environments and practices*. Brussels, European Commission, 2003.

[EUCO2005] European Commission: *Collaboration@Work / The 2005 Report on new working environments and practices*. Brussels, European Commission, 2005.

[EXPE2002] Stichting Het Expertise Centrum: *Informatiebeveiliging voor de overheid / Een praktische aanpak*. Den Haag, Stichting Het Expertise Centrum.

[GORG2005] Gorge, M.: 'USB & other portable storage device usage / Be aware of the risks to your corporate data in order to take pre-emptive and/or corrective action', in: *Computer Fraud & Security*, August 2005, pp. 15-17.

[GREE2002] Green, C.: 'Laptop security threats / Increasing theft stats encourage road warriors to play it safe with portable tech', in: *CMA Management*, July/August 2002, pp. 46-47.

[HADD2005] Haddon, L. and M. Brynin: 'The character of telework and the characteristics of teleworkers', in: *New Technology, Work and Employment*, Volume 20, Issue 1 (2005), pp. 34-46.

[HARP2002] Harpaz, I.: 'Advantages and disadvantages of telecommuting for the individual, the organization and society', in: *Work Study*, Volume 51, Number 2 (2002), pp. 74-80.

[ISF1997a] Information Security Forum: *SPRINT User Guide*. Information Security Forum, 1997.

[ISF1997b] Information Security Forum: *SPRINT Directory of Controls*. Information Security Forum, 1997.

[ISF1999] Information Security Forum: *Securing Remote Access by Staff / Directory of Risks and Controls*. Information Security Forum, 1999.

[ISF2002] Information Security Forum: *Securing PDAs / A Practical Approach*. Information Security Forum, 2002.

[ISF2003] Information Security Forum: *Using E-mail / Detailed Risks and Controls*. Information Security Forum, 2003.

[ISO2005] ISO/IEC: *Information technology – Security techniques – Code of practice for information security management*. ISO/IEC, 2005.

[JACO2000] Jacobs, C.W.J.M. and G.J.M. Janssen: *Óverheid en informatie / Werkprocessen en informatiestromen in de overheid*. Utrecht, Uitgeverij LEMMA BV, 2000.

[KURL1999] Kurland, N.B. and Bailey D.E.: 'Telework: The Advantages and Challenges of Working Here, There, Anywhere, and Anytime', in: *Organizational Dynamics*, autumn 1999, pp. 53-67.

[LIBB2004] Libbenga, J. (October 13, 2004): *Prosecutor resigns over hacked PC*. Available online via http://www.theregister.co.uk/2004/10/13/dutch_prosecutor_hacked. Accessed on June 12, 2006.

[MARO2001] Marot, J.C.: *EU-CIS Teleworking 2001*. Moscow, UIPE RAS, 2001.

[MEAR2006] Mearian, L.: 'Portable Storage Devices Pose IT Security Risk', in: *Computerworld*, Volume 40, Number 13, pp. 1 and 57.

[MORG2004] Morgan, R.E.: 'Teleworking: an assessment of the benefits and challenges', in: *European Business Review*, Volume 16, Number 4 (2004), pp. 344-357.

[NUNL2006] NU.NL (February 1, 2006): *Geheime informatie Defensie weer op straat*. Available online via http://www.nu.nl/news.jsp?n=666632&c=13. Accessed on June 13, 2006.

[OVER2000] Overbeek, P., E. Roos Lindgreen and M. Spruit: *Informatiebeveiliging onder controle*. Pearson Education Uitgeverij BV, 2000.

[PÉRE2005] Pérez, M.P., A.M. Sánches, P.L. Carnicer and J.V. Jiménez: 'Knowledge tasks and teleworking: a taxonomy model of feasibility adoption', in: *Journal of Knowledge Management*, Volume 6, Number 3 (2002), pp. 272-284.

[PHIF2003] Phifer, L.: 'Securing Teleworker Networks', in: *Business Communications Review*, October 2003, pp. 28-35.

[PLAN2006] Planet Internet (February 2, 2006): *Weer geheimen Defensie op straat*. Available online via http://www.planet.nl/planet/show/id=62967/contentid=678519/sc=99e55e. Accessed on June 13, 2006.

[POTT2004] Potter, B.: 'Securing the mobile device', in: *Network Security*, Volume 2004, Issue 2 (2004), pp. 4-5.

[PSTN2003] Professional Security Training Network: *Laptop theft prevention*. Professional Security Training Network, 2003.

[PYÖR2003] Pyöriä, P.: 'Knowledge work in distributed environments: issues and illusions', in: *New Technology, Work and Employment*, Volume 18, Issue 3 (2003), pp. 166-180.

[SIBI2003] SIBIS: *SIBIS Pocket Book 2002/03 / Measuring the Information Society in the EU, the EU Accession Countries, Switzerland and the US*. Bonn, Empirica, 2003.

[SULL2003] Sullivan, C.: 'What's in a name? Definitions and conceptualisations of teleworking and homeworking', in: *New Technology, Work and Employment*, Volume 18, Issue 3 (2003), pp. 158-165.

[SWS2004] SearchWebServices: *ICT*. Available online via http://searchwebservices.techtarget.com/gDefinition/0,294236,sid26_gci928405,00.html. Accessed on June 1, 2006.

[SYMA2005] Symantec: 'Security tips for laptop owners', in: *NZB*, July 2005, pp. 47-48.

[VNUN2004] VNUNET.NL: *CBI: beveiliging mobiele werkplekken ondermaats*. Available online via http://www.vnunet.nl/nieuws.jsp?id=376295. Accessed on June 16, 2006.

[VRIE2002] Vries de, A.: *De risicoanalyse voorbij / informatiebeveiliging door standaardisatie*. Master thesis Management van Informatietechnologie, Open Universiteit Nederland, 2002.

# Glossary

| | |
|---|---|
| ActiveX control | A software component that is used to add interactivity and more functionality, such as animation or a popup menu, to a Web page. An ActiveX control can be written in any of a number of languages, including Java, C++, and Visual Basic. http://www.microsoft.com/technet/prodtechnol/visio/visio2002/plan/glossary.mspx#ELC |
| Anti-malware software | Computer programs that attempt to identify, thwart and eliminate malware.<br><br>Anti-malware software typically uses two different techniques to accomplish this:<br>• Examining (scanning) files to look for known malware matching definitions in a malware dictionary<br>• Identifying suspicious behavior from any computer program which might indicate infection. Such analysis may include data captures, port monitoring and other methods.<br><br>Most commercial anti-malware software uses both of these approaches, with an emphasis on the virus dictionary approach. http://en.wikipedia.org/wiki/Anti_virus-software |
| Authentication | Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. http://www.myidpa.com/MediHelp/Glossary/B.htm |
| Authentication token | A portable device used for authenticating a user. Authentication tokens operate by challenge/response, time-based code sequences, or other techniques. This may include paper-based lists of one-time passwords. http://www.atharmahboob.com/courses/security/glossary/glossary-firewall.htm |
| Availability | The extent in which an information system is in operation at the moment the organization needs it. [BIZA1994] |
| Basic Input/Output System (BIOS) | Software code run by a computer when first powered on. The primary function of BIOS is to prepare the machine so other software programs stored on various media (such as hard drives, floppies, and CDs) can load, execute, and assume control of the computer. This process is known as booting up. http://en.wikipedia.org/wiki/BIOS |

| | |
|---|---|
| Brute force attack | A method of defeating a cryptographic scheme by trying a large number of possibilities; for example, exhaustively working through all possible keys in order to decrypt a message. In most schemes, the theoretical possibility of a brute force attack is recognized, but it is set up in such a way that it would be computationally infeasible to carry out. http://en.wikipedia.org/wiki/Brute_force_attack |
| Communication protocol | The rules governing the exchange of information between devices on a data link. http://www.tyner.com/glossary.htm |
| Communication software | A piece of software that establishes a connection between a computer and a server (e.g. ICA client , Java plug-in etc.). |
| Computer virus | A self-replicating computer program written to alter the way a computer operates, without the permission or knowledge of the user. http://en.wikipedia.org/wiki/Computer_virus |
| Confidentiality | The extent in which access to and inspection of an information system and the information it contains is restricted to a defined group of authorized persons. [BIZA1994] |
| Cryptographic key | A value which is used to control a cryptographic process, such as, encryption or authentication. Knowledge of an appropriate key allows correct decryption or validation of a message. http://www.maithean.com/products/glossary.html |
| Data | A representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automated means. http://sam.dgs.ca.gov/TOC/4800/4819.2.htm |
| Denial of Service (DoS) attack | An attack on a computer system or network that causes a loss of service to users, typically the loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computational resources of the victim system. http://en.wikipedia.org/wiki/Denial_of_service_attack |
| Dictionary attack | A technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by searching a large number of possibilities. In contrast with a brute force attack, where all possibilities are searched through exhaustively, a dictionary attack only tries possibilities which are most likely to succeed, typically derived from a list of words in a dictionary. http://en.wikipedia.org/wiki/Dictionary_attack |

| | |
|---|---|
| Email client | An application used to send, receive and view e-mail. Some common examples include Outlook, Outlook Express, and Netscape Messenger.<br>http://studentcomputing.usask.ca/glossary.htm |
| Encryption | The process of obscuring information to make it unreadable without special knowledge.<br>http://en.wikipedia.org/wiki/Encryption |
| File sharing | The practice of making files available for other users to download over the Internet and smaller networks. Usually file sharing follows the peer-to-peer (P2P) model, where the files are stored on and served by personal computers of the users. Popular file sharing programs are Kazaa, Audiogalaxy, WinMX and Limewire.<br>http://en.wikipedia.org/wiki/File_sharing |
| Firewall | A piece of hardware and/or software which functions in a networked environment to prevent some communications forbidden by the security policy, analogous to the function of firewalls in building construction.<br>http://en.wikipedia.org/wiki/Firewall_%28networking%29 |
| Guideline | A written statement or outline of a policy, practice or conduct. Guidelines may propose options to enable a user to satisfy provisions of a code, standard, regulation or recommendation.<br>http://www.steelbuildingsindustry.com/dictionary-g.htm |
| Information | Data that has been processed to add or create meaning and hopefully knowledge for the person who receives it. Information is the output of information systems.<br>http://dssresources.com/glossary/dssglossary1999.html |
| Information and communication technology (ICT) | The technology to gather, record and store, process, transport and/or provide data (information), including the knowledge about the appliance of that technology. [JACO2000] |
| Information security | Implementing and maintaining a coherent set of security controls in order to safeguard the confidentiality, integrity and availability of an information system and with that of the information therein. [BIZA1994] |
| Information system | A coherent data processing functionality that can be deployed to know, support or control one or more business processes. An information system can contain the following components: hardware, software, data, procedures and people. [OVER2000] |

| | |
|---|---|
| Instant messaging | Instant Messaging is a form of electronic communication which involves immediate correspondence between two or more users who are all online simultaneously. Popular IM programs include AOL's Instant Messenger (AIM), AOL's ICQ, Microsoft's MSN Messenger and Yahoo!<br>http://www.krollontrack.com/legalresources/glossary.aspx |
| Integrity | The extent in which an information system is errorless. [BIZA1994] |
| Internet | The publicly available worldwide system of interconnected computer networks that transmit data by packet switching using a standardized Internet Protocol (IP) and many other protocols.<br>http://en.wikipedia.org/wiki/Internet |
| Internet access device | A piece of hardware that is capable to connect a computer to the Internet (e.g. modems, wireless routers etc.). |
| Internet access provider | An organization (or person) that offers private persons or companies the facilities to enable a computer to make a connection with the Internet.<br>http://nl.wikipedia.org/wiki/Internetprovider |
| Intrusion detection system | A system which detects all types of malicious network traffic and computer usage that cannot be detected by a conventional firewall. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malware (viruses, Trojan horses, and worms).<br>http://en.wikipedia.org/wiki/Intrusion_detection_system |
| Java applet | A mini software program that a Java or ActiveX enabled browser downloads and uses automatically. It can add sophisticated support for Web pages, far beyond programming such as DHTML or Javascript.<br>http://www.netproject.com/docs/migoss/v1.0/glossary.html |
| Key logger | A small program designed to record which keys are pressed on a computer keyboard. Most commonly used to record passwords for later use by another person.<br>www.network-security.adopto-computers.com/glossary.html |
| Local Area Network (LAN) | A computer network covering a small local area, like a home, office, or small group of buildings. Current LANs are most likely to be based on switched Ethernet or Wi-Fi technology.<br>http://en.wikipedia.org/wiki/Local_area_network |
| Logical access control | A protection mechanism that limit users' access to information and restrict their forms of access on the system to only what is appropriate for them.<br>http://www.totse.com/en/privacy/encryption/hk_acces.html |
| Malware | Any software program developed for the purpose of causing harm to a computer system, similar to a virus or Trojan horse. |

| | |
|---|---|
| | Traditional examples of malware include viruses, worms, Trojan Horses, and attack scripts, while more modern examples include Java attack applets and dangerous ActiveX controls.<br>http://en.wikipedia.org/wiki/Malware |
| Motherboard | The main circuit board of a computer, which houses all the vital components usually including the microprocessor, internal memory, and device controllers such as for the disk drives.<br>http://www.techwriter.co.nz/nerd-im.html |
| Operating system | A software program that manages the hardware and software resources of a computer. The operating system performs basic tasks, such as controlling and allocating memory, prioritizing the processing of instructions, controlling input and output devices, facilitating networking, and managing files. (…) Examples of operating systems for personal computers include Microsoft Windows, Mac OS (and Darwin), Unix, and Linux.<br>http://en.wikipedia.org/wiki/Operating_system |
| Peripheral equipment | A type of computer hardware that is added to a host computer in order to expand its abilities. More specifically the term is used to describe those devices that are optional in nature, as opposed to hardware that is either demanded, or always required in principle. (…) Typical examples include joysticks, printers and scanners.<br>http://en.wikipedia.org/wiki/Peripherals |
| Personal Digital Assistant (PDA) | Any small mobile hand held device that provides computing and information storage retrieval capabilities for personal or business use, often for keeping schedule calendars and address book information handy.<br>http://www.auditmypc.com/acronym/PDA.asp |
| Personal firewall | Software installed on an end-user's PC which controls communications to and from the user's PC, permitting or denying communications based on a security policy.<br>http://en.wikipedia.org/wiki/Personal_firewall |
| Pre-boot authentication | A logon function that requires the user who is attempting to logon to authenticate himself before the boot process.<br>http://americas.utimaco.com/safeguard_easy/manual/1-078.html |
| Risk analysis | A process for understanding risks and determining what measures need to be taken to control them [ISF1997] |
| Security breach | A loss of the quality of an object arising from the manifestation of a security threat. |
| Security control | A policy, method, procedure, device or programmed mechanism which protects quality of an object from one or more threats. |
| Security policy | The set of rules, principles, and practices that determine how security is implemented in an organization.<br>http://slis-two.lis.fsu.edu/~security/SecurityGlossary2.html |

| | |
|---|---|
| Security risk | A function of the magnitude of possible damage which would arise as a result of a security breach and the likelihood of harm being suffered. [VRIE2002] |
| Security threat | An event or process which could compromise quality of an object. [OVER2000] |
| Social engineering | The practice of obtaining confidential information by manipulation of legitimate users. A social engineer will commonly use the telephone or Internet to trick people into revealing sensitive information or getting them to do something that is against typical policies. By this method, social engineers exploit the natural tendency of a person to trust his or her word, rather than exploiting computer security holes. http://en.wikipedia.org/wiki/Social_engineering_(computer_security |
| Teleworking | Working independent of time and place (with the help of information and communication technology). |
| Trojan horse | An apparently useful and innocent program containing additional hidden code which allows the unauthorized collection, exploitation, falsification, or destruction of data. www.tsl.state.tx.us/ld/pubs/compsecurity/glossary.html |
| Vulnerability | The extent in which an object is susceptible to a threat. [OVER2000] |
| Web browser | A software application that enables a user to display and interact with HTML documents hosted by web servers or held in a file system. Popular browsers available for personal computers include Microsoft Internet Explorer, Mozilla Firefox, Opera, and Safari. http://en.wikipedia.org/wiki/Web_browser |
| Wide Area Network (WAN) | A geographically dispersed telecommunications network. The term distinguishes a broader telecommunication structure from a local area network. A wide area network may be privately owned or rented, but the term usually connotes the inclusion of public (shared user) networks. An example of a WAN is the Internet. http://www.bytepile.com/definitions-w.php |

# Overview appendices

# Appendix A: Questionnaire

This appendix contains the questionnaire that was used for the interviews with security experts at the agencies in our field survey (see chapter 4). Since the interviews were held in Dutch, the questionnaire is also in Dutch.

---

## Informatiebeveiliging bij Telewerken door Rijksambtenaren

**Erasmus Universiteit Rotterdam / PricewaterhouseCoopers**

**Vragenlijst interview met … van XXX**

Dit interview is bedoeld om in kaart te brengen hoe er bij **XXX** vanuit het oogpunt van informatiebeveiliging, omgegaan wordt met telewerken. De resultaten van dit interview worden gebruikt voor een kwalitatieve analyse van de huidige stand van zaken ten aanzien van informatiebeveiliging bij telewerken binnen de rijksoverheid.

Het aldus verkregen beeld zal aan de basis liggen van een te ontwikkelen model (c.q. normenkader) dat tot doel heeft adequate beveiliging bij telewerken door rijksambtenaren te realiseren.

**Doelen van het interview:**

1. Bepalen wat onder telewerken verstaan wordt, waarom telewerken plaatsvindt en hoeveel er getelewerkt wordt.
2. Identificeren van de verschillende 'vormen van telewerken' (c.q. telewerktypologieën of telewerkvoorzieningen) binnen **XXX**.
3. Inventariseren hoe er in het kader van telewerken omgegaan wordt met informatiebeveiliging en achterhalen op welke gronden beveiligingsmaatregelen gekozen zijn.

**Doel 1**

1. Wat wordt er bij **XXX** onder telewerken verstaan?
    a. *Welke plaats heeft het gebruik van ICT hierin?*
2. Waarom wordt er binnen **XXX** getelewerkt? Welke afwegingen liggen ten grondslag aan het besluit om telewerken mogelijk te maken?
    a. *Welke voor- en nadelen worden ten aanzien van telewerken onderkend?*
    b. *Welke rol speelt informatiebeveiliging hierbij?*
3. Vindt telewerken plaats op initiatief van de werkgever of op initiatief van de werknemer?
    a. *Vindt telewerken plaats op vrijwillige basis?*
4. Hoeveel telewerkers zijn er en hoe vaak telewerken zij?
5. Welke functies komen voor telewerken in aanmerking (*en welke functies niet*)?

6. Met welke soorten informatie werken telewerkers? (bijvoorbeeld persoonsgegevens (WBP), bijzondere informatie (VIRBI) of overige informatie (VIR))
    a. *Is er informatie waarmee in geen geval getelewerkt mag worden? (maatregel)*
    b. *Worden er bij telewerken extra beperkingen opgelegd met betrekking tot toegang tot informatie en functionaliteit (t.o.v. werken op kantoor)? (maatregel)*
    c. *Welke rol speelt wet- en regelgeving hierbij?*
7. Wat zijn de toekomstverwachtingen ten aanzien van telewerken?
    a. *Met betrekking tot het aantal telewerkers.*
    b. *Met betrekking tot de functies die voor telewerken in aanmerking komen.*

**Doel 2**

1. Vanuit welke locatie(s) wordt er getelewerkt? (bijvoorbeeld vanuit huis, vanuit een satellietkantoor of geen vaste locatie)
2. Is er een beperking opgelegd ten aanzien van de tijdstippen waarop kan worden getelewerkt (c.q. van de telewerkvoorzieningen gebruik kan worden gemaakt)?
3. Met welke middelen (hard- en software) werken telewerkers?
    a. *Mogen deze middelen ook voor privé doeleinden gebruikt worden, of zijn ze uitsluitend voor 'het werk' bedoeld? (maatregel)*
        i. *In hoeverre worden deze middelen door de werkgever verstrekt?*
    b. *Wordt de telewerker beperkingen opgelegd ten aanzien van het gebruik van hard- en software en zo ja, wat zijn die beperkingen? (maatregel)*
    c. *Wat zijn de toekomstverwachtingen ten aanzien van de gebruikte hard- en software?*
4. Op welke wijze(n) vindt communicatie plaats tussen de telewerker en de organisatie.
    a. *Indien er sprake is van een elektronische verbinding tussen de organisatie en de telewerker:*
        i. *Welke protocollen worden gebruikt? (bijvoorbeeld het Internet protocol)*
        ii. *Welke applicaties worden gebruikt? (bijvoorbeeld het web, email of teleconferencing)*
        iii. *Welke technologieën worden gebruikt? (bijvoorbeeld ISDN, kabel of wireless)*
        iv. *In hoeverre is bekend hoe de infrastructuur aan de client zijde (d.w.z. bij de telewerker) is ingericht? (maatregel)*

   b. *Mag de telewerker uitsluitend een elektronische verbinding met de organisatie aangaan of ook met andere (mogelijk onbetrouwbare) partijen? (bijvoorbeeld door vrijelijk gebruik te maken van het Internet) (maatregel)*

5. Op welke locatie(s) wordt informatie opgeslagen? (bijvoorbeeld alleen centraal (d.w.z. op de server), alleen lokaal (d.w.z. op gegevensdragers bij de telewerker) of zowel centraal als lokaal) *(maatregel)*
6. Voor zover dat nog niet uit de antwoorden op bovenstaande vragen blijkt: Hoe ziet het technische ontwerp van de telewerkarchitectuur eruit?

