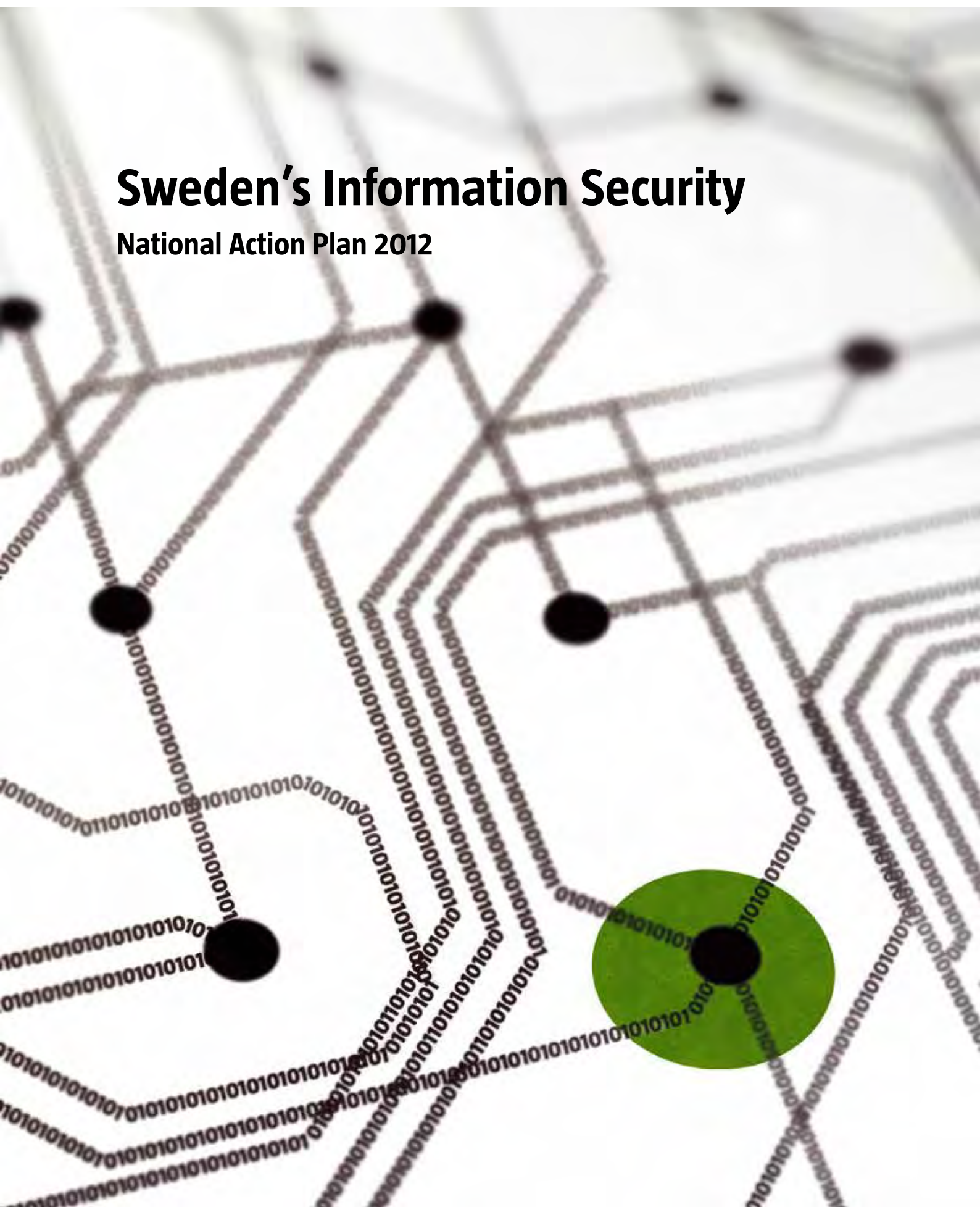


Sweden's Information Security

National Action Plan 2012



Sweden's Information Security

National Action Plan 2012

Sweden's Information Security
National Action Plan 2012

Swedish Civil Contingencies Agency (MSB)

Layout: Advant Produktionsbyrå AB
Press: DanagårdLiTHO

Order No: MSB455 - November 2012
ISBN: 978-91-7383-272-4

Preface

In today's information society we process, store, communicate, and multiply information in greater quantities than ever before. Information management is performed manually and is increasingly supported by IT, for example, the public internet.