**Doel 3**

1. Welke bedreigingen op het gebied van informatiebeveiliging brengt telewerken met zich mee?
   a. *In hoeverre zijn de bedreigingen en bijbehorende risico's afhankelijk van de verschillende telewerkvormen, zoals hierboven geïdentificeerd?*
2. Welke maatregelen (zowel organisatorisch, logisch als fysiek) zijn genomen om informatiebeveiliging bij telewerken te realiseren? *(een deel van deze maatregelen is mogelijk hierboven al geïdentificeerd)*
3. Hoe zijn deze maatregelen gekozen?
   a. *Worden uitgebreide risicoanalyses (A&K-analyses) ten aanzien van telewerken uitgevoerd?*
      i. *Zijn er betrouwbaarheidseisen aan (de verschillende vormen van) telewerken gesteld?*

      *Welke rol speelt de informatie waarmee de telewerker werkt hierbij?*

      ii. *Is er getoetst of de genomen beveiligingsmaatregelen (zie vraag 2) voldoen aan de gestelde betrouwbaarheidseisen m.a.w. of ze een voldoende hoog beveiligingsniveau realiseren?*
   b. *Is er gebruik gemaakt van standaarden of andere 'best practices'?*
4. Wie zijn verantwoordelijk voor het treffen en onderhouden van beveiligings-maatregelen bij telewerken?
   a. *In hoeverre is de telewerker zelf verantwoordelijk?*
5. Is er een informatiebeveiligingsbeleid en/of –plan voor telewerken opgesteld?

# Appendix B: Dependency and Vulnerability Analysis

In this appendix a summary of the Dependency and Vulnerability analysis (D&V-analysis) as described in the Guidebook D&V-analysis '*Handboek A&K-analyse*' [ACIB1998] is given. This summary is adopted from the article '*De kracht van de kwalitatieve analyse*' by Albert Brouwer [BROU1996].

## B.1 Introduction

A D&V-analysis starts with the common quality requirements and existing security controls which are laid down in the security policy. The result of the dependency analysis is a set of quality requirements. These quality requirements indicate to what extent the availability, confidentiality and integrity is desired. The quality requirements are established from the perspective of management and therefore expressed in management terminology. In addition to this an indication of the consequences of an inability to meet the quality requirements is given.

Starting from these quality requirements, relevant threats and associated incidents are identified in the vulnerability analysis. On this basis, information security controls are identified. Hereto a check between the proposed security controls and their effect in relation to the quality requirements is performed. The identified security controls are laid down in an information security plan. The positioning of the dependency and vulnerability analysis is depicted in the figure below.

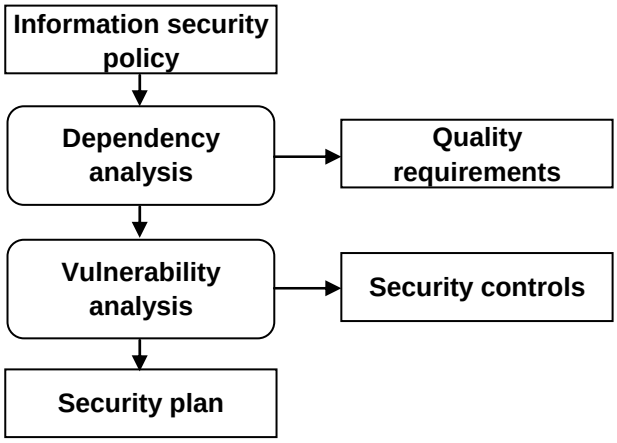


**Figure B.1: Coherence**

## B.2 Dependency analysis

The definition of dependency analysis can be unraveled as follows:

- to determine to what extent business processes;
- that are supported by information systems;
- depend on the quality of these systems;
- and to determine the potential damages in case these systems fail.

The dependencies between business processes, information systems and supporting services are depicted the figure below as a ‘chain of dependencies’.

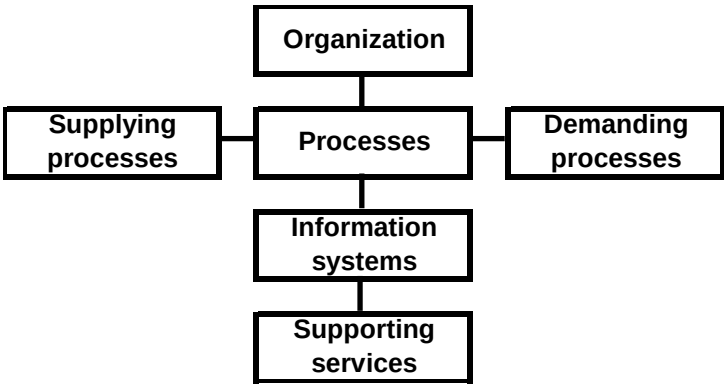


**Figure B.2: Chain of dependencies**

In relation to this definition and the depicted chain of dependencies the following steps can be distinguished in the process of performing a dependency analysis:

1. Analyse the business process(es) (possibly: business activities) to be reviewed.
2. Identify and analyse the associated information systems (possibly information system functions).
3. Determine the relations between the business process(es) or activities and the information system (functions).
4. Formulate the quality requirements in terms of availability, confidentiality and integrity.

*Ad 1*. In order to identify and analyse business processes it is essential to gain insight in rules and regulations, the way the process functions, which requirements the organization puts on the process etc. Furthermore it is important to consider the requirements that stem from the supplying and demanding processes. Supplying processes especially put requirements on the exclusiveness. Demanding processes put requirements on the availability, confidentiality as well as the integrity of products that stem from the business process under review. This is because the proper working of demanding processes depends on the quality of these products. An important component of the analysis is the question what requirements the ‘market’ (internal and external) puts on these products.

Hence in the analysis phase both factors that stem from the environment of the business process and internal factors that may have an influence on the quality requirements are assessed. Hereby questions like ‘what are the consequences for the business process if…? are considered. In other words: what are the consequences – in case (parts of) the business process no longer function in conform the requirements – for the customer, the legislator, the organization etc.

*Ad 2.* Subsequently the information systems associated with the business process under review have to be identified and analyzed. This step investigates which information systems contribute to the proper functioning of the business process. Because information systems can usually be divided into various functionalities, it may be necessary to distinguish different information system functions. The usual pattern is: collect input, mutate, process, make (parts of) databases available and produce output in primary and secondary forms. For many information systems a form of secondary output is management information.

*Ad 3.* In order to translate the quality requirements that result from the dependency analysis into security controls, it is necessary to relate the various information systems or information system functions to the relevant business functions. This step is necessary to connect the requirements that are put on the business processes to the relevant information systems or information system functions.

*Ad 4.* After performing the previous three steps it is possible to indicate per information system (function) what the quality requirements in terms of availability, confidentiality and integrity are. It is important to precisely formulate why these requirements are chosen and what the consequences are in case the requirements are not met. Since the requirements lie at the basis of the vulnerability analysis, they have to be formalized by the responsible line management.

## B.3 Vulnerability analysis

It follows from the dependency analysis which requirements are put on the reliable functioning of the information provision. The vulnerability analysis subsequently investigates to what extent the information provision is vulnerable in relation to the established requirements.

The vulnerability analysis consists of the following steps:

1. Identify the information security controls that are already in place.
2. Identify and analyse relevant threats.
3. Determine which controls need to be implemented.
4. Clean-up and replenish existing collections of controls.

These steps are depicted in the figure below:

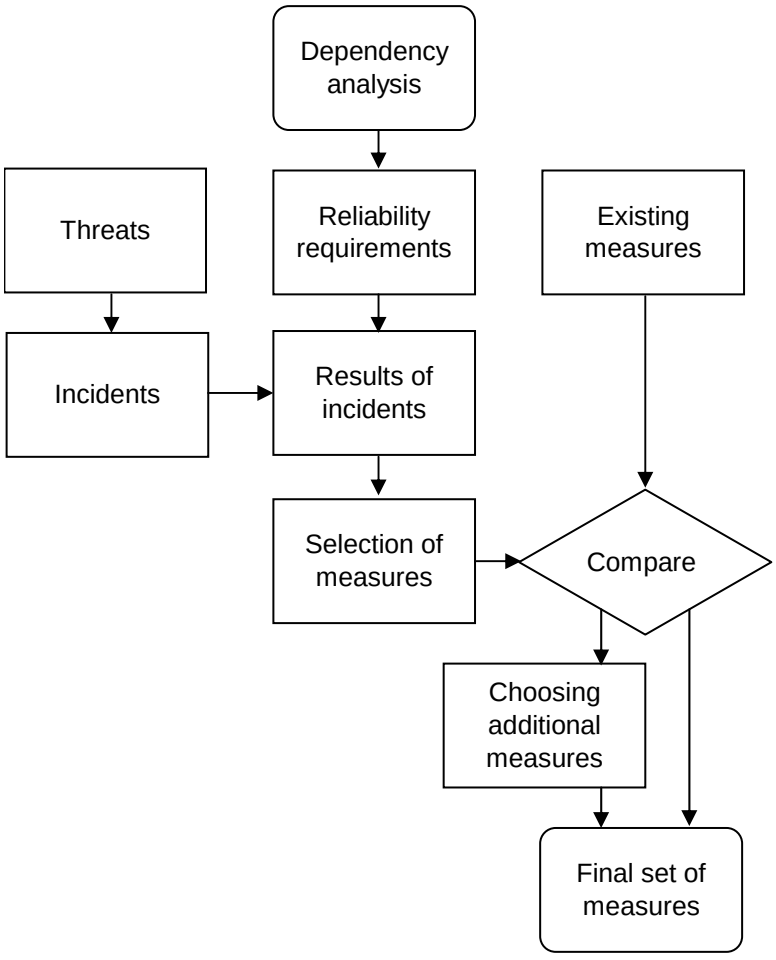


**Figure B.3: Vulnerability analysis**

*Ad 1.* In this phase of the vulnerability analysis an investigation takes place of the information security controls that are already in place. This concerns both general controls and controls that specifically apply to the information system in question. This is the *ist*-position.

During this investigation the limits of various responsibility areas are frequently overstepped. After all: information security concerns the whole of security controls in the area of the security of buildings, physical access, but also in the area of human resource management, computer centres, local area networks etcetera. Therefore it is important to clarify the boundaries of the investigation.

The description of existing security controls is necessary in order to determine which additional controls are necessary and where existing controls need to be reinforced or might be abolished.

*Ad 2.* In order to identify the relevant threats it is necessary that management has explicitly expressed the consequences of an inability to meet the quality requirements during the dependency analysis. Moreover it is important to know which threats are excluded by the organization's policy. Many organizations for example, do not take nuclear conflicts, acts of war and terrorism into account. Local situations require attention for other threats such as flooding, adjoining industries etcetera.

Almost all components of the information provision (LAN, WAN, work places, mainframe) consist of: people, apparatus, software, organization and environment and/or services (of internal or external third parties). For all these components variants of the following basic incidents can take place: temporarily absent, continuously absent or present but improperly functioning. These basic incidents can be caused by numerous threats. In this stadium of the investigation, these threats are not yet relevant, because the influence of these incidents on the established quality requirements needs to be determined first.

Therefore for every component and for every basic incident the consequences of that incident for the realization of the established quality requirements are determined. In this stadium the dependency and vulnerability analysis are connected. An insight is gained into which incidents need to be avoided. Subsequently it needs to be determined which threats may cause these incidents.

*Ad 3.* In case the impact of basic incidents on the quality requirements is too big, security controls need to be implemented against the threats that may cause the basic incidents concerned. These controls constitute the *soll*-position. The responsible management should assess if the impact of a basic incident on the quality requirements is too big.

*Ad 4.* The difference between the *ist*-postion (security controls already in place) and the *soll*-position (required security controls) indicates which security controls need to be implemented, which existing controls need to be adjusted or which existing security controls can be abolished.

# Appendix C: RAMST

In this appendix the steps required to complete the four phases of the Risk Analysis Methodology for Securing Teleworking (RAMST) are described. RAMST is a tool that can be used by national government agencies to assess the security risks associated with teleworking and to identify the security controls required to keep the risks within acceptable limits.

The security risks covered by RAMST primarily involve those risks that (1) have a direct impact on the confidentiality, integrity and availability of information and (2) are associated with two telework typologies (T1 and T2).

RAMST consists of the following four phases that should be successively completed:

| | |
|---|---|
| **Phase 1** | **Set the scene**<br>In this phase a review group is established and the scope of the risk analysis is determined. The latter is done by choosing a telework typology and by determining which information is used by teleworkers. |
| **Phase 2** | **Assess business risks**<br>In this phase telework information is classified in terms of its importance to the agency and hence the level of protection needed.<br><br>For this purpose the following appendices are relevant:<br>• Appendix D: Impact Assessment Form – Confidentiality<br>• Appendix E: Impact Assessment Form – Integrity<br>• Appendix F: Impact Assessment Form – Availability<br>• Appendix G: Impact Assessment Form – Summary |
| **Phase 3** | **Assess threats, vulnerabilities and controls**<br>In this phase the key threats and vulnerabilities associated with the chosen telework typology are determined as well as the controls required to keep the risks within acceptable limits.<br><br>For this purpose the following appendices are relevant:<br>• Appendix I: Threats, Vulnerabilities and Controls Assessment Form<br>• Appendix J: Directory of Threats<br>• Appendix K: Directory of Controls<br>• Appendix L: Threat/control matrix |
| **Phase 4** | **Produce agreed action plan**<br>In this phase a plan of action for implementing controls is agreed.<br><br>For this purpose the following appendix is relevant:<br>• Appendix H: Action Plan Form |

## Phase 1: Set the scene

### Objectives

Phase 1 consists of three steps and has the following objectives:

- To establish a review group that will conduct the risk analysis.
- To determine the scope of the risk analysis.

### Step 1: Establish a review group

Establish a review group that will conduct the risk analysis. This review group should consist of at least one coordinator and a line manager who is responsible for the telework service.

Coordinators should have the stature and inter-personal skills needed to work closely with management, the ability to work in a well organised, disciplined manner and a good working knowledge of information security. Coordinators may for example be information security specialists or internal auditors.

### Step 2: Determine the scope of the risk analysis

The scope of the risk analysis is determined by choosing a telework typology (step 1) and by identifying which information is available to teleworkers (step 2).

*Task 1.1:*
Determine which information will most likely be used by the teleworkers under review. Such information is subsequently called “telework information”.

*Task 1.2:*
Determine the telework typology – T1 or T2 – for which the risk analysis will be conducted.

| | |
|---|---|
| **T1** | Teleworking with a ‘stand-alone’ telework computer*. Information is **stored** and **processed locally**. |

| | |
|---|---|
| **T2** | Teleworking with a telework computer that is connected to the remote access farm** by means of a (Citrix) server based computing architecture. Information is **stored** and **processed centrally**.<br><br>Only user interfaces, keystrokes and mouse clicks are communicated between the telework computer and the remote access farm. Communication takes place over the Internet. The telework computer only generates application screens. |

* A telework computer is a computing device used for teleworking. A telework computer supplied by an agency is usually a laptop. A telework computer not supplied by an agency can theoretically be any device that satisfies technical requirements for teleworking (e.g. in order to run certain applications or establish an Internet connection), but is usually a privately owned desktop computer.
** The remote access farm is a collection of computer servers, typically housed inside the agency’s buildings, that facilitates remote access to certain applications in behalf of teleworkers.

## Phase 2: Assess business risks

**Objectives**
Phase 2 consists of four steps and has the following objectives:

- To assess the 'business' risk associated with teleworking by evaluating the consequences and impact of a loss of the confidentiality, integrity and availability of telework information.
- To determine the maximum severity of a loss of the confidentiality, integrity and availability of telework information.
- To classify telework information in terms of its importance to the agency and hence the level of protection needed.

**Step 1: Assess impact – Confidentiality**
The consequences and impact of a loss of the confidentiality of telework information are assessed by subsequently carrying out the five tasks below.

*Task 1*
Ask the line manager to consider the consequences of unauthorized or unintended disclosure of telework information (i.e. loss of confidentiality).

*Task 2*
Use the 'Confidentiality' page of the 'Impact Assessment Form' (appendix A) to:

- Focus attention on the different types of consequences which may arise
- Record the results of the discussion.

*Task 3*
Ask the line manager to rate, on a worst case basis, the damage which would arise on an A to D scale for each of the categories of consequence referred to on the form, using the following ratings:

| *Rating* | *Significance* |
|---|---|
| A | Serious Damage |
| B | Significant Damage |
| C | Minor Impact |
| D | Negligible |

*Task 4*
For ratings of A and B, ask the line manager to explain how a loss of confidentiality would be damaging to the agency and identify the particular:

- Types of telework information involved (e.g. financial data, rubricaded data).
- Persons to whom disclosure would be damaging (e.g. to the media or to employees).

*Task 5*
Decide on an overall rating for confidentiality, by considering, on a worst case basis, what damage could be caused by a loss of confidentiality.

**Step 2: Assess impact – Integrity**
The consequences and impact of a loss of the integrity of telework information are assessed by subsequently carrying out the five tasks below.

*Task 1:*
Ask the line manager to consider the consequences of a loss of integrity of telework information arising from:

- Accidental corruption of telework information (e.g. by error or mishap)
- Deliberate manipulation of telework information (e.g. by malicious act or to perpetrate or conceal fraud).

*Task 2:*
Use the 'Integrity' page of the 'Impact Assessment Form' (appendix B) to:

- Focus attention on the consequences of a loss of integrity
- Record the results of the discussion.

*Task 3:*
Ask the line manager to rate, on a worst case basis, the damage which would arise on an A to D scale for each consequence referred to on the form, using the following ratings:

| *Rating* | *Significance* |
|---|---|
| A | Serious Damage |
| B | Significant Damage |
| C | Minor Impact |
| D | Negligible |

*Task 4:*
For ratings of A or B, ask the line manager to describe how the integrity breach would be damaging to the agency and identify the particular:

- Types of telework information involved (e.g. customer balances, payment details)
- The nature of the manipulation or error (e.g. error resulting in overpayment, error in calculation).

*Task 5:*
Decide on an overall rating for integrity, by considering, on a worst case basis, what damage could be caused by a loss of integrity.

**Step 3: Assess impact – Availability**
The consequences and impact of a loss of the availability of telework information are assessed by subsequently carrying out the six tasks below.

*Task 1:*
Ask the line manager to consider the consequences of a loss of availability of telework information for a range of timescales, e.g. for:

- An hour
- 1-3 days
- A week
- A month

*Task 2:*
Use the 'Availability' page of the 'Impact Assessment Form' (appendix C) to:

- Focus attention on the consequences of a loss of availability.
- Record the results of the discussion.

*Task 3:*
Ask the line manager to rate the damage which would arise on an A to D scale for each business consequence and for each timescale referred to on the form, using the following ratings:

| *Rating* | *Significance* |
|---|---|
| A | Serious Damage |
| B | Significant Damage |
| C | Minor Impact |
| D | Negligible |

*Task 4:*
For ratings of A or B, ask the line manager to explain how a loss of availability would be damaging to the agency and to identify the particular:

- Process(es) supported by the telework information which are most important (e.g. recording of transactions, maintenance of customer details, generation of statements, production of cheques).
- Procedures that the agency would apply to continue operations following unavailability of telework information.

*Task 5:*
Decide on an overall rating to be applied to availability by considering, on a worst case basis, the overall damage that would be caused by a prolonged unavailability of telework information. This would normally be at least as high as the highest individual rating for each duration of unavailability.

*Task 6:*
Agree on the critical timescale for recovery of telework information, i.e. the timescale beyond which unavailability would be unacceptable to the agency. Typically this can be determined by reference to the time beyond which a B rating becomes an A rating.

**Step 4: Classify telework information**
Copy the overall ratings for confidentiality, integrity and availability and the overall critical timescale for availability onto the ‘Summary’ page of the ‘Impact Assessment Form’ (appendix D).

## Phase 3: Assess threats, vulnerabilities and controls

**Objectives**
Phase 3 consists of six tasks and has the following objectives:

- To assess key threats and vulnerabilities associated with the chosen telework typology.
- To identify the controls required to keep risks within acceptable limits.

*Task 1:*
Select all threats from the 'Directory of Threats' (appendix G) that are applicable to the chosen telework typology and copy the 'threat titles' and relevant 'security attributes' to a blank 'Threats, Vulnerabilities and Controls Assessment Form' (appendix E).

*Task 2:*
Use the filled in 'Threats, Vulnerabilities and Controls Assessment Form' to:

- Focus attention on key threats and vulnerabilities.
- Record the results of the discussion.

*Task 3:*
Determine how vulnerable the agency is to each threat included in the 'Threats, Vulnerabilities and Controls Assessment Form'. Take into consideration:

- The relevance of each of these threats for the chosen telework typology. A description of this relevance is added to most threats in the Directory of Threats.
- Any existing security controls.

*Task 4:*
Assign vulnerability ratings according to the likelihood of threats materializing. Use the following ratings:

| *Rating* | *Significance* |
|---|---|
| A | Highly Possible |
| B | Possible |
| C | Unlikely |
| D | Impossible |

*Task 5:*
If a high vulnerability is given, identify the specific reasons for the high rating.

*Task 6:*
For each threat identify the controls required, over and above those already implemented, to reduce the business risks associated with a loss of confidentiality, integrity or availability of telework information.

Use the 'Threat/Control Matrix' (appendix I) as well as the 'Directory of Controls' (appendix H) to identify controls that can be used to reduce relevant threats and consider prevention, detection and recovery controls as well as organizational, logical and physical controls

While identifying controls consider:

- The overall impact ratings for confidentiality, integrity and availability of telework information arrived at in phase 2 as well as the critical timescale for the availability of telework information.
- The likelihood of a threat materializing arrived at in task 4 and the relevance of a threat in relation to the confidentiality, integrity and availability of telework information. An indication of this relevance is given in the 'Directory of Threats'.

Keep in mind that:

- The proper implementation of logical controls on telework computers (e.g. anti-malware software) can only be safeguarded if software on the telework computer is installed and configured by the agency and if teleworkers do not have control rights that may enable them to change security settings.
- The implementation of controls associated with the teleworker's work location (e.g. the home) is only effective if teleworkers do not work at other remote locations and the location's owner is ready to cooperate.

## Phase 4: Produce an action plan

**Objectives**
Phase 4 has the following objectives:

- To produce an action plan for controls, designed to keep business risks associated with teleworking within acceptable limits.
- To record the overall results of the risk analysis.

*Task 1:*
Review the completed 'Impact Assessment Forms' and the 'Threats, Vulnerabilities and Controls Assessment Form'.

*Task 2:*
Record the identified controls on a blank 'Action Plan Form' (appendix F).

*Task 3*
Prioritize the controls taking into consideration:

- The effectiveness of the controls in relation to the required level of protection of the confidentiality, integrity and availability of telework information.
- The cost-effectiveness of controls.
- The ease with which controls can be implemented.

*Task 4:*
Indicate the priority by numbering the controls in descending importance (e.g. 1 – most important, 2 – less important, and so on).

*Task 5:*
Determine who will be responsible for implementing control requirements and record this on the 'Action Plan Form'.

*Task 6:*
Agree implementation dates with the individuals concerned and record them on the 'Action Plan Form'.

*Task 7:*
Review and agree the action plan with the responsible line manager, refining it as necessary in the light of the discussion.

# Appendix D: Impact Assessment Form – Confidentiality

| **Consequence**<br>*of unintended or unauthorized disclosure of telework information (worst case)* | **Impact rating**<br>*A) Serious damage*<br>*B) Significant damage*<br>*C) Minor impact*<br>*D) Negligible* | | | | **Explanatory comments** |
|---|---|---|---|---|---|
| **C1) Competitive disadvantage**<br>*Could disclosure of telework information harm the competitive position?* | **A** | **B** | **C** | **D** | |
| **C2) Political implications**<br>*Could publication of telework information lead to social commotion or political turbulence?* | **A** | **B** | **C** | **D** | |
| **C3) Public confidence**<br>*If telework information is disclosed, what damage could there be to customer confidence; public image; or shareholder or supplier loyalty?* | **A** | **B** | **C** | **D** | |
| **C4) Additional costs**<br>*Could extra costs be incurred if telework information is disclosed?* | **A** | **B** | **C** | **D** | |
| **C5) Legal liability**<br>*Could disclosure of telework information result in a breach of legal, regulatory or contractual obligations?* | **A** | **B** | **C** | **D** | |
| **C6) Staff morale**<br>*If telework information is disclosed, could there be a damaging effect on staff morale or motivation?* | **A** | **B** | **C** | **D** | |
| **C7) Fraud**<br>*If telework information is disclosed, could goods or funds be improperly diverted?* | **A** | **B** | **C** | **D** | |
| **Overall rating**<br>*In summary, taking into account the ratings noted above and any other consequences, what is the most serious damage which would arise from unintended or unauthorized disclosure of telework information? (This would normally be at least as high as the highest individual rating)* | **A** | **B** | **C** | **D** | |

# Appendix E: Impact Assessment Form – Integrity

| **Consequence**<br>*of errors in telework information or of deliberate manipulation of telework information to perpetrate or conceal fraud (worst case)* | **Impact rating**<br>*A) Serious damage*<br>*B )Significant damage*<br>*C) Minor impact*<br>*D) Negligible* | | | | **Explanatory comments** |
|---|---|---|---|---|---|
| **I1) Management decisions**<br>*Could incorrect decisions be made as a result of errors in or unauthorized changes to telework information?* | **A** | **B** | **C** | **D** | |
| **I2) Personal well-being**<br>*Could corrupted telework information lead to disasters in relation to the well-being of persons?* | **A** | **B** | **C** | **D** | |
| **I3) Fraud**<br>*Could fraudulent diversion of goods or funds arise from or be concealed by unauthorized changes to telework information?* | **A** | **B** | **C** | **D** | |
| **I4) Public confidence**<br>*What damage could there be to customer confidence, public image and reputation, or shareholders or supplier loyalty as a result of errors in or unauthorized changes to telework information?* | **A** | **B** | **C** | **D** | |
| **I5) Additional costs**<br>*Could additional costs arise through unauthorized changes to, or errors in, telework information e.g. through the need to investigate integrity problems, or to restore the integrity of lost or corrupted data?* | **A** | **B** | **C** | **D** | |
| **I6) Legal liability**<br>*Could legal, regulatory or contractual obligations be breached if there are errors in or unauthorized changes to telework information?* | **A** | **B** | **C** | **D** | |
| **I7) Staff morale**<br>*Could there be a damaging effect on staff morale or motivation e.g. if staff cannot rely on telework information?* | **A** | **B** | **C** | **D** | |
| **I8) Business disruption**<br>*Could the business be otherwise disrupted as a result of errors in or unauthorized changes to telework information?* | **A** | **B** | **C** | **D** | |
| **Overall rating**<br>*In summary, taking into account the ratings noted above, and any other consequences, what is the most serious damage which could arise through errors in or unauthorized changes to telework information? (This would normally be at least as high as the highest individual rating)* | **A** | **B** | **C** | **D** | |

# Appendix F: Impact Assessment Form – Availability

| **Consequence**<br>*of a prolonged unavailability of telework information (worst case)* | **Impact rating**<br>*A) Serious damage*<br>*B) Significant damage*<br>*C) Minor impact*<br>*D) Negligible* | | | | **Explanatory comments** |
|---|---|---|---|---|---|
| *Duration of unavailability* | An hour | 1-3 days | A week | A month | |
| **A1) Management decisions**<br>*Could decision making be adversely affected by telework information being unavailable?* | | | | | |
| **A2) Personal well-being**<br>*Could corrupted telework information directly lead to life threatening situations or seriously affect the health of persons?* | | | | | |
| **A3) Public confidence**<br>*Could customer confidence, public image and reputation, or shareholder or supplier loyalty be damaged if telework information is unavailable?* | | | | | |
| **A4) Additional costs**<br>*What additional costs could arise through telework information being unavailable?* | | | | | |
| **A5) Legal liability**<br>*Could legal, regulatory or contractual obligations be breached through a loss of the availability of telework information?* | | | | | |
| **A6) Recovery**<br>*How costly would it be to recover from the backlog in processing if telework information was unavailable?* | | | | | |
| **A7) Staff morale**<br>*Could there be a damaging effect on staff morale or motivation if the availability of telework information was disrupted?* | | | | | |
| **A8) Fraud**<br>*Could fraudulent diversion of goods or funds arise from, or be concealed by, telework information being unavailable?* | | | | | |
| **A9) Business disruption**<br>*Could the business be otherwise disrupted from telework information being unavailable?* | | | | | |
| **Overall rating**<br>*In summary, what is the most serious damage which would arise from unavailability of telework information at the worst possible time?* | | | | | |
| **Overall critical timescale**<br>*What is the critical timescale for recovery of this information (i.e. the timescale beyond which unavailability is unacceptable to the business)?* | | | | | |

# Appendix G: Impact Assessment Form – Summary

**Overall impact ratings**
*(Copy from the individual Impact Assessment forms)*

| | | | | |
|---|---|---|---|---|
| **Loss of confidentiality** | A | B | C | D |
| **Loss of integrity** | A | B | C | D |

| *Impact Ratings* | |
|---|---|
| *A* | *Serious Damage* |
| *B* | *Significant Damage* |
| *C* | *Minor Impact* |
| *D* | *Negligible* |

**Loss of availability for:**

| | | | | |
|---|---|---|---|---|
| An hour | A | B | C | D |
| 1-3 days | A | B | C | D |
| A week | A | B | C | D |
| A month | A | B | C | D |
| *Critical timescale* | | | | |

*The critical timescale is the timescale beyond which unavailability of telework information would be unacceptable to the agency (e.g. 5 days).*

# Appendix H: Action Plan Form

| Priority | Title of control | Responsibility | Implementation date |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# Appendix I: Threats, Vulnerabilities and Controls Assessment Form

| **Threats** *(Circle or underline threats which are of particular concern)* | **Sec. attrib.** | **Vulnerability rating** *A) Highly Possible B) Possible C) Unlikely D) Impossible* | | | | **Comments** | **Controls required** |
|---|---|---|---|---|---|---|---|
| **Component A: The teleworker** | | | | | | | |
| Disclosure of log-on information | *CIA* | | | | | | |
| Loss of authentication token | *CIA* | | | | | | |
| Etc. | | | | | | | |
| **Component B: The location** | | | | | | | |
| Unreliable power supply | *IA* | | | | | | |
| Etc. | | | | | | | |
| **Component C: The telework computer** | | | | | | | |
| **Component D: The Internet connection** | | | | | | | |
| **Component E: The remote access farm** | | | | | | | |

# Appendix J: Directory of Threats

## Index

| | | | Security attributes | | | Typologies | |
|---|---|---|---|---|---|---|---|
| **Component A: The teleworker** | | | **C** | **I** | **A** | **T1** | **T2** |
| | A1.1 | Disclosure of log-on information | + | + | - | + | + |
| | A1.2 | Loss of authentication token or certificate | + | + | - | + | + |
| | A1.3 | Chosen passwords are weak | + | + | - | + | + |
| | A1.4 | Introduction of malware from the Internet or email | + | + | + | + | - |
| | A1.5 | Introduction of malware code from portable data carriers | + | + | + | + | - |
| | A1.6 | Connection of telework computer to computer networks | + | + | - | + | - |
| | A1.7 | Malfunctioning telework computers in the hands of third parties | + | - | + | + | - |
| | A1.8 | Use of telework computers by third parties | + | + | + | + | + |
| | A1.9 | Neglect of important 'housekeeping activities' | + | + | + | + | - |
| | A1.10 | Loading of harmful software | + | + | + | + | - |
| | A1.11 | Inappropriate changes to software configuration | + | + | + | + | - |

| | | | Security attributes | | | Typologies | |
|---|---|---|---|---|---|---|---|
| **Component B: The telework location** | | | **C** | **I** | **A** | **T1** | **T2** |
| | *Category 1: Teleworker is unable to access telework equipment or the remote access farm* | | | | | | |
| | B1.1 | Unreliable power supply | X | - | + | + | + |
| | B1.2 | Absence of an Internet connection | X | X | + | X | + |
| | B1.3 | Incompatible technologies for access to the Internet | X | X | + | X | + |
| | *Category 2: The remote location is not physically secure* | | | | | | |
| | B2.1 | Loss or theft of telework equipment | + | X | + | + | - |
| | B2.2 | Damage to telework computers | X | - | + | + | - |
| | B2.3 | Inspection of information through overlooking | + | X | X | + | + |

| | | | Security attributes | | | Typologies | |
|---|---|---|---|---|---|---|---|
| **Component C: The telework computer** | | | **C** | **I** | **A** | **T1** | **T2** |
| | *Category 1: Poor hard- and software configuration* | | | | | | |
| | C1.1 | Telework computer not suitable for teleworking | X | + | + | + | + |
| | C1.2 | Logical access control on telework computer bypassed | + | + | + | + | - |
| | C1.3 | Security features not properly configured | + | + | + | + | - |
| | C1.4 | Inadequate malware protection | + | + | + | + | - |
| | *Category 2: Telework computer vulnerable to tampering* | | | | | | |
| | C2.1 | Discovery of log-on information stored on telework computer | + | + | + | + | + |
| | C2.2 | Encryption keys stored on telework computer compromised | + | + | + | X | + |
| | *Category 3: Telework computer unable to connect to the remote access farm* | | | | | | |
| | C3.1 | Internet access device malfunctions | X | + | + | X | + |
| | C3.2 | Communications software malfunctions | X | + | + | X | + |

| | | | Security attributes | | | Typolo-gies | |
|---|---|---|---|---|---|---|---|
| **Component D: The Internet connection** | | | **C** | **I** | **A** | **T1** | **T2** |
| | D1 | Unavailable Internet connection | X | X | + | X | + |
| | D2 | Unreliable or slow Internet connection | X | + | X | X | + |
| | D3 | Unauthorized inspection of data in transit | + | X | X | X | + |
| | D4 | Hijacking of the connection | + | + | + | X | + |
| | D5 | Unused connections remain open | + | + | + | X | + |

| | | | Security attributes | | | Typolo-gies | |
|---|---|---|---|---|---|---|---|
| **Component E: The remote access farm** | | | **C** | **I** | **A** | **T1** | **T2** |
| | E1 | Remote access farm not continuously available | X | + | + | X | + |
| | E2 | Teleworker has too many access rights on remote access farm | + | + | + | X | + |
| | E3 | Unauthorized parties gain access to the remote access farm | + | + | + | X | + |

## Threat boxes

### Component A: The teleworker

| Threat A1.1 | | | Disclosure of log-on information |
|---|---|---|---|
| *Security attributes* | *C*<br>*I*<br>*A* | +<br>+<br>- | **Unauthorized parties may gain access to telework information if the teleworker discloses log-on information.** |
| *Typologies* | *T1*<br>*T2* | +<br>+ | The teleworker may have to identify and authenticate himself by means of log-on information, such as usernames (identification) and passwords (authentication), in order to gain access to telework information. If log-on information is disclosed to others, they may also be able to gain access to that information.<br><br>Log-on information may for example come in the hands of others if a teleworker writes down his username and password or if the teleworker is mislead through social engineering.<br><br>***T1***<br>*In case authentication to the telework computer is based 'what the teleworker knows', locally stored information may be compromised if log-on information is disclosed to unauthorized parties.*<br><br>***T2***<br>*In case authentication to the remote access farm is based on 'what the teleworker knows', centrally stored information may be compromised if log-on information is disclosed to unauthorized parties.* |

| Threat A1.2 | | | Loss of authentication token |
|---|---|---|---|
| *Security attributes* | *C*<br>*I*<br>*A* | +<br>+<br>- | **Unauthorized parties may gain access to telework information if the teleworker loses his authentication token.**<br><br>In addition to usernames and passwords a teleworker may have to authenticate himself by means of a token in order to gain access to telework information. If others are in possession of a token in combination with relevant log-on information, they may also be able to gain access to that information.<br><br>Tokens may for example come in the hands of unauthorized parties if the teleworker loses them or if he is mislead through social engineering.<br><br>***T1***<br>*In case authentication to the telework computer is based on 'what the teleworker has', locally stored information may be compromised if the teleworker loses his authentication token.*<br><br>***T2***<br>*In case authentication to the remote access farm is based on 'what the teleworker has', centrally stored information may be compromised if the teleworker loses his authentication token.* |
| *Typologies* | *T1*<br>*T2* | +<br>+ | |

| Threat A1.3 | | | Choosing weak passwords |
|---|---|---|---|
| *Security attributes* | *C*<br>*I*<br>*A* | +<br>+<br>- | **Unauthorized parties may gain access to sensitive agency information if the teleworker chooses weak passwords.**<br><br>The average user can only remember a limited number of different passwords. Therefore they are inclined to choose obvious passwords, such as their first, last or child's name, a birth date, or even the word 'password'. Such obvious passwords can be easily guessed, especially if the intruder knows something about the teleworker's background.<br><br>Users may also use less obvious passwords such as random dictionary words. Although it may not be possible for an intruder to guess such passwords, they may be easily discovered by means of a software-led brute force or dictionary attack.<br><br>***T1***<br>*In case authentication to the telework computer is based 'what the teleworker knows', locally stored information may be compromised if the teleworker chooses weak passwords*<br><br>***T2***<br>*In case authentication to the remote access farm is based on 'what the teleworker knows', centrally stored information may be compromised if the teleworker chooses weak passwords.* |
| *Typologies* | *T1*<br>*T2* | +<br>+ | |

| Threat A1.4 | | | Introduction of malware via Internet or email |
|---|---|---|---|
| *Security attributes* | *C*<br>*I*<br>*A* | +<br>+<br>+ | **Malware may infect the telework computer if the teleworker accesses untrusted web sites or opens untrusted email.**<br><br>Internet browsers may automatically run self-executing mobile code contained in for example JAVA applets or ActiveX controls that are normally used to enhance web sites. Email clients may automatically run program scripts contained in email. If mobile code or program scripts are malicious in nature they may affect the telework computer.<br><br>It may also be that the teleworker downloads files from the Internet or email attachments that contain malware. Opening such files may lead to infection of the telework computer.<br><br>***T1***<br>*Locally stored information may be compromised if a telework computer is infected with malware.*<br><br>***T2***<br>*Centrally stored information is unlikely to be compromised if a telework computer is infected with malware, because only application views, keystrokes and mouse clicks are being communicated between telework computers and the remote access farm.*<br><br>*Certain malware may however create a backdoor on a telework computer through which data (e.g. key strokes or screen prints) are leaked to unauthorized parties (e.g. a key logger in combination with a Trojan horse). In case log-on information is leaked this way and authentication to the remote access farm is based on only one factor, centrally stored information may be accessed by unauthorized parties.*<br><br>*Centrally stored information may become (temporarily) unavailable to a teleworker if his telework computer does not work properly due to malware.* |
| *Typologies* | *T1*<br>*T2* | +<br>- | |