Information security is about information being protected, based on the demands for confidentiality, data integrity and availability. This applies both to individuals and organisations.

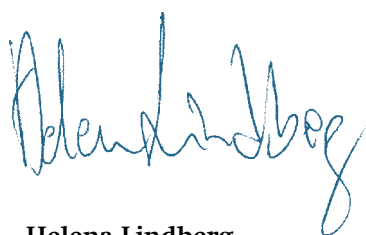
Information security is in other words a concern for everyone.

Information and its management must be of high quality in Sweden. All actors must possess the requisite knowledge about information security and be able to trust information and its management at all levels of society.

Shortcomings in information management can lead to a drop in trust in services and the actors providing them. Serious and repeated disruptions can lead to crises of confidence, which can also spread to other bodies and services and also to other societal sectors.

To succeed with the challenges in information security it is important that society has a common understanding of information security work - i.e. a strategy.

In light of this, the MSB has, in consultation with the Swedish Armed Forces, Swedish Defence Materiel Administration, Swedish Defence Radio Establishment, Swedish Post and Telecom Agency and the Swedish Criminal Police and the Swedish Security Service produced this action plan for Sweden's information security.



Helena Lindberg
Director-General

Contents

Introduction	7
Producing the National Action Plan	8
<i>Connection between strategy, situational assessment and the Action Plan</i>	8
<i>National Action Plan work process</i>	10
Management of the Action Plan	11
1. Information security in organisations	13
1.1 Develop a framework for information security	14
1.2 Requirements for security analyses when the Security Protection Ordinance is applied	15
1.3 Develop methods for continuity planning	16
1.4 Supporting work with secure e-administration and secure e-services	16
1.5 Developing support for specific activities	18
1.6 Self-measurement of information security	19
1.7 Enhance the protection of privacy as part of information security	20
1.8 National terminology for information security	21
2. Competence	23
2.1 Study training and competence needs in the field of information security	24
2.2 Increase awareness about Sweden's information security	25
2.3 Announcement of framework research programme on information security	25
2.4 Information campaign on signal protection.....	26
3. Information sharing, collaboration and response	29
3.1 Increased collaboration to prevent and manage serious it-incidents	30
3.2 IT incident reporting	31
3.3 Technical detection and warning system	32
3.4 National cooperation on work with information security in the EU.....	33
3.5 Plan, implement and evaluate information security exercises	34
4. Communications security	37
4.1 Preventive measures to increase security in electronic communications	38
4.2 Measures for Steps to follow up security in the electronic communication sector	39
4.3 Special initiative on the introduction of DNSSEC	39
4.4 Encryption for classified data.....	40
4.5 Develop Swedish Government Secure Intranet (SGSI)	41
4.6 Accessible and protected communications infrastructures for the public sector	41
5. Security in products and systems	45
5.1 Develop encryption audit regulations for commercial products	46
5.2 Increased use of CC evaluated products	46
5.3 National evaluation laboratory	47
5.4 Increased security in industrial information and control systems (SCADA) ..	48

Introduction

Introduction

The Swedish Civil Contingencies Agency (MSB) has in conjunction with other agencies involved in the Cooperation Group for Information Security (SAMFI) produced a strategy for information security for 2010-2015. To realize the intentions of the strategy objectives need to be broken down into concrete action. This Action Plan is a tool for the authorities in SAMFI to identify priority measures, and it should also be seen as a successor to the Action Plan that was published in 2008 by the Swedish Emergency Management Agency (SEMA) on behalf of the government.