| Threat A1.5 | | | Introduction of malware from portable data carriers |
|---|---|---|---|
| *Security attributes* | *C*<br>*I*<br>*A* | +<br>+<br>+ | **Malware may infect the telework computer if the teleworker loads data from portable data carriers such as diskettes, CDs or memory sticks.** |
| *Typologies* | *T1*<br>*T2* | +<br>- | Data on portable data carriers may contain malware. If the teleworker accesses those data carriers or opens infected files, malware may be introduced to the telework computer.<br><br>***T1***<br>*See A1.4*<br><br>***T2***<br>*See A1.4* |

| Threat A1.6 | | | Connection of telework computer to computer networks |
|---|---|---|---|
| *Security attributes* | *C*<br>*I*<br>*A* | +<br>+<br>- | **Telework information may be accessed by unauthorized parties if the teleworker connects his computer to computer networks.** |
| *Typologies* | *T1*<br>*T2* | +<br>- | The teleworker may connect his telework computer to insecure computer networks such as WANs like the Internet or LANs like home networks.<br><br>Other parties connected to the same network as the teleworker may be able to remotely gain access to telework computers. This may lead to unauthorized inspection or modification of information (including log-on information) or to its unavailability.<br><br>***T1***<br>*Locally stored information may be compromised if others remotely gain access to the telework computer.*<br><br>***T2***<br>*Centrally stored information is unlikely to be compromised if others remotely gain remote access to the telework computer, because the telework computer does not actually become part of the remote access farm.*<br><br>*Access to telework computers may however enable third parties to collect log-on information. If authentication to the remote access farm is based on only one factor, this may lead to unauthorized access.* |

| Threat A1.7 | | | Malfunctioning telework computers in the hands of third parties |
|---|---|---|---|
| *Security attributes* | *C*<br>*I*<br>*A* | +<br>-<br>+ | **Telework information may be lost or accessed by unauthorized parties if the teleworker throws away a malfunctioning telework computer or lets untrusted parties repair it.** |
| *Typologies* | *T1*<br>*T2* | +<br>- | Throwing away telework computers or repair activities may lead to information unavailability, if that information is not also stored elsewhere.<br><br>Throwing away telework computers may also lead to disclosure of sensitive information if other parties collect the computer before it is definitely destroyed and the data on it still is recoverable.<br><br>Repair activities may harm information confidentiality and integrity, especially if parties who perform repair activities (e.g. local computer shops or acquaintances) are malicious.<br><br>***T1***<br>*Locally stored information may be lost or accessed by unauthorized parties if the telework computer is thrown away or repaired.*<br><br>***T2***<br>*Centrally stored information is unlikely to be lost or accessed by unauthorized parties if telework computers are thrown away or being repaired, unless log-on information is discovered on telework computers and authentication to the remote access farm is based on only one factor.* |

| Threat A1.8 | | | Use of telework computers by third parties |
|---|---|---|---|
| *Security attributes* | *C*<br>*I*<br>*A* | +<br>+<br>+ | **The teleworker may give third parties the opportunity to make use of his telework computer, thereby introducing extra security risks related to unauthorized access and malware.** |
| *Typologies* | *T1*<br>*T2* | +<br>+ | A teleworker may allow family or friends to make use of available applications or install new ones. This can possibly introduce various security risks associated with access to information by unauthorized parties and malicious programs.<br><br>The teleworker may also unwittingly give unauthorized parties the opportunity to make use of telework equipment, for example by leaving it temporarily unattended. These parties are more likely to be malicious in nature than parties that have wittingly been allowed by the teleworker to work on his computer.<br><br>***T1***<br>*The teleworker may enable third parties to access applications and information that are available on the telework computer.*<br><br>***T2***<br>*The teleworker may enable third parties to access applications and information that are available on the remote access farm.* |

| Threat A1.9 | | | Neglect of important 'housekeeping activities' |
|---|---|---|---|
| *Security attributes* | *C*<br>*I*<br>*A* | +<br>+<br>+ | **Telework information may come in the hands of unauthorized parties or become unavailable or corrupted if the teleworker does not carry out important 'housekeeping activities'.** |
| *Typologies* | *T1*<br>*T2* | +<br>- | Examples of important housekeeping activities are taking back-ups, updating (security and system) software and installing patches. The majority of these activities can be technically realized, but to a certain extent involvement of the teleworker may also be necessary. The teleworker however may not realize the importance of his contribution and neglect his share in the housekeeping for the sake of convenience.<br><br>A lack of back-up may result in a loss of data. This may not only include telework information, but also computer software and hardware configurations. The introduction of malware, as a result of outdated security software, may harm one or more security attributes of information, depending on its nature.<br><br>***T1***<br>*Locally stored information is susceptible to malware and unauthorized access which stresses the importance of proper up-to-date security software. Back-ups of locally stored information may not be made on a regular basis.*<br><br>***T2***<br>*It is unlikely that centrally stored information will be compromised due to inadequate housekeeping on the telework computer, unless log-on information comes into the hands of unauthorized parties and authentication to the remote access farm is based on only one factor. Back-ups of centrally stored information are normally made on a regular basis.* |

| Threat A1.10 | | | Loading of harmful software |
|---|---|---|---|
| *Security attributes* | *C*<br>*I*<br>*A* | +<br>+<br>+ | **Telework information may be accessed by unauthorized parties and telework computers may become unreliable if the teleworker loads potentially harmful software.** |
| *Typologies* | *T1*<br>*T2* | +<br>- | The teleworker may install and/or make use of potentially harmful software, because it has certain functionalities he desires. Examples of such software are instant messaging and file sharing programs.<br><br>This software is not necessarily malicious in nature (like Trojan horses), but may bypass security controls in place. It thereby possibly allows third parties to remotely access information on telework computers. Harmful software may also cause telework computers to operate unpredictably.<br><br>Sensitive telework information may for example come available if file sharing programs such as Kazaa or Limewire are misconfigured.<br><br>***T1***<br>*Locally stored information may be accessed by unauthorized parties or become unavailable due to the installation of harmful software.*<br><br>***T2***<br>*It is unlikely that centrally stored information will be compromised due to installation of harmful software on the telework computer, unless log-on information comes into the hands of unauthorized parties and authentication to the remote access farm is based on only one factor.* |

| Threat A1.11 | | | Inappropriate changes to software configuration |
|---|---|---|---|
| *Security attributes* | *C*<br>*I*<br>*A* | +<br>+<br>+ | **Telework information may be exposed to various security risks if the teleworker adjusts the default configuration of important software on his computer.**<br><br>The teleworker may change the default configuration of important software on his computer, such as the operating system, communications software, anti-malware software, personal firewalls and web browsers. This may lead to various security risks associated with information unavailability, unauthorized access and the introduction of malware.<br><br>***T1***<br>*Locally stored information may be compromised if software configurations are changed inappropriately.*<br><br>***T2***<br>*It is unlikely that centrally stored information will be compromised due to inappropriate changes to software configurations, unless log-on information comes into the hands of unauthorized parties and authentication to the remote access farm is based on only one factor.* |
| *Typologies* | *T1*<br>*T2* | +<br>- | |

## Component B: The telework location

*Category 1: Teleworker is unable to access telework equipment or the remote access farm*

| Threat B1.1 | | | Unreliable power supply |
|---|---|---|---|
| *Security attributes* | *C*<br>*I*<br>*A* | X<br>-<br>+ | **Telework equipment may not be accessible when needed or data may get corrupted if the power supply at remote locations is unreliable.** |
| *Typologies* | *T1*<br>*T2* | +<br>+ | The Dutch electricity grid is considered to be one of the most reliable grids in the world. Nevertheless occasional net interferences are unavoidable.<br><br>Telework computers and peripherals may be unavailable during a power failure, especially if they are not equipped with batteries.<br><br>Power failure may also lead to prolonged unavailability of telework computers or corruption of data. For example if power failure has damaged equipment or if data was being processed at the moment power failure occurred.<br><br>***T1***<br>*Locally stored information may become (temporarily) unavailable or be corrupted due to unreliable power supply at the remote location.*<br><br>***T2***<br>*Centrally stored information may be corrupted due to unreliable power supply at the remote location or become temporarily unavailable to teleworkers who cannot use their computers during power failure.* |

| Threat B1.2 | | | Absence of an Internet connection |
|---|---|---|---|
| *Security attributes* | *C*<br>*I*<br>*A* | X<br>X<br>+ | **Teleworkers may not be able to communicate with the remote access farm if there are no available Internet connections at the remote location.** |
| *Typologies* | *T1*<br>*T2* | X<br>+ | If the remote location does not have an available Internet connection for the teleworker to use, electronic communication with the remote access farm cannot take place. |

| Threat B1.3 | | | Incompatible technologies for access to the Internet |
|---|---|---|---|
| *Security attributes* | *C*<br>*I*<br>*A* | X<br>X<br>+ | **Teleworkers may not be able to connect to the remote access farm if Internet access devices are not compatible with available Internet access technologies at remote locations.** |
| *Typologies* | *T1*<br>*T2* | X<br>+ | There are various ways to connect a telework computer to the Internet. Different Internet access technologies (e.g. cable, telephone line or wireless) require different Internet access devices (e.g. cable modem, dial-up modem or wireless adapter).<br><br>If a telework computer is not equipped with an Internet access device that suits the Internet access technology at the remote location, the remote access farm will be unavailable from that location.<br><br>If a teleworker works 'on the fly' available technologies for access to the Internet may differ from location to location. If the teleworker works at a fixed location, the available technology is normally unchanging and known. |

*Category 2: The remote location is not physically secure*

| **Threat B2.1** | | | **Loss or theft of telework equipment** |
|---|---|---|---|
| *Security attributes* | *C*<br>*I*<br>*A* | +<br>X<br>+ | **Telework information may be lost or accessed by unauthorized parties if telework computers are stolen from a remote location.**<br><br>Telework computers are susceptible to loss through carelessness or targeted theft when the teleworker works from insecure remote locations.<br><br>Sensitive data stored on a telework computer (e.g. telework information, usernames and passwords) can be exposed if the computer is lost or stolen. Both the machine and any data stored on it may be irrecoverable as a result.<br><br>Physical access security is usually better if teleworking takes place from fixed locations than if it takes place 'on the fly'. In both cases however, it is unlikely to be as good as at within the agency's premises.<br><br>***T1***<br>*Locally stored information may become unavailable or may be inspected by unauthorized parties if the telework computer is lost or stolen.*<br><br>***T2***<br>*Centrally stored information is unlikely to become unavailable or to be accessed by unauthorized parties if telework computers are lost or stolen, unless log-on information is discovered on telework computers and authentication to the remote access farm is based on only one factor.* |
| *Typologies* | *T1*<br>*T2* | +<br>- | |

| **Threat B2.2** | | | **Damage to telework computers** |
|---|---|---|---|
| *Security attributes* | *C*<br>*I*<br>*A* | X<br>-<br>+ | **Information may become unavailable or corrupted if telework computers at the remote location are damaged.**<br><br>If telework computers are physically damaged at remote locations, information stored and/or processed by those computers may become corrupted or unavailable.<br><br>The nature of threats that can cause physical damage varies considerably. Damage may for example be caused by earthquakes, lightening, flooding, storm, fire, shocks, electromagnetism and explosions.<br><br>Telework computers are more likely to be damaged if a teleworker works 'on the fly' than if he works from a fixed location. In the first case computers may be frequently exposed to threats inherent to travelling, such as shocks. Nevertheless computers used from fixed locations, will also be at risk from damage if they are not placed securely and kept free from domestic hazards.<br><br>***T1***<br>*Locally stored information may become (permanently) unavailable or corrupted if telework computers are damaged.*<br><br>***T2***<br>*Centrally stored information is less likely to become (permanently) unavailable or corrupted if telework computers are damaged, unless damage occurs during data exchange between the computer and the remote access farm.* |
| *Typologies* | *T1*<br>*T2* | +<br>- | |

| Threat B2.3 | | | Inspection of information through overlooking |
|---|---|---|---|
| *Security attributes* | *C*<br>*I*<br>*A* | +<br>X<br>X | **The confidentiality of telework information may be compromised if it is displayed on the screen of telework computers and if that screen is visible to unauthorized parties.** |
| *Typologies* | *T1*<br>*T2* | +<br>+ | The size and location of the computer screen determine the risk that information is compromised through overlooking. Laptop screens for example are relatively big and visible from a wide angle, whereas information on small PDA screens is a lot harder to see.<br><br>The risk that unauthorized people read the computer screen is relatively high if teleworking takes place 'on the fly'. Especially if the computer is used while travelling in public transport. Nevertheless unauthorized people may also read the screen if a teleworker works from a fixed location.<br><br>***T1***<br>*Locally stored information displayed on the screen of the telework computer may be inspected through overlooking.*<br><br>***T2***<br>*Centrally stored information displayed on the screen of the telework computer may be inspected through overlooking.* |

## Component C: The telework computer

*Category 1: Poor hard- and software configuration*

| **Threat C1.1** | | | **Telework computer not suitable for teleworking** |
|---|---|---|---|
| *Security attributes* | *C*<br>*I*<br>*A* | X<br>+<br>+ | **The teleworker may not be able to run required applications if the telework computer is unsuitable for teleworking.**<br><br>Telework computers may be of insufficient technical specification or too unreliable to properly execute applications. This may impair the teleworker to work effectively.<br><br>The computer may for example not have enough internal memory or the processor and/or hardware ports may be too slow. It may also be that computers are of poor quality or available hard- and software conflicts.<br><br>***T1***<br>*Locally stored information may be unavailable or become corrupted if the telework computer cannot properly run the required applications.*<br><br>***T2***<br>*Centrally stored information may be unavailable or become corrupted if the telework computer cannot establish a proper connection with the remote access farm.* |
| *Typologies* | *T1*<br>*T2* | +<br>+ | |

| **Threat C1.2** | | | **Logical access control on telework computer bypassed** |
|---|---|---|---|
| *Security attributes* | *C*<br>*I*<br>*A* | +<br>+<br>+ | **An unauthorized party may be able to bypass logical access control on telework computers and gain access to telework information.**<br><br>Pre-boot authentication may be bypassed by removing the back-up battery on the computer's motherboard. This resets BIOS settings including any pre-boot password protection.<br><br>Operating system level authentication may be bypassed by booting the telework computer from an external data carrier (e.g. floppy or CD-Rom) instead of its hard disk.<br><br>***T1***<br>*Locally stored information may be compromised if logical access control on telework computers is bypassed by unauthorized parties.*<br><br>***T2***<br>*Centrally stored information is unlikely to be compromised if logical access control on telework computers is bypassed, unless it leads to disclosure of log-on information and authentication to the remote access farm is based on only one factor.* |
| *Typologies* | *T1*<br>*T2* | +<br>- | |

| Threat C1.3 | | | Security features not properly configured |
|---|---|---|---|
| *Security attributes* | *C*<br>*I*<br>*A* | +<br>+<br>+ | **An unauthorized party may be able to gain access to the telework computer if security features are not properly configured.**<br><br>Operating systems, web browsers, email clients and security software (e.g. personal firewalls) have many security features, but they are not always configured by default.<br><br>If the teleworker is not very knowledgeable he may not be able to configure security features by himself or he may make improper changes to default configurations.<br><br>***T1***<br>*Locally stored information may be compromised if important security features are not configured correctly.*<br><br>***T2***<br>*Centrally stored information is unlikely to be compromised if security features are not configured properly, unless it leads to disclosure of log-on information and access to the remote access farm is based on only one factor.* |
| *Typologies* | *T1*<br>*T2* | +<br>- | |

| Threat C1.4 | | | Inadequate malware protection |
|---|---|---|---|
| *Security attributes* | *C*<br>*I*<br>*A* | +<br>+<br>+ | **Unless anti-malware software is installed, configured correctly and kept up-to-date, the telework computer will potentially be exposed to the introduction of malware.**<br><br>The introduction of malware may harm the confidentiality, integrity, and/or availability of information. Which security attributes are actually compromised depends on the nature of the malware in question.<br><br>***T1***<br>*See A1.4*<br><br>***T2***<br>*See A1.4* |
| *Typologies* | *T1*<br>*T2* | +<br>- | |

*Category 2: Telework computer vulnerable to tampering*

| **Threat C2.1** | | | **Discovery of log-on information stored on telework computer** |
|---|---|---|---|
| *Security attributes* | *C*<br>*I*<br>*A* | +<br>+<br>+ | **Log-on information stored on telework computers may be discovered by unauthorized parties which possibly enables them to gain access to telework information.**<br><br>Operating systems usually store log-on information in order to save the users from having to re-enter usernames and/or passwords each time a resource is accessed.<br><br>While such files are often encrypted, gaining access to a client computer may also enable an unauthorised user to access all resources protected by stored log-on information.<br><br>***T1***<br>*Locally stored information may be compromised if log-on information for access to the telework computer is discovered.*<br><br>***T2***<br>*Centrally stored information may be compromised if log-on information for access to the remote access farm is discovered, unless authentication to the remote access farm is based on more than one factor.* |
| *Typologies* | *T1*<br>*T2* | +<br>+ | |

| **Threat C2.2** | | | **Encryption keys stored on telework computer compromised** |
|---|---|---|---|
| *Security attributes* | *C*<br>*I*<br>*A* | +<br>+<br>+ | **If encryption keys generated in software on telework computers are compromised, unauthorized parties may gain access to the remote access farm.**<br><br>If discovered, encryption keys stored on telework equipment could enable an unauthorized party to complete the authentication process, potentially allowing access to the remote access farm. |
| *Typologies* | *T1*<br>*T2* | X<br>+ | |

*Category 3: Telework computer unable to connect to the remote access farm*

| **Threat C3.1** | | | **Internet access device malfunctions** |
|---|---|---|---|
| *Security attributes* | *C*<br>*I*<br>*A* | X<br>+<br>+ | **The teleworker may not be able to properly communicate with the remote access farm if the Internet access device malfunctions.**<br><br>Internet access devices, such as cable modems or wireless adapters, are used to connect telework computers with the Internet.<br><br>Such devices may malfunction due to a number of reasons, ranging from fabrication errors, incompatibility with other hard- and software to improper configuration. |
| *Typologies* | *T1*<br>*T2* | X<br>+ | |

| **Threat C3.2** | | | **Communications software malfunctions** |
|---|---|---|---|
| *Security attributes* | *C*<br>*I*<br>*A* | X<br>+<br>+ | **Telework computers may not be able to properly communicate with the remote access farm if communications software malfunctions.**<br><br>Communication software is used to enable the telework computer to communicate with the remote access farm through the Internet access device.<br><br>Such software may for example malfunction because it is incompatible with other software installed on the telework computer, the Internet access device or communication protocols in use (e.g. ICA). It may also be that communications software malfunctions because it is misconfigured. |
| *Typologies* | *T1*<br>*T2* | X<br>+ | |

## Component D: The Internet connection

| Threat D1 | | | Unavailable Internet connection |
|---|---|---|---|
| *Security attributes* | *C*<br>*I*<br>*A* | X<br>X<br>+ | **Teleworkers may not be able to gain access to the remote access farm if the Internet connection is unavailable.** |
| *Typologies* | *T1*<br>*T2* | X<br>+ | The public Internet is very reliable, but it may be that the communications infrastructure from the agency's premises to a local telephone exchange or from a local telephone exchange to the telework location is damaged for example due to repair or construction work. (Wireless) local networks may also be unavailable for example if routers are damaged or overburdened.<br><br>An Internet connection may also be unavailable if the Internet Access provider of the agency or the teleworker does not guarantee continuous availability or a comprehensive support service, or in case of contractual disputes or unpaid Internet bills |

| Threat D2 | | | Unreliable or slow Internet connection |
|---|---|---|---|
| *Security attributes* | *C*<br>*I*<br>*A* | X<br>+<br>X | **Teleworkers may not be able to properly communicate with the remote access farm if the connection is unreliable or slow.** |
| *Typologies* | *T1*<br>*T2* | X<br>+ | There are various reasons why an Internet connection may be unreliable or slow. The Internet Access Provider may not be able to deliver a consistent, robust and reliable service. These problems may relate to insufficient network capacity or poor support arrangements.<br><br>It may also be that access to the remote access farm is gained via unreliable (wireless) local networks on the telework location. The data transmission speed and reliability of such networks may not always be very good. Network routers may for example be overburdened and wireless networks may have unreliable signal strength |

| Threat D3 | | | Unauthorized inspection of data in transit |
|---|---|---|---|
| *Security attributes* | *C*<br>*I*<br>*A* | +<br>X<br>X | **Data communication between a telework computer and the remote access farm may be inspected by unauthorized parties.** |
| *Typologies* | *T1*<br>*T2* | X<br>+ | The risk that data that is transmitted via the Internet is inspected by unauthorized parties is considerable. Anyone who for example has control of a network server on the Internet or can intercept wireless data communication may eavesdrop on data communication.<br><br>Eavesdropping is a passive attack that can lead to a confidentiality breach of data in transit, such as sensitive agency information or log-on information. The latter can be used by an unauthorized party to gain access to the remote access farm. |

| Threat D4 | | | Hijacking of the connection |
|---|---|---|---|
| *Security attributes* | *C*<br>*I*<br>*A* | +<br>+<br>+ | **Data may be modified, inspected or become unavailable if the connection between the remote access farm and the telework computer is hijacked.** |
| *Typologies* | *T1*<br>*T2* | X<br>+ | Connection hijacking, also know as Man In the Middle Attack, is an active attack in which an attacker seizes control of the connection between the remote access farm and a telework computer. This may be done during the authentication procedure or in the middle of an established connection.<br><br>Once the connection is hijacked, the attacker can control the flow of communication and eliminate or alter the information sent by one of the two endpoints. This may for example enable the attacker to compromise data in transit or to gain access to the remote access farm. |

| Threat D5 | | | Unused connections remain open |
|---|---|---|---|
| *Security attributes* | *C*<br>*I*<br>*A* | +<br>+<br>+ | **Unused telework connections that remain open confiscate the resources on the remote access farm and increase the risk of unauthorized access.**<br><br>If teleworkers do not properly close connections after they have finished their work activities, those connections may stay open for a long time.<br><br>Open connections consume server resources and, as their number increases, may lead a considerable decline in server performance. Besides that, open connections may be used by unauthorized parties to gain access to the remote access farm. |
| *Typologies* | *T1*<br>*T2* | X<br>+ | |

## Component E: The remote access farm

| Threat E1 | | | Remote access farm not continuously available |
|---|---|---|---|
| *Security Attributes* | *C*<br>*I*<br>*A* | X<br>+<br>+ | **Failure of components of the remote access farm may lead to the unavailability or loss of telework information.**<br><br>Failure of (parts of) the remote access farm may be caused by various security incidents. The agency's servers may for example be overburdened if too many applications are running at the same time or if the workload is unequally divided over available servers. Natural disasters, power failures or fire may also lead to server unavailability.<br><br>The remote access farm may also be infected with malicious programs or victim of attacks by malicious third parties (e.g. DoS attacks). |
| *Typologies* | *T1*<br>*T2* | X<br>+ | |

| Threat E2 | | | Teleworker has too many access rights on remote access farm |
|---|---|---|---|
| *Security Attributes* | *C*<br>*I*<br>*A* | +<br>+<br>+ | **A teleworker may have access to more applications or files on the remote access farm than he should have.**<br><br>Improper implementation of access rights or misconfiguration of the remote access farm may enable the teleworker to remotely access applications or files that should not be available to him.<br><br>It may also be that applications have a 'backdoor' exit, which enables teleworkers to gain unauthorized access to other applications or (system) files on the agency's servers. |
| *Typologies* | *T1*<br>*T2* | X<br>+ | |

| Threat E3 | | | Unauthorized parties gain access to the remote access farm |
|---|---|---|---|
| *Security attributes* | *C*<br>*I*<br>*A* | +<br>+<br>+ | **Information may come available to unauthorized parties if they have the ability to gain access to the remote access farm.**<br><br>Unauthorized parties may be able to gain access to the remote access farm due to weak or nonexistent logical access control or because the servers have been infected by malware (e.g. a Trojan horse).<br><br>It may also be that they have gained access with the support of the teleworker or are in the possession of a teleworker's authentication means (e.g. usernames and password). Unauthorized parties may also have access rights on the agency's servers, because they are former teleworkers. |
| *Typologies* | *T1*<br>*T2* | X<br>+ | |

# Appendix K: Directory of Controls

## Index

| | | | Why | | | When | | | What | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Group A: General controls** | | | **C** | **I** | **A** | **P** | **D** | **R** | **O** | **L** | **P** |
| | *Category 1: Policy and standards* | | | | | | | | | | |
| | A1.1 | Develop and implement a security policy for teleworking | V | V | V | V | | | V | | |
| | A1.2 | Manage telework requests | V | V | V | V | | | V | | |
| | A1.3 | Develop and implement a telework agreement | V | V | V | V | | | V | | |
| | | | | | | | | | | | |
| | *Category 2: Authorization* | | | | | | | | | | |
| | A2.1 | Formally authorize teleworkers | V | V | V | V | | | V | | |
| | A2.2 | Approve remote locations | V | V | V | V | | | V | | |
| | A2.3 | Approve telework computers | V | V | V | V | | | V | | |
| | | | | | | | | | | | |
| | *Category 3: System and network management* | | | | | | | | | | |
| | A3.1 | Maintain adequate documentation of the telework service | V | V | V | V | V | V | V | | |
| | A3.2 | Manage authentication tools | V | V | V | V | | | V | V | V |
| | A3.3 | Manage cryptographic keys | V | V | V | V | | | V | V | V |
| | A3.4 | Monitor audit logs | V | V | V | | V | | V | | |
| | A3.5 | Monitor performance levels | | | V | | V | | V | | |
| | | | | | | | | | | | |
| | *Category 4: User support* | | | | | | | | | | |
| | A4.1 | Provide helpdesk support to teleworkers | V | V | V | V | V | V | | | |
| | A4.2 | Provide security software | V | V | V | V | V | V | V | V | |
| | A4.3 | Log all incidents | V | V | V | V | V | V | V | V | |
| | A4.4 | Ensure the proper return of telework equipment | V | V | V | V | | | V | | |
| | A4.5 | Securely dispose or re-use telework equipment | V | V | V | V | | | V | | |
| | A4.6 | Report stolen telework equipment | V | V | V | | V | | V | | |

| | | | Why | | | When | | | What | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Group B: Controls teleworker** | | | **C** | **I** | **A** | **P** | **D** | **R** | **O** | **L** | **P** |
| | *Category 1: Code of conduct and guidelines* | | | | | | | | | | |
| | B1.1 | Develop a code of conduct for teleworking | V | V | V | V | | | V | | |
| | B1.2 | Establish guidelines for using sensitive agency information | V | V | V | V | | | V | | |
| | B1.3 | Establish guidelines for non-work-related use of computers | V | V | V | V | | | V | | |
| | B1.4 | Establish guidelines for using wireless networks | V | V | V | V | | | V | | |
| | B1.5 | Establish guidelines for using anti-malw. software and firew. | V | V | V | V | | | V | | |
| | B1.6 | Establish guidelines for taking back-ups | V | V | V | V | | | V | | |
| | B1.7 | Establish guidelines for using portable data carriers | V | V | V | V | | | V | | |
| | B1.8 | Establish guidelines for using the Internet | V | V | V | V | | | V | | |
| | B1.9 | Establish guidelines for using email | V | V | V | V | | | V | | |
| | B1.10 | Establish guidelines for using authentication means | V | V | V | V | | | V | | |
| | B1.11 | Establish guidelines to prevent theft | V | V | V | V | | | V | | |
| | B1.12 | Establish guidelines for securing the remote location | V | V | V | V | | | V | | |
| | B1.13 | Provide copies of the code and guidelines to teleworkers | V | V | V | V | | | V | | |
| | | | | | | | | | | | |
| | *Category 2: Security awareness* | | | | | | | | | | |
| | B2.1 | Distribute awareness material | V | V | V | V | | | V | | |
| | B2.2 | Provide security awareness training | V | V | V | V | | | V | | |

| | | | Why | | | When | | | What | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Group C: Controls telework location (controls aimed at protecting a teleworker's home)** | | | **C** | **I** | **A** | **P** | **D** | **R** | **O** | **L** | **P** |
| | C1 | Properly construct the remote location | V | V | V | V | | | | | V |
| | C2 | Install a burglar alarm | V | V | V | | V | V | | | V |
| | C3 | Install a secure safe | V | V | V | V | | | | | V |
| | C4 | Install smoke detectors | | V | V | | V | | | | V |
| | C5 | Install sprinklers | | V | V | | V | V | | | V |
| | C6 | Install fire extinguishers | | V | V | | | V | | | V |
| | C7 | Install lightening protection | | V | V | | | V | | | V |

| | | | Why | | | When | | | What | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Group D: Controls telework computer (controls aimed at protecting a laptop computer issued by the agency)** | | | **C** | **I** | **A** | **P** | **D** | **R** | **O** | **L** | **P** |
| | *Category 1: General controls* | | | | | | | | | | |
| | D1.1 | Implement a standard technical configuration | V | V | V | V | | | V | V | V |
| | D1.2 | Use telework computers of sufficient technical specification | | V | V | V | | | V | | V |
| | D1.3 | Use reliable hardware and software | V | V | V | V | | | V | V | V |
| | D1.4 | Preinstall and -configure software | V | V | V | V | V | V | V | V | |
| | | | | | | | | | | | |
| | *Category 2: Software controls* | | | | | | | | | | |
| | D2.1 | Implement anti-malware software | V | V | V | V | V | V | | V | |
| | D2.2 | Implement a personal firewall | V | V | V | V | V | V | | V | |
| | D2.3 | Automatically download and install updates and patches | V | V | V | V | | | | V | |
| | D2.4 | Implement screen notifications | V | V | V | V | | | | V | |
| | D2.5 | Implement an adequate log-on procedure | V | V | V | V | | | | V | |
| | D2.6 | Implement an authentication mechanism | V | V | V | V | | | | V | |
| | D2.7 | Ensure the use of strong passwords | V | V | V | V | | | | V | |
| | D2.8 | Ensure regular password change | V | V | V | V | | | | V | |
| | D2.9 | Ensure the computer is only bootable from specified media | V | V | V | V | | | | V | |
| | D2.10 | Implement automatic access lock | V | V | V | V | | | | V | |
| | D2.11 | Automatically encrypt data on the hard disk | V | V | | V | | | | V | |
| | D2.12 | Implement automatic power-safe | | V | V | V | V | | | V | |
| | D2.13 | Implement device lock software | V | V | V | V | V | | | V | |
| | D2.14 | Implement an URL filter | V | V | V | V | V | | | V | |
| | D2.15 | Prevent installation of unauthorized software | V | V | V | V | V | | | V | |
| | D2.16 | Securely store passwords and cryptographic keys | V | V | V | V | | | | V | |
| | D2.17 | Implement anti-theft tracking software | V | V | V | | | V | | V | |
| | D2.18 | Automatically back-up data on the hard disk | | V | V | | | V | | V | |
| | | | | | | | | | | | |
| | *Category 3: Hardware controls* | | | | | | | | | | |
| | D3.1 | Equip computers with a travel pack | V | V | V | V | | | | | V |
| | D3.2 | Label computers with an anonymous telephone number | V | | V | | | V | | | V |
| | D3.3 | Provide computers with a serial number | V | | V | V | | V | | | V |
| | D3.4 | Implement alarm systems and motion detectors | V | V | V | V | V | V | | | V |
| | D3.5 | Mark computer with an anti-theft sticker | V | V | V | V | | V | | | V |
| | D3.6 | Limit the physical availability of ports and drives | V | V | V | V | | | | | V |

| | | | Why | | | When | | | What | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Group E: Controls connection** | | | **C** | **I** | **A** | **P** | **D** | **R** | **O** | **L** | **P** |
| | E1 | Manage Internet Access Providers | | V | V | V | | V | V | | |
| | E2 | Provide multiple lines to different telephone exchanges | | | V | | | V | | | V |
| | E3 | Safeguard the confidentiality of data in transit | V | | | V | | | | V | |
| | E4 | Prevent connection hijacking | V | V | V | V | | | | V | |
| | E5 | Automatically terminate unused connections | V | V | V | V | V | | | V | |
| | E6 | Restrict the number of simultaneously open connections | | | V | V | | | | V | |

| | | | Why | | | When | | | What | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Group F: Controls remote access farm** | | | **C** | **I** | **A** | **P** | **D** | **R** | **O** | **L** | **P** |
| | *Category 1: Software controls* | | | | | | | | | | |
| | F1.1 | Implement and maintain anti-malware software and firewalls | V | V | V | V | V | V | V | V | |
| | F1.2 | Implement an adequate log-on procedure | V | V | V | V | | | | V | |
| | F1.3 | Implement an authentication mechanism | V | V | V | V | | | | V | |
| | F1.4 | Ensure the use of strong passwords | V | V | V | V | | | | V | |
| | F1.5 | Ensure regular password change | V | V | V | V | | | | V | |
| | F1.6 | Implement teleworker access rights | V | V | V | V | | | V | V | |
| | F1.7 | Restrict access to authorized computers | V | V | V | V | | | | V | |
| | F1.8 | Apply load balancing techniques | | | V | V | | | | V | |
| | F1.9 | Log security relevant actions | V | V | V | | V | V | V | V | |
| | F1.10 | Back-up data on the remote access farm | | V | V | | | V | V | V | |
| | | | | | | | | | | | |
| | *Category 2: Hardware controls* | | | | | | | | | | |
| | F2.1 | Physically secure the remote access farm | V | V | V | V | | | | | V |
| | F2.2 | Implement and maintain a redundant remote access farm | | | V | | | V | V | | V |

## Control boxes

### Group A: General controls

*Category 1: Policy and standards*

| **Control A1.1** | **Develop and implement a security policy for teleworking** |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>**O** L P | A clear and unambiguous security policy for teleworking should be developed and implemented. Management should approve and actively support this policy to increase its effectiveness.<br><br>The security policy might be part of the agency's general information security policy. It should be evaluated periodically and adjusted to the environment.<br><br>The security policy for teleworking may contain the following:<br>▪ A description of the policy's scope.<br>▪ A definition of the term "teleworking".<br>▪ An overview of the locations from where teleworking may or may not take place.<br>▪ An overview of telework equipment that may or may not be used at a remote location.<br>▪ A specification of minimum (technical) requirements for telework equipment.<br>▪ A specification of times on which teleworking is allowed.<br>▪ A specification of types of information that may or may not be used while teleworking.<br>▪ A description of the way in which telework requests are processed and the role information security plays in this process.<br>▪ A high-level description of relevant information security risks related to teleworking.<br>▪ A high-level description of the most important information security controls related to teleworking.<br>▪ A description of the agency's and the teleworker's responsibilities for information security issues related to teleworking (e.g. the implementation of security controls).<br>▪ A description of actions that need to be performed by agency and/or the teleworker in the event of telework security breaches (e.g. the teleworker should immediately report serious breaches to line management).<br>▪ A description of possible sanctions as a result of negligence or a violation of the policy by the teleworker.<br><br>All teleworkers should receive a copy of the security policy for teleworking. |

| Control A1.2 | Manage telework requests |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>**O** L P | An employee should formally submit a request for teleworking to his line manager.<br><br>The line manager may grant or deny the request, taking for example the following into consideration:<br>▪ The significance of teleworking for the agency and/or the teleworker<br>▪ The associated security risks and costs.<br><br>A detailed procedure should be described and implemented for the assessment of telework requests. The actual assessment may take place on an individual basis or be associated with a particular job role or function.<br><br>*R&R*<br>*Raamregeling Telewerken (article 4): The civil servant who wants to telework for one or more days per week can submit an application to an authorized party. An application can be approved if that is in the interest of the agency.* |

| Control A1.3 | Develop and implement a telework agreement |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>**O** L P | Clear, documented agreements with teleworkers should be developed and implemented to ensure they understand their responsibilities and obligations.<br><br>Telework agreements should include, amongst other things, a description of the most important security risks related to teleworking and the teleworker's responsibilities in mitigating these risks.<br><br>The telework agreement should be signed by both a representative of the agency (e.g. a line manager) and the teleworker. Telework agreements typically supplement contracts of employment.<br><br>*R&R*<br>*Raamregeling Telewerken (article 5): Agreements with the teleworker are put in writing. Such agreements must include amongst other things:*<br>▪ *The telework facilities (e.g. computers) to be provided to the teleworker*<br>▪ *Information security*<br>▪ *The grounds on which and the way in which a telework agreement should be ended*<br>▪ *The consequences that the ending of a telework agreement has on provided telework facilities* |

*Category 2: Authorization*

| **Control A2.1** | **Formally authorize teleworkers** |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>**O** L P | Management should formally authorize teleworkers to certain applications or information.<br><br>Authorizations may be allocated on a case-by-case basis or per group of teleworkers. All authorizations should be documented and evaluated periodically.<br><br>In case a teleworker changes position or leaves the agency authorizations should immediately be reassessed and changed appropriately.<br><br>*R&R*<br>*VIR-BI (Restricted+): Authorizations of all users are recorded.*<br>*VIR-BI (Restricted+): Information is only taken outside a controlled area if that is necessary for the continuation of work activities and if the line manager has given a written approval.*<br>*VIR-BI (Top Secret): Information is not taken home or to a foreign country. A connection with the internal network is not allowed.* |

| **Control A2.2** | **Approve remote locations** |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>**O** L P | Where the teleworker will be working from a fixed location (e.g. at his home), the location should be periodically reviewed and approved. This should be done in consultation with the location's owner (e.g. the teleworker).<br><br>The review may include:<br>▪ Compliance with legislation, such as ARBO.<br>▪ Physical security measures in place, such as burglar alarms, safes, smoke detectors etc.<br>▪ The reliability and security of local networks (e.g. wireless networks) and Internet connections. |

| **Control A2.3** | **Approve telework computers** |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>**O** L P | Telework computers should be periodically reviewed and approved. This should include telework computers that are not provided by the agency.<br><br>Telework hardware should be reliable and of sufficient technical specification. Software, such as the operating system, anti-malware software, personal firewalls, email clients and browsers, should be up-to-date, configured correctly and run properly. |

*Category 3: System and network management*

| **Control A3.1** | **Maintain adequate documentation of the telework service** |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** **D** **R**<br>*Sphere of action (what)*<br>**O** L P | Up-to-date documentation of all key components of the telework service should be in place.<br><br>This documentation should include all information necessary to recover from a disaster, such as:<br>▪ Type of asset (e.g. information, hardware, software etc.)<br>▪ Details of the asset (e.g. serial numbers)<br>▪ Location<br>▪ Teleworker assigned to (if applicable)<br>▪ Date assigned (if applicable)<br><br>The inventory should not duplicate other inventories unnecessarily, but it should be ensured that the content is aligned.<br><br>*R&R*<br>*VIR-BI (Restricted+): Register hard- and software configurations.*<br>*VIR-BI (Secret): Register which person has the information at his disposal.* |

| **Control A3.2** | **Manage authentication tools** |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>**O** **L** **P** | The allocation, maintenance, physical/logical storage, withdrawal/destruction and administration of authentication tools (e.g. passwords and tokens) should be described by formal procedures.<br><br>These procedures should be periodically tested and adequate segregation of duties should be realized. |

| **Control A3.3** | **Manage cryptographic keys** |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>**O** **L** **P** | All cryptographic keys should be protected against modification, loss, and destruction. In addition, secret and private keys need protection against unauthorized disclosure and the authenticity of public keys needs to be safeguarded (e.g. by means of certifying authorities).<br><br>A key management system should be based on an agreed set of standards, procedures, and secure methods for (amongst other things):<br>▪ Generating keys.<br>▪ Distributing keys.<br>▪ Storing keys.<br>▪ Dealing with compromised keys.<br>▪ Changing and updating keys.<br>▪ Archiving keys.<br>▪ Revoking and destroying keys.<br><br>In order to reduce the likelihood of compromise, activation, and deactivation dates for keys should be defined so that the keys can only be used for a limited period of time.<br><br>*R&R*<br>*VIR-BI (Restricted+): The distribution of keys has to be registered and keys that are not in use have to be stored securely. Only certified keys are used.* |

| Control A3.4 | Monitor audit logs |
|---|---|
| *Security attributes (why)*<br>**C** I **A**<br>*Place in event cycle (when)*<br>P **D** R<br>*Sphere of action (what)*<br>**O** L P | All audit logs concerning the remote access farm should be periodically analyzed to identify actual or attempted security breaches or any access outside agreed terms. Peculiarities should be reported.<br><br>Where necessary system administrators should be trained in the interpretation of system logs. |

| Control A3.5 | Monitor performance levels |
|---|---|
| *Security attributes (why)*<br>C I **A**<br>*Place in event cycle (when)*<br>P **D** R<br>*Sphere of action (what)*<br>**O** L P | The performance of the remote access farm should be monitored to identify potential bottlenecks and overloads and to enable remedial action to be taken before they materialize.<br><br>Network monitoring tools may be used to measure traffic levels and call logs may be analyzed to determine the frequency of use and the duration of access. |