The proposed measures in the Action Plan fall within the framework of the responsibilities owned by the authorities in SAMFI, and they can be implemented by an authority individually or in joint projects. The plan should not however be viewed as a comprehensive account of all the measures that the various authorities will implement in their respective operations.

The authorities in SAMFI have specifically set tasks with regards to information security. To enhance Sweden's information security requires however involvement and activities at all levels of society. A basis for the Action Plan as a whole is to develop ways to work in which several actors are involved and affect both the measures included in the current plan and the content of future work with information security.

The target group for the Action Plan includes all actors that work with information security in their daily operations. For actors in, for example, the transport sector, energy sector, financial sector, as well as in medical and health care it is supportive to know in what direction the national work is moving. The Action Plan provides both a foundation for active dialogue about objectives and methods, and an opportunity for individual organisations to coordinate their security work with the national security work. The plan runs for three years and was produced by the MSB in consultation with other agencies involved in SAMFI, i.e. Swedish Defence Materiel Administration (FMV), Swedish Certification Body for IT Security (CSEC), Swedish Defence Radio Establishment (FRA), Swedish Armed Forces, Swedish Post and Telecom Agency (PTS) and Swedish Security Service (Säpo) and Swedish Criminal Police (RKP).

Producing the National Action Plan

Connection between strategy, situational assessment and the Action Plan

The national strategy for information security is an important basis for formulation of the Action Plan. An additional important input value is the ongoing work to produce a national situational assessment regarding Sweden's information security. This section describes how the Action Plan relates to the strategy and the work on the situational assessment.

Strategy for Sweden's information security 2010-2015 states that the aim is to achieve effective information security within society which promotes:

- Freedoms and rights, as well as privacy.
- Functionality, efficiency and quality within society.
- The fight against crime within society.
- The ability of society to prevent and manage serious disruptions and crises.
- Economic growth.
- Citizens' and organisations' knowledge of, and trust in, information management and IT systems.

The strategy also designates five strategic areas:

1. Information security in organisations
2. Competence
3. Information sharing, collaboration and feedback
4. Communications security
5. Security in products and systems.

The Action Plan is a vital instrument for implementing the strategy and therefore takes the five strategic areas as its starting point. The relationship between strategy and the Action Plan is illustrated in Figure 1.

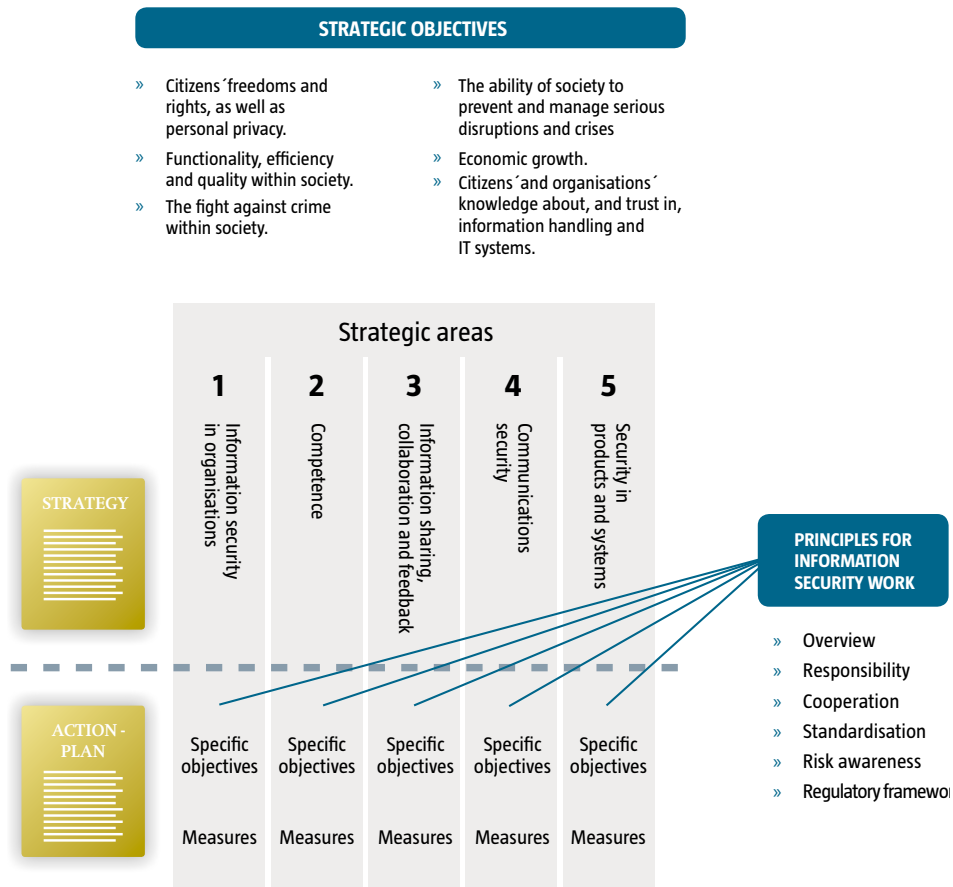


Figure 1. Relationship between strategy and the Action Plan.

The basis for the work with Sweden's information security is a good understanding of society's risks and vulnerabilities. The Action Plan's activities are based on the MBS' ongoing situational assessments, the overall perceptions of the authorities included in the SAMFI and the threat and risk assessments developed in cooperation with other stakeholders. Figure 2 illustrates the process for working with strategy, situational assessment and the Action Plan.

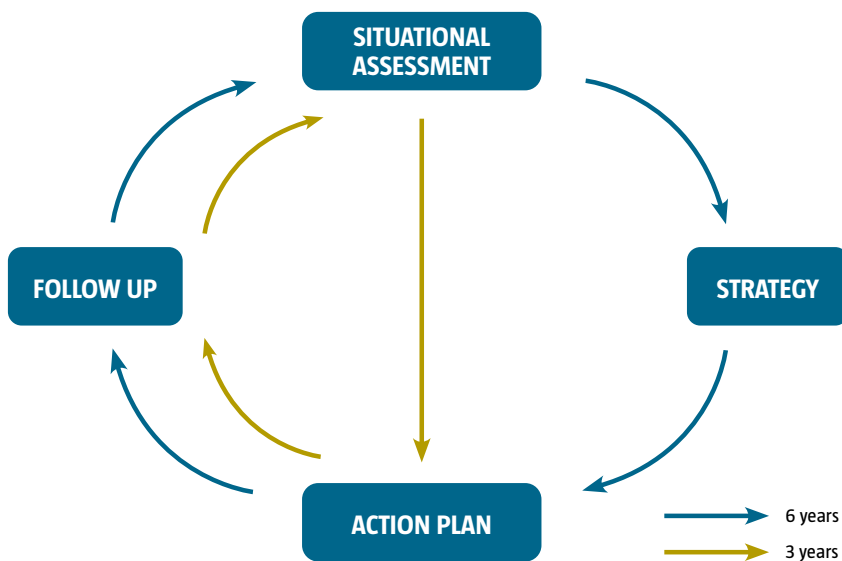


Figure 2. Process for working with strategy, situational assessment and the Action Plan.

National Action Plan work process

The National Action Plan has been developed by a working group within SAMFI. The work has comprised joint meetings and work within the framework of the ordinary activities of the authorities included in SAMFI.

The work with the Action Plan has also included discussions and cooperation with a large number of stakeholders within society, for example the Information Security Council¹. This has made it possible to continually anchor the Action Plan at different levels of society.

The terminology in the original Swedish version of the Action Plan mainly complies with the SIS handbook Information Security Terminology (SIS HB 550, version 3). Information security encompasses both administrative and technical aspects with regard to confidentiality, accuracy and availability of information assets. As a complement to these three aspects, the concept of traceability is also applied, amongst others. The term information assets refer both to information and the resources used to process the information. Information security thus concerns more than securing IT systems. Other resources – not least, human resources – are also important components of the information security concept.