*Category 4: User support*

| Control A4.1 | Provide helpdesk support to teleworkers |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** **D** **R**<br>*Sphere of action (what)*<br>**O** L P | Where teleworking is implemented on a large scale, a helpdesk should be establish which provides 'first line' support to teleworkers. 'Out of office hours' helpdesk support should be considered if a considerable part of the teleworking workforce works outside office hours.<br><br>The helpdesk may form part of a larger agency-wide facility and should have access to technical and business experts who will be able to respond quickly and effectively to problems.<br><br>In case teleworking is only implemented on a small scale, responsibility for supporting teleworkers should be assigned to one or more individuals. Those individuals should be available to provide technical support and answer queries within a reasonable timescale. They should also have access to sufficient technical expertise to deal with more complex problems, should they arise. |

| Control A4.2 | Provide security software |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** **D** **R**<br>*Sphere of action (what)*<br>**O** **L** P | Where telework equipment is not provided by the agency, proper security software such as anti-malware software and personal firewalls should be made available to teleworkers.<br><br>Teleworkers should also receive adequate documentation and/or oral clarification on how to use such software. In order to encourage teleworkers to make use of security software it should be available for free. |

| Control A4.3 | Log all incidents |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** **D** **R**<br>*Sphere of action (what)*<br>**O** **L** P | Incidents such as malfunctions, loss of power, mistakes by teleworkers or computer staff and security breaches, should be dealt with in accordance with a formal process.<br><br>Incidents should be:<br>▪ Identified<br>▪ Reported to a focal port (e.g. a 24-hour helpline)<br>▪ Logged (e.g. for trend analysis)<br>▪ Prioritised for action<br>▪ Resolved on a timely basis |

| Control A4.4 | Ensure the proper return of telework equipment |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>**O** L P | All teleworkers should return all of the agency's equipment in their possession upon termination of the telework agreement and/or their employment.<br><br>In cases where a teleworker takes over the agency's equipment or uses their own personal equipment, procedures should be followed to ensure that all relevant information is transferred to the organization and securely erased from the equipment. |

| Control A4.5 | Securely dispose or re-use telework equipment |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>**O** L P | All telework computers should be checked to ensure that any sensitive data (and licensed software) has been removed or securely overwritten prior to disposal or re-use.<br><br>Devices containing sensitive information should be physically destroyed or the information should be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function.<br><br>Damaged devices containing sensitive data may require a risk assessment to determine whether the items should be physically destroyed rather than sent for repair or discarded.<br><br>*R&R*<br>*VIR-BI (Restricted+): Information on data carriers that are going to be disposed needs to be removed using a method that suits the classification of the information in question.* |

| Control A4.6 | Report stolen telework equipment |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>P **D** R<br>*Sphere of action (what)*<br>**O** L P | Stolen telework equipment (e.g. mobile computers) should be immediately reported to the police and the manufacturer, not only for insurance or warranty purposes, but also to aid recovery.<br><br>The police may be able to recover a stolen computer if they are in possession of its serial number and if that computer is properly security marked. A manufacturer may be able to 'flag' a computer if a thief ever sends it in for maintenance. |

## Group B: Controls teleworker

*Category 1: Code of conduct and guidelines*

| **Control B1.1** | **Develop a code of conduct for teleworking** |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>**O** L P | A code of conduct should be developed in which 'appropriate behaviour' of teleworkers with respect to information security, is described.<br><br>A code of conduct for teleworking may contain the following:<br>▪ A description of the code of conduct's scope.<br>▪ A description of the code of conducts' goal.<br>▪ A definition of the term 'teleworking'.<br>▪ A broad description of the teleworker's responsibilities with respect to information security put down in the 'general line of conduct'.<br>▪ A detailed elaboration on these responsibilities put down in 'rules of conduct' or guidelines. Rules of conduct may concern for example:<br>o Malware prevention and back-up.<br>o Equipment theft prevention.<br>o The use of unauthorized software<br>o Internet and email usage<br>▪ Possible consequences of behaviour that violates the code of conduct.<br><br>*R&R*<br>*Algemene Rijksambtenarenreglement (article 50): A civil servant should always conduct appropriate behaviour. (A code of conduct for teleworking can implement this prescript by further specifying what 'appropriate behaviour' with respect to teleworking actually is.)* |

| **Control B1.2** | **Establish guidelines for using sensitive agency information** |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>**O** L P | Guidelines should be established that communicate restrictions put on teleworking with sensitive agency information, such as rubricaded data, personal data or financial data.<br><br>Examples of such guidelines are:<br>▪ Do not telework with certain classes of agency information (e.g. 'top secret' information)<br>▪ Do not process sensitive agency information on computers that are publicly available (e.g. in Internet cafes).<br>▪ Sufficiently remove all agency information on computers when the contract of employment has ended.<br>▪ Sufficiently remove all agency information on computers that are sold, thrown away or going to be repaired by third parties. |

| Control B1.3 | Establish guidelines for non-work-related use of computers |
|---|---|
| *Security attributes (why)*<br>**C** I **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>**O** L P | Non-work-related use of telework computers, by the teleworker and/or third parties, should be discouraged or prohibited if it introduces unacceptable security risks.<br><br>Guidelines should be established that communicate the agency's standpoint on non-work-related use of agency computers. This standpoint may be:<br>▪ To fully allow non-work-related use of agency computers.<br>▪ To only allow non-work-related use of agency computers insofar it does not conflict with business interests.<br>▪ To disallow non-work-related use of agency computers. |

| Control B1.4 | Establish guidelines for using wireless networks |
|---|---|
| *Security attributes (why)*<br>**C** I **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>**O** L P | The use of wireless networks should be should be discouraged or prohibited if it introduces unacceptable security risks.<br><br>Guidelines should be established that reflect the agency's standpoint on the use of wireless networks. This standpoint may be:<br>▪ The use of wireless networks is allowed.<br>▪ The use of wireless networks is only allowed if the teleworker does not work with information that is too sensitive.<br>▪ The use of wireless networks is not allowed.<br><br>In case the agency allows the use of wireless networks, the following guidelines may for example be issued:<br>▪ Use trustworthy wireless routers (the agency may recommend certain routers or issue preconfigured routers).<br>▪ Properly configure the wireless router to avoid eavesdropping and unauthorized access to the telework computer (make use of manuals provided by the manufacturer and/or directions from agency).<br>▪ Only connect the telework computer to known and/or trusted wireless networks. |

| Control B1.5 | Establish guidelines for using anti-malware softw. and firew. |
|---|---|
| *Security attributes (why)*<br>**C** I **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>**O** L P | Guidelines should be established that concern the use of anti-malware software and firewalls on telework computers.<br><br>Examples of such guidelines are:<br>▪ Use trustworthy anti-malware software and personal firewalls (the agency may recommend or provide certain security software).<br>▪ Properly install and configure anti-malware software and personal firewalls (make use of the manual provided by the maker and/or directions from the agency). |

| Control B1.6 | Establish guidelines for taking back-ups |
|---|---|
| *Security attributes (why)*<br>**C** I **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>**O** L P | Guidelines should be established that concern the back-up of information and software on telework computers.<br><br>Examples of such guidelines are:<br>▪ Back-up information and software on a regular basis (e.g. every week).<br>▪ Use trustworthy software and devices for taking back-ups (the agency may recommend or provide certain software devices).<br>▪ Store back-ups at secure locations to protect them from damage or theft (e.g. a safe).<br>▪ Safeguard the confidentiality of back-ups by means of encryption. |

| Control B1.7 | Establish guidelines for using portable data carriers |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>**O** L P | Guidelines should be established for the use of portable data carriers by teleworkers.<br><br>Examples of such guidelines are:<br>▪ Do not access portable data carriers (e.g. floppy disks or memory sticks) that come from an unknown or untrusted source.<br>▪ Use anti-malware software to scan the contents of portable data carriers, before they are accessed.<br>▪ Do not open unknown or untrusted files stored on portable data carriers. |

| Control B1.8 | Establish guidelines for using the Internet |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>**O** L P | Guidelines should be established for the use of the Internet by teleworkers.<br><br>Examples of such guidelines are:<br>▪ Do not access unknown or untrusted websites.<br>▪ Do not download files or software from the Internet unless the source is trusted. Be especially careful with shareware programs.<br>▪ Use anti-malware software to scan all downloaded files before opening.<br>▪ Do not install and use peer-to-peer file sharing programs such as Limewire or Kazaa.<br>▪ Disable scripting features in web browsers (e.g. Java, JavaScript and ActiveX).<br>▪ Do not wittingly allow untrusted parties to take remote control over the telework computer.<br>▪ Use robust Internet connections that are provided by a reliable Internet Access Provider. |

| Control B1.9 | Establish guidelines for using email |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>**O** L P | Guidelines should be established for the use of email by teleworkers.<br><br>Examples of such guidelines are:<br>▪ Do not open files attached to e-mail messages unless the source is trusted. Be especially cautious with executable files (.exe) or Microsoft Word documents (.doc).<br>▪ Never send sensitive agency information through open, unencrypted e-mail.<br>▪ Disable scripting features in email clients.<br>▪ Use anti-malware software to scan email attachments before opening. |

| Control B1.10 | Establish guidelines for using authentication means |
|---|---|
| *Security attributes (why)*<br>**C** \| **I** \| **A**<br>*Place in event cycle (when)*<br>**P** \| D \| R<br>*Sphere of action (what)*<br>**O** \| L \| P | Guidelines should be established that communicate the proper use of authentication means (e.g. passwords and tokens) that are used to gain access to the remote access farm or telework equipment.<br><br>Examples of such guidelines are:<br>▪ Use passwords that are easy to remember.<br>▪ Use passwords that are sufficiently 'strong'.<br>▪ Change passwords on a regular basis or whenever there is any indication of possible password compromise.<br>▪ Do not base passwords on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers, and dates of birth.<br>▪ Keep passwords confidential. Do not write passwords down or electronically store them in unencrypted form.<br>▪ Choose unique passwords i.e. do not use them for any other purposes.<br>▪ Store tokens and associated PINs at separate locations or destroy PINs.<br>▪ Ensure certificates are securely stored.<br>▪ Do not share any authentication means with other parties, even if those parties seem to be trustworthy.<br><br>*R&R*<br>*VIR-BI (Confidential+): Passwords are changed frequently (every 30 days).*<br>*VIR-BI (Restricted+): Passwords are treated in such a way that they cannot be compromised.* |

| Control B1.11 | Establish guidelines to prevent theft |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>**O** L P | Guidelines that inform the teleworker on how to prevent or deal with theft or loss of telework computers and the information they contain should be established.<br><br>Examples of such guidelines are:<br>*Equipment*<br>▪ Always keep an eye on the mobile computer in public places.<br>▪ When travelling, keep the mobile computer at hand at all times. Do not leave it on empty seats in busses or trains.<br>▪ Use a cable locking device when the mobile computer is left unattended, even if the computer is located in a locked room.<br>▪ Avoid leaving mobile computers in hotel rooms. If that is not possible keep the mobile computer out of sight. Lock it in another piece of luggage or have it put in the hotel's safe or room safe.<br>▪ Whenever possible do not leave the mobile computer in a vehicle. If it must be stored in a car make sure it is in the trunk or under the seat where it is not visible. Extreme temperature ranges within the vehicle could spell trouble for the mobile computer. The summer heat inside a parked car could reach temperatures that will melt computer components. In the winter, LCD screens can freeze solid and split.<br>▪ Do not carry mobile computers in a clearly definable computer case. Use a normal backpack or shoulder bag instead. Make sure the carrying case is sturdy and weatherproof.<br>▪ Supervise third party visitors in the remote environment.<br>▪ Immediately report theft or loss of mobile computers to the agency and/or the police.<br><br>*Information*<br>▪ Keep screens of telework computers out of view. Do not process sensitive information in public places and keep screens away from windows.<br>▪ Always log-off telework computers or disconnect them from the remote access farm when they are not in use.<br>▪ Sufficiently encrypt sensitive information stored on telework computers. |

| Control B1.12 | Establish guidelines for securing the remote location |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>**O** L P | Guidelines should be established concerning the physical security of the remote location in order to protect telework computers from theft or damage.<br><br>Examples of such guidelines are:<br>▪ Properly construct the remote location.<br>▪ Install a burglar alarm.<br>▪ Install a secure safe.<br>▪ Install smoke detectors.<br>▪ Install fire extinguishers.<br>▪ Install lightening protection. |

| Control B1.13 | Provide copies of the code and guidelines to teleworkers |
|---|---|
| *Security attributes (why)*<br>**C** I **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>**O** L P | All teleworkers should receive a copy of the code of conduct and relevant guidelines when they first start teleworking or in case the code of conduct and/or guidelines have changed.<br><br>Possible consequences of behaviour that violates the code of conduct and/or guidelines should also be put in writing and sufficiently communicated to all teleworkers. |

*Category 2: Security awareness*

| Control B2.1 | Distribute awareness material |
|---|---|
| *Security attributes (why)*<br>**C** I **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>**O** L P | Material aimed at making teleworkers aware of security risks associated with teleworking should be distributed to all teleworkers.<br><br>This may be done by means of an awareness campaign that is aimed at promoting good teleworking practice among all teleworkers. Such a campaign may include the production of brochures and posters, displayed in prominent places. |

| Control B2.2 | Provide security awareness training |
|---|---|
| *Security attributes (why)*<br>**C** I **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>**O** L P | All teleworkers should periodically receive appropriate security awareness training. The first training should be given before they actually start teleworking.<br><br>Security awareness trainings are intended to educate teleworkers in the correct and safe use of the telework facility. Teleworkers should be made aware of security risks associated with teleworking and their own responsibilities for reducing those risks.<br><br>Teleworkers should also be trained to recognize information security incidents and to respond in an appropriate way (i.e. using the proper channels). They should know who to contact for further security advice (e.g. the helpdesk).<br><br>Security awareness trainings should be supported by comprehensive documentation. This includes the security policy, code of conduct and/or guidelines. |

## Group C: Controls telework location (Controls aimed at protecting a teleworker's home)

| Control C1 | Properly construct the remote location |
|---|---|
| *Security attributes (why)*<br>**C** I **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>O L **P** | The external walls of a remote location should be of solid construction and all external doors and windows should be suitably protected.<br><br>This should prevent intruders from gaining access to telework equipment or delay them in such a way that timely intervention can take place.<br><br>*R&R*<br>*VIR-BI (Confidential+): The room in which special information is located has to offer sufficient physical protection.* |

| Control C2 | Install a burglar alarm |
|---|---|
| *Security attributes (why)*<br>**C** I **A**<br>*Place in event cycle (when)*<br>P **D** **R**<br>*Sphere of action (what)*<br>O L **P** | A burglar alarm should be installed at the remote location to detect intruders who attempt to break into the remote location and to ensure intervention takes place on time.<br><br>An alarm basically consists of a central control box that monitors several motion detectors and perimeter guards. Once an intruder is detected an alarm may:<br>▪ Activate a loud alarm noise or flashing outdoor lights to alert occupants, neighbours and the police that someone has broken into the building and to scare the intruder away and/or<br>▪ Automatically dial the police or the security company that installed the equipment.<br><br>*R&R*<br>*VIR-BI (Restricted): The security is realized in such a way that unauthorized access is detected.*<br>*VIR-BI (Confidential+): The security is realized in such a way that unauthorized access is detected and timely intervention takes place.* |

| Control C3 | Install a secure safe |
|---|---|
| *Security attributes (why)*<br>**C** I **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>O L **P** | A secure safe should be installed at the remote location to protect telework equipment (e.g. computers and back-up media) from theft or damage.<br><br>The safe should prevent a burglar from getting to its contents or delay him in such a way that timely intervention can take place. Besides that a safe should be sufficiently resistant to fire, water and dust.<br><br>*R&R*<br>*VIR-BI (Restricted+): Data carriers that contain unencrypted special information have to be stored in a sufficiently secure storage facility when the workplace is left.* |

| Control C4 | Install smoke detectors |
|---|---|
| *Security attributes (why)*<br>C **I** **A**<br>*Place in event cycle (when)*<br>P **D** R<br>*Sphere of action (what)*<br>O L **P** | Smoke detectors should be installed at the remote location to detect airborne smoke and subsequently alert nearby people (by means of a very loud electronic horn) to the danger of fire.<br><br>If smoke detectors go off in time and are noticed soon, nearby people might be able to prevent or restrict fire damage to telework equipment. |

| Control C5 | Install sprinklers |
|---|---|
| *Security attributes (why)*<br>C **I** **A**<br>*Place in event cycle (when)*<br>P **D** **R**<br>*Sphere of action (what)*<br>O L **P** | In addition to smoke alarms, fire sprinklers should be installed to limit the size and impact of a fire in case nobody timely responds to smoke alarms.<br><br>Sprinklers may however cause water damage to telework equipment. |

| Control C6 | Install fire extinguishers |
|---|---|
| *Security attributes (why)*<br>C **I** **A**<br>*Place in event cycle (when)*<br>P D **R**<br>*Sphere of action (what)*<br>O L **P** | Fire extinguishers should be in place to enable people at the remote location to timely put out a fire in order to prevent or restrict fire damage to telework equipment.<br><br>It is important for users to familiarise themselves with the use of fire extinguishers in their vicinity, because improper or untimely use may be counterproductive. |

| Control C7 | Install lightening protection |
|---|---|
| *Security attributes (why)*<br>C **I** **A**<br>*Place in event cycle (when)*<br>P D **R**<br>*Sphere of action (what)*<br>O L **P** | Lightening protection should be in place to prevent damage to telework computers as a result of a stroke of lightening.<br><br>There are various sorts of lightening protection systems. They generally are designed to provide a designated path for the lightning current to travel so that it does cause damage to electronic devices. |

## Object D: Telework equipment
## (Controls aimed at protecting a laptop computer issued by the agency)

*Category 1: General controls*

| **Control D1.1** | **Implement a standard technical configuration** |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>**O** **L** **P** | Telework equipment should be standardised as much as possible in order to simplify maintenance and remove the need to perform an individual review of every remote technical environment.<br><br>Ideally all teleworkers should be provided with the same type of hardware (e.g. laptop computers and Internet access devices) and consistent versions of software (e.g. standard operating systems, applications and security software). |

| **Control D1.2** | **Use telework computers of sufficient technical specification** |
|---|---|
| *Security attributes (why)*<br>C **I** **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>**O** L **P** | Telework computers provided by the agency should satisfy certain technical requirements to enable the teleworker to work effectively.<br><br>Computers should for example be equipped with a sufficiently fast processor, have enough internal memory and adequate hard disk space.<br><br>If access to the remote access farm is required, telework computers should be equipped with Internet access devices (e.g. modems or wireless adaptors) that suit the way in which the Internet can be accessed at relevant remote locations. |

| **Control D1.3** | **Use reliable hardware and software** |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>**O** **L** **P** | High priority should be given to reliability in selecting hardware and software that will be issued to teleworkers.<br><br>All hard and software should be:<br>▪ Of the highest quality possible.<br>▪ Purchased from a reputable supplier.<br>▪ Up-to-date (i.e. not obsolete).<br>▪ Compatible with each other. |

| **Control D1.4** | **Preinstall and -configure software** |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** **D** **R**<br>*Sphere of action (what)*<br>**O** **L** P | Software on telework computers should be correctly preinstalled and -configured.<br><br>This includes for example the BIOS, logical access control, the operating system, device drivers, Internet browsers, anti-malware software, personal firewalls and user applications. Teleworkers should not be able to change important configuration settings or install unauthorized software.<br><br>Applications (and information) to which the teleworker is not authorized should not be preinstalled on telework equipment. |