The objectives and measures specified in the Action Plan are linked to the strategic areas specified in the strategy for Sweden's information security. The work must be carried out in accordance with the six principles for information security work as defined in the strategy:

Overview: All stakeholders are required to have an overview of information security to ensure that the development of information management and IT use in society proceeds in a safe and secure manner. Information security is a complex and cross-border field that embraces, amongst other things, technology, administration, economy and law.

Responsibility: All information security work should be based on responsibility as regulated by society, for example, the responsibility principle. This means that those responsible for an activity under normal conditions should also be responsible in a crisis situation.

Cooperation: The complex, cross-border nature and rapid pace of development of information security require effective cooperation.

Standardisation: Standards which support information security work should be applied as they are based on experience and take advantage of previous advances. In this way, a higher degree of security can be achieved and unnecessary mistakes avoided.

Risk awareness: Resources are required to achieve safe and secure information management in society. Security aspects should not be seen as an extra cost burden, but rather as a self-evident investment to achieve the intended function and quality.

1. <https://www.msb.se/sv/Forebyggande/Informationssakerhet/Samhallets-informationssakerhet-/Informationssakerhetsradet/>

Regulatory framework: A prerequisite for efficient information security in society is the establishment of rules applicable to modern information handling. This applies at both an operational and social level.

Management of the Action Plan

Management of the Action Plan is closely linked to SAMFI work. The Action Plan is produced by the MSB in consultation with the authorities included in SAMFI and is supposed to be updated every three years.

The 2008 Action Plan contained 47 proposed measures. The proposed measures generally resulted in projects and activities. A large number of proposed measures have been implemented while others are in the process of being implemented. Where appropriate, some proposed measures have also been merged with new or ongoing activities in the 2012 Action Plan.

The government has been kept continuously apprised of the outcome of the measures in the 2008 Action Plan.

Information security in organisations

1. Information security in organisations

Information management occurs in all sections of society, and Sweden's information security is consequently dependent on a large number of stakeholders. Authorities at national, municipal and county level, businesses and other organisations have different criteria and therefore different needs and requirements in relation to information security.

Organisations sometimes handle information in circumstances where confidentiality, integrity and availability are critical. In most organisations, efficient information security is an important internal matter which is vital to fulfilling their own quality and efficiency requirements. At the same time, information security cannot be considered solely as an internal matter. The flow of services and products is a multi-stage process and the consequences of ineffective information security can therefore be felt far outside the confines of the individual organisation.

Information security is intrinsic to the quality of the organisation. This means, amongst other things, identifying the organisation's risks and allocating responsibility for managing these risks. Improving information security does not just entail the meeting of external requirements, but also improving the actual organisation. Having effective information security must therefore be seen as a quality aspect, a way of achieving effective internal control, order and tidiness. Effective information security is also a prerequisite for several different IT-based services that can provide cost savings or generate revenue for an organisation.

1.1 Develop a framework for information security

The basic element in work with information security is management and control, a fact emphasized by ISO/IEC 27000, the international family of standards for information security. Support for the development of administrative information security is therefore a vital element of the National Action Plan.

An information security management system (ISM) is necessary to enable an organisation's management to control information security work to ensure it corresponds to the organisation's requirements for being able to satisfactorily fulfil its mission. ISM is also an effective tool for creating a security culture which actively involves all employees in security work.

The authorities included in SAMFI, together with other stakeholders active in the project Support for organisations' information security work (SVISA), have cooperated to develop a support network which encourages different organisations to introduce an information security management system. The SVISA project is now concluded and is being followed by an administrative phase in which systematic work is being carried out to create quality and usability in the long term. In sectors where the need is assessed as being particularly pressing, method support will also be adapted to the individual sector.