*Category 2: Software controls*

| Control D2.1 | Implement anti-malware software |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** **D** **R**<br>*Sphere of action (what)*<br>O **L** P | Proper anti-malware software should be installed on the telework computer to identify, thwart and eliminate computer viruses and other malware.<br><br>Such software should both scan files to look for known malware matching definitions in a malware dictionary and identify suspicious behaviour from any computer program which might indicate infection. |

| Control D2.2 | Implement a personal firewall |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** **D** **R**<br>*Sphere of action (what)*<br>O **L** P | A proper personal firewall should be installed on telework computers to control communication to and from the telework computer.<br><br>A personal firewall should also provide some level of intrusion detection, allowing the software to terminate or block connectivity where it suspects an intrusion is being attempted. |

| Control D2.3 | Automatically download and install updates and patches |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>O **L** P | Important software updates and patches should be automatically downloaded and installed on the telework computer for example when the teleworker accesses the Internet or the agency's network.<br><br>This should at least include updates and patches for the operating system, anti-malware software, personal firewalls and web browsers. |

| Control D2.4 | Implement screen notifications |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>O **L** P | Before a user logs-on to a telework computer, a warning should appear on its screen which indicates that unauthorized access is prohibited and liable to punishment.<br><br>Warning screens may also be implemented, in for example screen savers, to remind the teleworker of important information security issues.<br><br>*R&R*<br>*VIR-BI (Restricted+): The first screen mentions that unauthorized access is prohibited by law.* |

| Control D2.5 | Implement an adequate log-on procedure |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>O **L** P | The procedure for logging into the telework computer should be designed to minimize the opportunity for unauthorized access.<br><br>A good log-on procedure should for example:<br>▪ Disclose only the minimum of information about the system.<br>▪ Not provide help messages during the log-on procedure that would aid an unauthorized user.<br>▪ Validate the log-on information only on completion of all input data. If an error condition arises, the system should not indicate which part of the data is correct or incorrect.<br>▪ Limit the number of unsuccessful log-on attempts allowed, e.g. to three attempts, or force a time delay before further log-on attempts are allowed.<br>▪ Not display the password being entered or hide the password characters by symbols.<br>▪ Limit the maximum and minimum time allowed for the log-on procedure. If exceeded, the system should terminate the log-on.<br><br>*R&R*<br>*VIR-BI (Restricted+): The log-on dialogue does not help unauthorized parties to gain access.*<br>*VIR-BI (Restricted): The number of failed log-on attempts is limited to five.*<br>*VIR-BI (Confidential+): The number of failed log-on attempts is limited to three and exceeding this limit leads to definitive blockage of access.* |

| Control D2.6 | Implement an authentication mechanism |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>O **L** P | An authentication mechanism should be implemented that forces a user to prove his identity in order to access the telework computer.<br><br>Normally the authentication mechanism is implemented at the operating system level, but it may also be implemented before the boot process (i.e. pre-boot authentication).<br><br>Although authentication to telework computers is usually based on only one factor (i.e. 'what the teleworker knows'), the inclusion of other factors (i.e. 'what the teleworker has' and/or 'who the teleworker is') may also be considered.<br><br>*R&R*<br>*VIR-BI (Restricted+): Users have to be identified and authenticated in advance.*<br>*VIR-BI (Secret): Users have to be authenticated by means of a token or biometrics.* |

| Control D2.7 | Ensure the use of strong passwords |
|---|---|
| *Security attributes (why)*<br>**C** \| **I** \| **A**<br>*Place in event cycle (when)*<br>**P** \| D \| R<br>*Sphere of action (what)*<br>O \| **L** \| P | Mechanisms should be implemented that enforce the use of strong passwords for access to the telework computer.<br><br>Such mechanisms should make sure that passwords satisfy certain requirements, such as:<br>▪ A password should be of sufficient minimum length (e.g. eight or more characters).<br>▪ A password should not consist of words included in dictionaries.<br>▪ A password should be free of consecutive identical, all-numeric or all-alphabetic characters.<br>▪ A password should contain both small and capital letters as well as special characters (e.g. $&%). |

| Control D2.8 | Ensure regular password change |
|---|---|
| *Security attributes (why)*<br>**C** \| **I** \| **A**<br>*Place in event cycle (when)*<br>**P** \| D \| R<br>*Sphere of action (what)*<br>O \| **L** \| P | Mechanisms should be implemented that control the change of passwords used for access to the telework computer.<br><br>Such mechanisms should make sure that:<br>▪ Temporary passwords are changed at the first log-on.<br>▪ Passwords are changed at regular intervals (e.g. every 30 days) or based on the number of accesses.<br>▪ Old passwords are not reused or recycled.<br>▪ Passwords are changed whenever there is any indication of possible system or password compromise.<br><br>*R&R*<br>*VIR-BI (Confidential+): Passwords are changed frequently (every 30 days).* |

| Control D2.9 | Ensure the computer is only bootable from specified media |
|---|---|
| *Security attributes (why)*<br>**C** \| **I** \| **A**<br>*Place in event cycle (when)*<br>**P** \| D \| R<br>*Sphere of action (what)*<br>O \| **L** \| P | The telework computer should only be able to boot from specified media (e.g. its hard disk) and not from other – untrusted – data carriers (e.g. floppy disks or CDs).<br><br>Hereto the telework computer's BIOS should be properly configured. This is only effective if others cannot easily change the BIOS settings, therefore a password for entering the BIOS should be in place. |

| Control D2.10 | Implement automatic access lock |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>O **L** P | An automatic access lock should be implemented to prevent telework computers from remaining 'logged on' if they are not in use.<br><br>The automatic access lock should automatically 'lock' the computer after a short period of time or by order of the user. It should at least empty the computer screen (e.g. by running a screen saver), but it may also terminate running applications and/or network sessions.<br><br>The automatic access lock should only 'unlock' the computer after successful authentication of the teleworker.<br><br>*R&R*<br>*VIR-BI (Restricted+): Automatic access lock is automatically activated after pressing a key combination/mouse click or after a certain time (thirty, ten or five minutes).* |

| Control D2.11 | Automatically encrypt data on the hard disk |
|---|---|
| *Security attributes (why)*<br>**C** **I** A<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>O **L** P | Sensitive telework information stored on hard disks of telework computers should be automatically encrypted. This encryption should be sufficiently strong.<br><br>Encryption approaches include for example:<br>▪ Automatically encrypt all data on telework computers.<br>▪ Create encrypted folders for the storage of sensitive information. This approach requires less processor overhead (since the encryption will only operate when accessing sensitive data) and only requires user authentication for access to data in encrypted folders.<br><br>*R&R*<br>*VIR-BI (Restricted+): Information is stored in encrypted form. The encryption method (including key management) must suit the classification of the information in question.* |

| Control D2.12 | Implement automatic power-safe |
|---|---|
| *Security attributes (why)*<br>C **I** **A**<br>*Place in event cycle (when)*<br>**P** **D** R<br>*Sphere of action (what)*<br>O **L** P | Telework computers should automatically go into a power-safe modus (e.g. 'stand-by' or 'sleep') in case of imminent power shortage.<br><br>An actual power shortage will abruptly turn off telework computers and that may lead to the loss of valuable data. This can be prevented by switching telework computers into a power-safe modus just before batteries run down.<br><br>If a battery reaches a certain lower limit while the telework computer is in power-safe modus, the computer should 'awake' for a short period of time, safe all important data and subsequently shut down completely. |

| Control D2.13 | Implement device lock software |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** **D** R<br>*Sphere of action (what)*<br>O **L** P | The use of external devices on telework computers should be controlled by means of device lock software.<br><br>With such software it is possible to control access to any device that may be used in combination with telework computers. The intention is to allow special devices (e.g. a mouse), but lock all other devices. |

| Control D2.14 | Implement an URL filter |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** **D** R<br>*Sphere of action (what)*<br>O **L** P | The availability of webpages accessible through telework equipment should be restricted by means of an URL filter.<br><br>An URL filter blocks web pages based on their URL. They can be configured in such a way that only specific web pages can be accessed or that certain (categories of) web pages can be blocked. |

| Control D2.15 | Prevent installation of unauthorized software |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** **D** R<br>*Sphere of action (what)*<br>O **L** P | The installation of unauthorized software (e.g. programs or malware) on telework computers should be prevented.<br><br>This may be realized by implementing security software that prevents the installation or launching of executables by means of white lists (that specify which executables may be run) black lists (that specify which executables may not be run) or heuristic techniques.<br><br>It may also be that software can only be installed and executed after it has been verified (e.g. by the operating system) that the software in question contains a valid digital signature. |

| Control D2.16 | Securely store passwords and cryptographic keys |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>O **L** P | Passwords (or equivalents) used to gain access to the remote access farm should only be stored on telework computers if they are sufficiently encrypted.<br><br>Operating systems and web browsers usually automatically store passwords by default. Since encryption used with automatic storage of passwords often has known vulnerabilities, it may be preferable to disable automatic storage.<br><br>If cryptographic keys are stored on telework computers, they should be stored securely.<br><br>*R&R*<br>*VIR-BI (Restricted+): Passwords are stored by means of a one-way hashing algorithm.*<br>*VIR-BI (Restricted+): Passwords are treated in such a way that they cannot be compromised.* |

| Control D2.17 | Implement anti-theft tracking software |
|---|---|
| *Security attributes (why)*<br>**C** I **A**<br>*Place in event cycle (when)*<br>P D **R**<br>*Sphere of action (what)*<br>O **L** P | Anti-theft tracking software should be installed on telework computers to aid its recovery in case of theft.<br><br>Such software runs inconspicuously in the background and usually uses the internet to (securely) send its location to a server or email address of a monitoring company. It may do this continuously or only when the laptop is reported stolen and a recovery effort is initiated.<br><br>Location information should enable the monitoring company (in cooperation with law enforcement) to recover a stolen mobile computer. |

| Control D2.18 | Automatically back-up data |
|---|---|
| *Security attributes (why)*<br>C **I** **A**<br>*Place in event cycle (when)*<br>P D **R**<br>*Sphere of action (what)*<br>O **L** P | Important data on the hard disks of telework computers should be backed-up automatically.<br><br>This may be realized by means of third party products that perform automatic back-ups whenever a connection to the Internet is detected. It may also be that a back-up of data automatically takes place when telework computers are connected to the remote access farm. |

*Category 3: Hardware controls*

| Control D3.1 | Equip telework computers with a travel pack |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>O L **P** | Telework computers should be equipped with a travel pack to protect them from theft and damage.<br><br>The pack should include for example:<br>▪ An inconspicuous travel bag that does not directly reveal its contents to others.<br>▪ Power adaptors.<br>▪ Batteries (one inside the mobile telework computer and a spare one, if necessary).<br>▪ Appropriate Internet access devices.<br>▪ A decent security cable with a lock to secure the telework computer when (temporarily) left unattended. Usually the lock is connected to a lock interface on the telework computer. This interface should destroy the computer in the event someone tries to break the lock. The computer's hard disk should not be easily removable or separately locked.<br>▪ A portable laptop safe that can be attached to any work surface. This also secures external devices, such as CD-ROM and portable data carriers. |

| Control D3.2 | Label computers with an anonymous telephone number |
|---|---|
| *Security attributes (why)*<br>**C** I **A**<br>*Place in event cycle (when)*<br>P D **R**<br>*Sphere of action (what)*<br>O L **P** | A label with an anonymous telephone number should be attached to all telework computers (and peripherals) to enable the finder to report its discovery.<br><br>This telephone number should be anonymous, because information about the owner of the computer may encourage a thief or finder to abuse the information it contains. The person that answers this number should therefore not reveal details about the agency.<br><br>Information about the agency should also not come available before completion of the authentication process (e.g. on log-on screens). |

| Control D3.3 | Provide computers with a serial number |
|---|---|
| *Security attributes (why)*<br>**C** I **A**<br>*Place in event cycle (when)*<br>**P** D **R**<br>*Sphere of action (what)*<br>O L **P** | A serial number should be available on telework computers (and peripherals) to aid identification in case of theft.<br><br>The serial number should be visibly etched on telework equipment, because marked equipment is less attractive to receivers of stolen goods and therefore to thieves.<br><br>A duplicate of the number should also be concealed so that equipment is still identifiable after the visible number has been erased. A number can for example be concealed by etching it on hidden places or by using ultra violet markings. |

| Control D3.4 | Implement alarm systems and motion detectors |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** **D** **R**<br>*Sphere of action (what)*<br>O L **P** | Alarm systems and motion detectors should be implemented on telework computers to alert the teleworker when the computer is moved.<br><br>There are several kinds of alarm systems available on the market. Examples are:<br>▪ Alarm systems that create a 'maximum separation zone'. If the teleworker moves out of range of his telework computer, or if the computer is moved out of range of the teleworker, an alarm will sound. The alarm will stop once the teleworker moves back within the range.<br>▪ Alarms systems rely on nothing more than movement of the object that it is attached to. If the object that the sensor is attached to is moved, an alarm will sound. Entering a security code will reset or disable the alarm once the device has been recovered.<br>▪ Alarm systems that passively monitor the position of a mobile computer. If the motion sensors detect that the laptop has been moved outside of the designated work zone, an alarm can sound or the computer can automatically lock or shut down. A (gesture) password can disarm the system. |

| Control D3.5 | Mark computer with an anti-theft sticker |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** D **R**<br>*Sphere of action (what)*<br>O L **P** | A mobile computer should be marked with an anti-theft sticker at a visible location to deter potential thieves from stealing the computer.<br><br>If stolen the sticker would be able to be removed, but it would leave a tattoo on the casing indicating stolen property. This will alert others that the mobile computer is stolen. |

| Control D3.6 | Limit the physical availability of ports and drives |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>O L **P** | The use of external devices on telework computers should be controlled by limiting the physical availability of hardware ports and removable media drives.<br><br>There are several ways to do this:<br>▪ Issue computers without relevant ports and removable media drives.<br>▪ Remove relevant ports and removable media drives.<br>▪ Seal relevant ports and removable media drives by using (physical) locking devices. |

## Group E: Controls connection

| Control E1 | Manage Internet Access Providers |
|---|---|
| *Security attributes (why)*<br>C **I** **A**<br>*Place in event cycle (when)*<br>**P** D **R**<br>*Sphere of action (what)*<br>**O** L P | Data communications services required from Internet Access Providers should be defined in formal agreements (e.g. service level agreements or contracts). Focal points of contact should be established so that changes can be made and incidents dealt with in a disciplined manner.<br><br>Optionally more than one Internet Access Provider could be used, so that in if one provider cannot provide sufficient Internet access the other can be used as an alternative. |

| Control E2 | Provide multiple lines to different telephone exchanges |
|---|---|
| *Security attributes (why)*<br>C I **A**<br>*Place in event cycle (when)*<br>P D **R**<br>*Sphere of action (what)*<br>O L **P** | The communications infrastructure from the remote access farm to the public Internet should be strengthened<br><br>This may be done by installing multiple lines to different telephone exchanges so that if one line or exchange fails, an alternative communications link is available. |

| Control E3 | Safeguard the confidentiality of data in transit |
|---|---|
| *Security attributes (why)*<br>**C** I A<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>O **L** P | Mechanisms should be implemented to ensure that the confidentiality of data in transit is not compromised.<br><br>Data communication between telework equipment and the remote access farm should be sufficiently end-to-end encrypted, using a strong cipher (e.g. AES) in combination with a strong and confidential encryption key (e.g. 128-bit).<br><br>*R&R*<br>*VIR-BI (Restricted+): Information that is spread through (external) networks is encrypted. The encryption method (including key management) must suit the classification of the information in question.* |

| Control E4 | Prevent connection hijacking |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>O **L** P | Mechanisms should be implemented to prevent connections from being hijacked.<br><br>Various defences against connection hijacking use authentication techniques that are based on for example strong mutual authentication to assure two communicating parties of each others identity. |

| Control E5 | Automatically terminate unused connections |
|---|---|
| *Security attributes (why)*<br>**C** I **A**<br>*Place in event cycle (when)*<br>**P** **D** R<br>*Sphere of action (what)*<br>O **L** P | Connections to the remote access farm should automatically be terminated if they are no longer in use.<br><br>Unused open connections unnecessarily confiscate resources on the remote access farm and introduce extra security risks related to unauthorized access because they can be misused by third parties.<br><br>The following approaches may be used to terminate connections:<br>▪ Terminate an individual connection if it has not been used for a certain period of time.<br>▪ Terminate all open connections at certain moments in time (e.g. at 12:00 pm), to prevent them from being open for too long (e.g. 24 hours). Teleworkers who have established an open connection at those moments and want to continue their work activities will have to log in again. |

| Control E6 | Restrict the number of simultaneously open connections |
|---|---|
| *Security attributes (why)*<br>C I **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>O **L** P | The number of simultaneously open connections to the remote access farm should be restricted to a certain maximum.<br><br>Open connections confiscate resources on the remote access farm. If there are too many simultaneously open connections, the work load of the remote access farm may become too high, which may lead to its unavailability. |

## Group F: Controls remote access farm

*Category 1: Software controls*

| **Control F1.1** | **Implement and maintain anti-malware software and firewalls** |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** **D** **R**<br>*Sphere of action (what)*<br>**O** **L** P | Adequate anti-malware software and firewalls (including intrusion detection systems) should be installed and running on the remote access farm. This software should be up-to-date and properly configured.<br><br>Firewalls may function as a security perimeter that separates different domains within the agency's computer network. If desired, a firewall may logically separate the remote access farm from the agency's internal network (demilitarized zone). |

| **Control F1.2** | **Implement an adequate log-on procedure** |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>O **L** P | The procedure for logging into the remote access farm should be designed to minimize the opportunity for unauthorized access.<br><br>A good log-on procedure should for example:<br>▪ Disclose only the minimum of information about the system.<br>▪ Display a general notice warning that the computer should only be accessed by authorized users.<br>▪ Validate the log-on information only on completion of all input data. If an error condition arises, the system should not indicate which part of the data is correct or incorrect.<br>▪ Limit the number of unsuccessful log-on attempts allowed, e.g. to three attempts, and consider:<br>o Recording unsuccessful and successful attempts.<br>o Forcing a time delay before further log-on attempts are allowed or rejecting any further attempts without specific authorization.<br>o Disconnect data connections.<br>▪ Not display the password being entered or hide the password characters by symbols.<br>▪ Not transmit passwords in clear text over a network.<br><br>*R&R*<br>*VIR-BI (Restricted+): The first screen mentions that unauthorized access is prohibited by law.*<br>*VIR-BI (Restricted+): The log-on dialogue does not help unauthorized parties to gain access.*<br>*VIR-BI (Restricted): The number of failed log-on attempts is limited to five.*<br>*VIR-BI (Confidential+): The number of failed log-on attempts is limited to three and exceeding this limit leads to definitive blockage of access.* |

| Control F1.3 | Implement an authentication mechanism |
|---|---|
| *Security attributes (why)*<br>**C** I **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>O **L** P | An authentication mechanism should be implemented that forces teleworkers to prove their identity before accessing the remote access farm.<br><br>Authentication to the remote access farm may be based on one or more of the following factors:<br>▪ 'What the teleworker knows' e.g. a username or password.<br>▪ 'What the teleworker has' e.g. a token.<br>▪ 'Who the teleworker is' i.e. biometric characteristics of the teleworker such as fingerprints.<br><br>*R&R*<br>*VIR-BI (Restricted+): Users have to be identified and authenticated in advance.*<br>*VIR-BI (Secret): Users have to be authenticated by means of a token or biometrics.* |

| Control F1.4 | Ensure the use of strong passwords |
|---|---|
| *Security attributes (why)*<br>**C** I **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>O **L** P | Mechanisms should be implemented that enforce the use of strong passwords for access to the remote access farm.<br><br>Such mechanisms should make sure that passwords satisfy certain requirements, such as:<br>▪ A password should be of sufficient minimum length (e.g. eight or more characters).<br>▪ A password should not consist of words included in dictionaries.<br>▪ A password should be free of consecutive identical, all-numeric or all-alphabetic characters.<br>▪ A password should contain both small and capital letters as well as special characters (e.g. $&%). |

| Control F1.5 | Ensure regular password change |
|---|---|
| *Security attributes (why)*<br>**C** I **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>O **L** P | Mechanisms should be implemented that control the change of passwords used for access to remote access farm.<br><br>Such mechanisms should make sure that:<br>▪ Temporary passwords are changed at the first log-on.<br>▪ Passwords are changed at regular intervals (e.g. every 30 days) or based on the number of accesses.<br>▪ Old passwords are not reused or recycled.<br>▪ Passwords are changed whenever there is any indication of possible system or password compromise.<br><br>*R&R*<br>*VIR-BI (Confidential+): Passwords are changed frequently (every 30 days).* |

| Control F1.6 | Implement teleworker access rights |
|---|---|
| *Security attributes (why)*<br>**C** I **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>**O** **L** P | The access rights of all teleworkers to applications and information on the remote access farm should be implemented in accordance with formal authorizations granted by management.<br><br>User tracking mechanisms should ensure that access rights are revoked or amended when necessary, particularly when remote users change roles, leave the agency, or when the telework agreement has ended.<br><br>*R&R*<br>*VIR-BI (Restricted+): Access rights of users are evaluated periodically (every 180, 90 or 30 days).* |

| Control F1.7 | Restrict access to authorized computers |
|---|---|
| *Security attributes (why)*<br>**C** I **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>O **L** P | Access to the remote access farm should only be granted to telework computers that satisfy certain conditions.<br><br>Examples of conditions for access are:<br>▪ Computers have to be provided by the agency. Hereto the identity of telework computers has to be verified for example by means of their IP-address.<br>▪ Correct software versions have to be installed on telework computers and they must run certain processes and not run certain other processes (e.g. malware). This can for example be checked by means of agent-based applications that run on the telework computer. |

| Control F1.8 | Apply load balancing techniques |
|---|---|
| *Security attributes (why)*<br>C I **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>O **L** P | Users of the remote access farm should automatically be divided over the available application servers in order to spread the workload.<br><br>Application servers that have the least workload in terms of for example memory and processor usage should be the first to run a new application. |

| Control F1.9 | Log security relevant actions |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>P **D** **R**<br>*Sphere of action (what)*<br>**O** **L** P | Audit logs that record activities of teleworkers and information security events should be produced and kept for an agreed period to assist in future investigations.<br><br>Audit logs should include for example:<br>▪ User IDs.<br>▪ Dates, times, and details of key events, e.g. log-on and log-off.<br>▪ Use of system utilities and applications.<br>▪ Files accessed and the kind of access.<br>▪ Alarms raised by the access control system.<br>▪ Alerts from firewalls and intrusion detection systems.<br><br>Audit logs should not be accessible by unauthorized parties. |

| Control F1.10 | Back-up data on the remote access farm |
|---|---|
| *Security attributes (why)*<br>C **I** **A**<br>*Place in event cycle (when)*<br>P D **R**<br>*Sphere of action (what)*<br>**O** **L** P | Back-up copies of telework information and software on the remote access farm should be taken and tested on a regular basis.<br><br>The back-ups should be made on reliable media and stored in a secure remote location, at a sufficient distance to escape any damage from a disaster at the agency. Back-ups of sensitive data should be protected by means of encryption. All back-ups are retained for a certain time.<br><br>Restoration procedures should be regularly checked and tested to ensure that they are effective and that they can be completed within reasonable time. |