While the work was in progress, a number of priority areas were identified where further measures are needed. The priority areas include:

- supporting management functions in fulfilling their responsibility with regard to information security, amongst other things by conducting systematic risk analyses and prioritising protective measures.
- developing risk analysis methods which also facilitate evaluation of information security risks in relation to other types of risk and assessing how different investments pay dividends in the form of better security.
- developing the existing model for information classification to ensure it supports the process from evaluation of the consequences to the application of systematically developed protection levels. This work may also involve developing definitions of specific joint national protection levels.
- developing support for controls relating to the procurement of systems, e-services and other products/services which are relevant to information security for organisations which are intrinsic to the functioning of society.
- developing the website www.informationssakerhet.se to provide relevant information and services in the field of information security for different stakeholders to ensure that it forms a central support structure for developing and coordinating information security within society.

Note that training and awareness-raising, which are also important components of administrative information security, are examined in Chapter 2.

A specific action plan will be developed to prioritise and coordinate work with administrative information security.

OBJECTIVES

To provide an easy-to-use, effective support mechanism over time to help organisations develop their information security.

MEASURES

Manage the work of the SVISA project and implement further measures as described above.

IMPLEMENTATION

The MSB is coordinating the work primarily with the authorities included in SAMFI and with authorities on a sector, county and municipal level and other relevant stakeholders.

1.2 Requirements for security analyses when the Security Protection Ordinance is applied

Authorities and other bodies for example at municipal and county level, which are subject to the Security Protection Ordinance (1996:633) are responsible for examining which activities require security protection in respect of national security and anti-terrorism protection (security analysis).² This can include assets in the form of personnel, materiel, information, facilities or activities. A security analysis forms the basis for a well-adjusted security protection system and is partly an examination which aims to map which information is subject to confidentiality and relates to national security in an organisation, and partly an action which documents the reasoning behind the assessment of what requires a security protection system. Security analysis refers both to the identification and prioritising of assets worthy of protection, the assessment of security threats, vulnerabilities and risks, and the prioritising and management of risks, including decisions on protection measures. The end result of a security analysis should be a security plan to manage the risks identified in the security analysis.

OBJECTIVES

To ensure all authorities and other parties subject to the Security Protection Ordinance have been informed of the obligation to examine which organisations require security protection in respect of national security or anti-terrorism protection.

MEASURES

All authorities must be given specific information on the applicable obligation to carry out security analyses in accordance with the Security Protection Ordinance, and on the link to risk management based on MSBFS 2009:10.

IMPLEMENTATION

The Swedish Security Service and the Swedish Armed Forces are responsible for the cooperation with the MSB.

2. A review of security legislation is currently being carried out. The aim is primarily to better adapt legislation to the protection requirements of activities which are significant in terms of national security and to the requirements of international cooperation. The outcome of the review will be reported by 30 April 2014 at the latest. (<http://www.regeringen.se/content/1/c6/18/22/43/8492cf99.pdf>)

1.3 Develop methods for continuity planning

Continuity planning is a method for maintaining an organisation's delivery capacity by planning for a continuation of operations in the event of operational incapacity, i.e. to ensure that, despite disruption, it is able to deliver the products and services most vital to the organisation and its interests.

Today, access to information is a basic prerequisite for ensuring that an organisation can continue to operate. Planning which enables maintenance of systems, networks and other IT architecture components is therefore a vital element of continuity planning, i.e. the information security dimension forms a particularly important part of the planning. At the same time, the planning should also describe how it will be possible to carry out vital activities, even without IT support.

Continuity planning is complicated by the many interdependencies that exist both within and between organisations. To be able to manage these interdependencies and where necessary develop a coordinated continuity plan, joint models should be established for use by other stakeholders in their respective organisation. This can also be viewed as a basis for different types of contractual relationships between stakeholders and for consensus at different escalation stages, including at the national level.

OBJECTIVES

A generic model for continuity planning with well-defined concepts should be established, which can be adapted to the needs of different organisations.

MEASURES

Carry out an analysis which describes both the need for continuity planning from an information security standpoint, and how the field relates, for example, to crisis management and coordination in the event of serious IT incidents. Proposals for generic continuity planning methods are then developed on this basis, which can also be synchronised with an organisation's overall continuity planning.

IMPLEMENTATION

The MSB is responsible for ensuring that a continuity planning analysis is carried out and then accepted by SAMFI and other interested parties.