*Category 2: Hardware controls*

| **Control F2.1** | **Physically secure the remote access farm** |
|---|---|
| *Security attributes (why)*<br>**C** **I** **A**<br>*Place in event cycle (when)*<br>**P** D R<br>*Sphere of action (what)*<br>O L **P** | The remote access farm should be housed in a secure area that prevents unauthorized access and offers physical protection against damage.<br><br>The secure area should have appropriate security barriers (e.g. walls), sufficient entry controls (e.g. locks) and an alarm system to prevent or detect unauthorized access. An audit trail of all access should be securely maintained. The secure area should give minimum indication of its purpose.<br><br>The remote access farm should be protected against damage by means of for example fire fighting equipment, air conditioning, humidification equipment, uninterruptible power supply and lightning protection. |

| **Control F2.2** | **Implement and maintain a redundant remote access farm** |
|---|---|
| *Security attributes (why)*<br>C I **A**<br>*Place in event cycle (when)*<br>P D **R**<br>*Sphere of action (what)*<br>**O** L **P** | The remote access farm should be redundantly available at another location than the main location to ensure continuity after a calamity.<br><br>This location should be properly physically secured and at a safe distance away from the main site to avoid damage from the same disaster that has affected the main site. All necessary applications and data should be timely available on the 'spare' remote access farm. |

# Appendix L Threat/Control Matrix

(See next pages)

| | | | Teleworker | | | | | | | | | | | | | | | | | Location | | | | | | | Telework computer | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | General controls | Develop a code of conduct for teleworking | Establish guidelines for using sensitive agency information | Establish guidelines for non-work-related use of computers | Establish guidelines for using wireless networks | Establish guidelines for using anti-malw. software and firew. | Establish guidelines for taking back-ups | Establish guidelines for using portable data carriers | Establish guidelines for using the Internet | Establish guidelines for using email | Establish guidelines for using authentication means | Establish guidelines to prevent theft | Establish guidelines for securing the remote location | Provide copies of the code and guidelines to teleworkers | Distribute awareness material | Provide security awareness training | Properly construct the remote location | Install a burglar alarm | Install a secure safe | Install smoke detectors | Install sprinklers | Install fire extinguishers | Install lightening protection | Implement a standard technical configuration | Use telework computers of sufficient technical specification | Use reliable hardware and software | Preinstall and -configure software | Implement anti-malware software | Implement a personal firewall | Automatically download and install updates and patches | Implement screen notifications | Implement an adequate log-on procedure | Implement an authentication mechanism | Ensure the use of strong passwords | Ensure regular password change | Ensure the computer is only bootable from hard disk | Implement automatic access lock | Automatically encrypt data on the hard disk | Implement automatic power-safe | Implement device lock software | Implement an URL filter | Prevent installation of unauthorized software | Securely store passwords and cryptographic keys | Implement anti-theft tracking software | Automatically back-up data on the hard disk |
| | | | B1.1 | B1.2 | B1.3 | B1.4 | B1.5 | B1.6 | B1.7 | B1.8 | B1.9 | B1.10 | B1.11 | B1.12 | B1.13 | B2.1 | B2.2 | C1 | C2 | C3 | C4 | C5 | C6 | C7 | D1.1 | D1.2 | D1.3 | D1.4 | D2.1 | D2.2 | D2.3 | D2.4 | D2.5 | D2.6 | D2.7 | D2.8 | D2.9 | D2.10 | D2.11 | D2.12 | D2.13 | D2.14 | D2.15 | D2.16 | D2.17 | D2.18 |
| **Teleworker** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| A1.1 | Disclosure of log-on information | G | V | | | | | | | | | V | | | V | V | V | | | | | | | | | | V | | | | V | V | V | | | | | | | V | | | | | |
| A1.2 | Loss of authentication token or certificate | G | V | | | | | | | | | V | | | V | V | V | | | | | | | | | | V | | | | V | V | V | | | | | | | V | | | | | |
| A1.3 | Chosen passwords are weak | G | V | | | | | | | | | V | | | V | V | V | | | | | | | | | | V | | | | V | V | | V | V | | | | | V | | | | | |
| A1.4 | Introduction of malware from the Internet or email | G | V | | | | V | | | V | V | | | | V | V | V | | | | | | | | | | V | V | V | V | | | | | | | | V | V | | | | | |
| A1.5 | Introduction of malware from portable data carriers | G | V | | | | V | | V | | | | | | V | V | V | | | | | | | | | | V | V | V | V | | | | | | | | V | | | | | | |
| A1.6 | Connection of telework computer to computer networks | G | V | | | V | V | | | | | | | | V | V | V | | | | | | | | | | V | V | V | V | | | | | | | | V | | | | | | |
| A1.7 | Malfunctioning computers in the hands of third parties | G | V | V | | | | V | | | | | | | V | V | V | | | | | | | | | | V | | | | V | V | V | V | V | V | | | V | | | | V |
| A1.8 | Use of telework computers by third parties | G | V | | V | | | | | | | | | | V | V | V | | | | | | | | | | V | | | | V | | | | | | V | | | | | | | |
| A1.9 | Neglect of important 'housekeeping activities' | G | V | | | | V | | | | | | | | V | V | V | | | | | | | | | | V | | | V | | | | | | | | | | | | | |
| A1.10 | Loading of harmful software | G | V | | | | | | | | | | | | V | V | V | | | | | | | | | | V | | | | | | | | | | | | V | | V | | | |
| A1.11 | Inappropriate changes to software configuration | G | V | | | V | V | | | | | | | | V | V | V | | | | | | | | | | V | | | | | | | | | | | | | | | | |
| **Location** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | *Category 1: Teleworker is unable to access telework equipment or the remote access farm* | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| B1.1 | Unreliable power supply | G | | | | | | | | | | | | | | | | | | | | | | | | | V | | | | | | | | | | | V | | | | | |
| B1.2 | Absence of an Internet connection | G | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| B1.3 | Incompatible technologies for access to the Internet | G | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | *Category 2: The remote location is not physically secure* | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| B2.1 | Loss or theft of telework equipment | G | | | | | | V | | | | | V | V | V | V | V | V | V | V | | | | | | | | V | | | | V | V | V | V | V | V | | V | | | V | V | V |
| B2.2 | Damage to telework computers | G | | | | | | V | | | | | | V | V | V | V | | | V | V | V | V | V | | | | V | | | | | | | | | | | | | | | | V |
| B2.3 | Inspection of information through overlooking | G | | | | | | | | | | | V | | V | V | V | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| | | Telework computer | | | | | | Connection | | | | | | Remote access farm | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Equip computers with a travel pack | Label computers with an anonymous telephone number | Provide computers with a serial number | Implement alarm systems and motion detectors | Mark computer with an anti-theft sticker | Limit the physical availability of ports and drives | Manage Internet Access Providers | Provide multiple lines to different telephone exchanges | Safeguard the confidentiality of data in transit | Prevent connection hijacking | Automatically terminate unused connections | Restrict the number of simultaneously open connections | Implement and maintain anti-malware software and firewall | Implement an adequate log-on procedure | Implement an authentication mechanism | Ensure the use of strong passwords | Ensure regular password change | Implement teleworker access rights | Restrict access to authorized computers | Apply load balancing techniques | Log security relevant actions | Back-up data on the remote access farm | Physically secure the remote access farm | Implement and maintain a redundant remote access farm |
| | | D3.1 | D3.2 | D3.3 | D3.4 | D3.5 | D3.6 | E1 | E2 | E3 | E4 | E5 | E6 | F1.1 | F1.2 | F1.3 | F1.4 | F1.5 | F1.6 | F1.7 | F1.8 | F1.9 | F1.10 | F2.1 | F2.2 |
| **Teleworker** | | | | | | | | | | | | | | | | | | | | | | | | | |
| A1.1 | Disclosure of log-on information | | | | | | | | | | | | | | V | V | | | | V | | | | | |
| A1.2 | Loss of authentication token or certificate | | | | | | | | | | | | | | V | V | | | | V | | | | | |
| A1.3 | Chosen passwords are weak | | | | | | | | | | | | | | V | V | V | V | | | | | | | |
| A1.4 | Introduction of malware from the Internet or email | | | | | | V | | | | | | | V | | | | | | V | | | | | |
| A1.5 | Introduction of malware from portable data carriers | | | | | | V | | | | | | | V | | | | | | V | | | | | |
| A1.6 | Connection of telework computer to computer networks | | | | | | V | | | | | | | V | | | | | | | | | | | |
| A1.7 | Malfunctioning computers in the hands of third parties | | V | V | V | | | | | | | | | | V | V | | V | | | | | | | |
| A1.8 | Use of telework computers by third parties | | | | | | | | | | | | | | | | | | | | | | | | |
| A1.9 | Neglect of important 'housekeeping activities' | | | | | | | | | | | | | V | | | | | | | | | | | |
| A1.10 | Loading of harmful software | | | | | | V | | | | | | | V | | | | | | | | | | | |
| A1.11 | Inappropriate changes to software configuration | | | | | | | | | | | | | | | | | | | | | | | | |
| **Location** | | | | | | | | | | | | | | | | | | | | | | | | | |
| | *Category 1: Teleworker is unable to access telework equipment or the remote access farm* | | | | | | | | | | | | | | | | | | | | | | | | |
| B1.1 | Unreliable power supply | V | | | | | | | | | | | | | | | | | | | | | | | |
| B1.2 | Absence of an Internet connection | | | | | | | V | | | | | | | | | | | | | | | | | |
| B1.3 | Incompatible technologies for access to the Internet | V | | | | | | | | | | | | | | | | | | | | | | | |
| | *Category 2: The remote location is not physically secure* | | | | | | | | | | | | | | | | | | | | | | | | |
| B2.1 | Loss or theft of telework equipment | V | V | V | V | V | | | | | | | | | V | V | | V | | | | | | | |
| B2.2 | Damage to telework computers | V | | | | | | | | | | | | | | | | | | | | | | | |
| B2.3 | Inspection of information through overlooking | | | | | | | | | | | | | | | | | | | | | | | | |

| | | | Teleworker | | | | | | | | | | | | | | | | | Location | | | | | | | Telework computer | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | General controls | Develop a code of conduct for teleworking | Establish guidelines for using sensitive agency information | Establish guidelines for non-work-related use of computers | Establish guidelines for using wireless networks | Establish guidelines for using anti-malw. software and firew. | Establish guidelines for taking back-ups | Establish guidelines for using portable data carriers | Establish guidelines for using the Internet | Establish guidelines for using email | Establish guidelines for using authentication means | Establish guidelines to prevent theft | Establish guidelines for securing the remote location | Provide copies of the code and guidelines to teleworkers | Distribute awareness material | Provide security awareness training | Properly construct the remote location | Install a burglar alarm | Install a secure safe | Install smoke detectors | Install sprinklers | Install fire extinguishers | Install lightening protection | Implement a standard technical configuration | Use telework computers of sufficient technical specification | Use reliable hardware and software | Preinstall and -configure software | Implement anti-malware software | Implement a personal firewall | Automatically download and install updates and patches | Implement screen notifications | Implement an adequate log-on procedure | Implement an authentication mechanism | Ensure the use of strong passwords | Ensure regular password change | Ensure the computer is only bootable from hard disk | Implement automatic access lock | Automatically encrypt data on the hard disk | Implement automatic power-safe | Implement device lock software | Implement an URL filter | Prevent installation of unauthorized software | Securely store passwords and cryptographic keys | Implement anti-theft tracking software | Automatically back-up data on the hard disk |
| | | | B1.1 | B1.2 | B1.3 | B1.4 | B1.5 | B1.6 | B1.7 | B1.8 | B1.9 | B1.10 | B1.11 | B1.12 | B1.13 | B2.1 | B2.2 | C1 | C2 | C3 | C4 | C5 | C6 | C7 | D1.1 | D1.2 | D1.3 | D1.4 | D2.1 | D2.2 | D2.3 | D2.4 | D2.5 | D2.6 | D2.7 | D2.8 | D2.9 | D2.10 | D2.11 | D2.12 | D2.13 | D2.14 | D2.15 | D2.16 | D2.17 | D2.18 |
| **Telework computer** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | *Category 1: Poor hard- and software configuration* | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| C1.1 | Telework computer not suitable for teleworking | G | | | | | | | | | | | | | | | | | | | | | | | V | V | V | V | | | | | | | | | | | | | | | | | |
| C1.2 | Logical access control on telework computer bypassed | G | | | | | | | | | | | | | | | | | | | | | | | V | | | V | | | | | | | | | | | | | | | | | |
| C1.3 | Security features not properly configured | G | V | | | V | V | | | | | | | | V | V | V | | | | | | | | V | | | V | | | | | | | | | | | | | | | | | |
| C1.4 | Inadequate malware protection | G | V | | | | V | | | | | | | | V | V | V | | | | | | | | V | | | V | V | V | V | | | | | | | | | | | | | |
| | *Category 2: Telework computer vulnerable to tampering* | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| C2.1 | Discovery of log-on information stored on computer | G | | | | | | | | | | | | | | | | | | | | | | | | | | V | | | | | | | | | | | | | | | | V | |
| C2.2 | Encryption keys stored on computer compromised | G | | | | | | | | | | | | | | | | | | | | | | | | | | V | | | | | | | | | | | | | | | | V | |
| | *Category 3: Telework computer unable to connect to the remote access farm* | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| C3.1 | Internet access device malfunctions | G | | | | | | | | | | | | | | | | | | | | | | | V | | V | V | | | | | | | | | | | | | | | | | |
| C3.2 | Communications software malfunctions | G | | | | | | | | | | | | | | | | | | | | | | | V | | V | V | | | | | | | | | | | | | | | | | |
| **Internet connection** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| D1 | Unavailable Internet connection | G | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| D2 | Unreliable or slow Internet connection | G | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| D3 | Unauthorized inspection of data in transit | G | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| D4 | Hijacking of the connection | G | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| D5 | Unused connections remain open | G | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Remote access farm (RAF)** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| E1 | RAF not continuously available | G | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| E2 | Teleworker has too many access rights on RAF | G | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| E3 | Unauthorized parties gain access to the RAF | G | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| | | Telework computer | | | | | | Connection | | | | | | Remote access farm | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Equip computers with a travel pack | Label computers with an anonymous telephone number | Provide computers with a serial number | Implement alarm systems and motion detectors | Mark computer with an anti-theft sticker | Limit the physical availability of ports and drives | Manage Internet Access Providers | Provide multiple lines to different telephone exchanges | Safeguard the confidentiality of data in transit | Prevent connection hijacking | Automatically terminate unused connections | Restrict the number of simultaneously open connections | Implement and maintain anti-malware software and firewalls | Implement an adequate log-on procedure | Implement an authentication mechanism | Ensure the use of strong passwords | Ensure regular password change | Implement teleworker access rights | Restrict access to authorized computers | Apply load balancing techniques | Log security relevant actions | Back-up data on the remote access farm | Physically secure the remote access farm | Implement and maintain a redundant remote access farm |
| | | D3.1 | D3.2 | D3.3 | D3.4 | D3.5 | D3.6 | E1 | E2 | E3 | E4 | E5 | E6 | F1.1 | F1.2 | F1.3 | F1.4 | F1.5 | F1.6 | F1.7 | F1.8 | F1.9 | F1.10 | F2.1 | F2.2 |
| **Telework computer** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | *Category 1: Poor hard- and software configuration* | | | | | | | | | | | | | | | | | | | | | | | | | |
| C1.1 | Telework computer not suitable for teleworking | | | | | | | | | | | | | | | | | | | | | | | | | |
| C1.2 | Logical access control on telework computer bypassed | | | | | | | | | | | | | | | | | | | | | | | | | |
| C1.3 | Security features not properly configured | | | | | | | | | | | | | | | | | | | | | | | | | |
| C1.4 | Inadequate malware protection | | | | | | | | | | | | | | | | | | | | | | | | | |
| | *Category 2: Telework computer vulnerable to tampering* | | | | | | | | | | | | | | | | | | | | | | | | | |
| C2.1 | Discovery of log-on information stored on computer | | | | | | | | | | | | | | | | | | | | | | | | | |
| C2.2 | Encryption keys stored on computer compromised | | | | | | | | | | | | | | | | | | | | | | | | | |
| | *Category 3: Telework computer unable to connect to the remote access farm* | | | | | | | | | | | | | | | | | | | | | | | | | |
| C3.1 | Internet access device malfunctions | | | | | | | | | | | | | | | | | | | | | | | | | |
| C3.2 | Communications software malfunctions | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Internet connection** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| D1 | Unavailable Internet connection | | | | | | | V | | | | | | | | | | | | | | | | | | |
| D2 | Unreliable or slow Internet connection | | | | | | | V | V | | | | | | | | | | | | | | | | | |
| D3 | Unauthorized inspection of data in transit | | | | | | | | | V | | | | | | | | | | | | | | | | |
| D4 | Hijacking of the connection | | | | | | | | | | V | | | | | | | | | | | | | | | |
| D5 | Unused connections remain open | | | | | | | | | | | V | V | | | | | | | | | | | | | |
| **Remote access farm (RAF)** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| E1 | RAF not continuously available | | | | | | | | | | | | | V | | | | | | | V | | V | V | V | |
| E2 | Teleworker has too many access rights on RAF | | | | | | | | | | | | | | | | | | V | | | V | | | | |
| E3 | Unauthorized parties gain access to the RAF | | | | | | | | | | | | | V | V | V | V | V | | V | | V | | | | |