1.4 Supporting work with secure e-administration and secure e-services

For more than a decade, there has been a strong intention to develop Swedish public administration in the direction of what has today become known as e-government. Amongst other things, this entails the authorities providing citizens and other interested parties with ever increasing options for managing their official contacts via the Internet.

Effective information security is a necessary prerequisite for efficient and trustworthy e-government systems. In such an advanced information management system as e-government, it is vital that security issues are not solely addressed by technical solutions. The focus of the security work should be management,

control and analysis in conjunction with development work to achieve effective security solutions. As e-government is based on cooperation between different agencies and stakeholders, the eGovernment Delegation's work must also contribute to effective information security control.

Controlling information is a prerequisite for systematic information security work. The most effective method of identifying which information is created and communicated in an organisation is to map the organisation's processes and the information it generates. The National Archives of Sweden has a related interest in that it provides a process-based account of information from governmental agencies³, a system which may also be advantageously applied by other organisations.

In many e-services provided by governmental agencies and municipalities, counterparties need to be identified electronically in a secure manner. Methods for signing documents electronically are also necessary to ensure that it is possible to identify from whom the document originates and that the document cannot be corrupted. The eGovernment Delegation's report SOU 2010:62 points out that Sweden has used the same technical solution since the 1990s with regard to cryptographic security for e-identifications and electronic signatures.⁴

OBJECTIVES

To ensure that the eGovernment Delegation's intentions and other initiatives within the field of e-government are implemented with information security adapted to identified and assessed risks.

MEASURES

An initiative to support secure e-government must be introduced. Amongst other things, the initiative must pave the way to a strategy for secure e-government, as well as more specific measures, such as support for process-oriented mapping of information and an investigation into enhanced cryptographic security for e-identification and electronic signatures.

IMPLEMENTATION

Within the framework of work with the eGovernment Delegation, the MSB is taking the initiative to develop, amongst other things, a strategy for information security in the field of e-government and is responsible for initiating other measures. Other stakeholders, such as the authorities included in SAMFI and the Swedish Association of Local Authorities and Regions (SKL) will also be involved in the practical work to develop the strategy.

3. RA-FS 2008:4 Regulations on amending the National Archives of Sweden's regulations and guidelines (RA-FS 1991:1) on governmental agencies' archives.

4. *As simple as possible for as many as possible: Under construction – e-government of the future*, SOU 2010:62 (<http://www.regeringen.se/content/1/c6/15/27/07/2744b8f7.pdf>).

1.5 Developing support for specific activities

The functioning of society is based on a large number of stakeholders being able to create and manage effective information security in their organisations. Support in information security matters should therefore be provided to stakeholders who sustain activities important to society. The MSB has prioritised the following three areas for its work in the next three-year period:

- Municipal activities
- Healthcare
- Small and medium-sized enterprises

The prioritisation is based both on the importance of the activity and the assessment of the need for support. The activities undertaken by Sweden's municipalities are varied and complex and vital to the life and health of their citizens. The complexity of activities places great demands on the municipalities' information security systems. At the same time, many municipalities are relatively small organisations which are hard pressed economically and therefore rarely have the opportunity to establish all the necessary conditions required for a systematic approach to information security.

Healthcare plays a very critical role, both as regards human life and health and the functioning of society. It is therefore very important, both from the perspective of society and the individual, that healthcare functions in a secure manner, which means being able to resist and quickly recover from undesirable events, accidents and crises. To ensure that healthcare is able to fulfil its vital function within society, citizens and other stakeholders also have to have considerable confidence in the various organisations providing the different types of care. All these factors are essential for effective information security.

The important functions of society are maintained not only by public stakeholders but also, and to an ever increasing extent, by private stakeholders. The private stakeholders' need for security in respect of their information management solutions is no less pressing than that of public stakeholders and it is therefore vital that business and industry are supported in their security work. In the first instance, support should be directed at small and medium-sized enterprises, as the major stakeholders can be assumed to have more resources available to develop the necessary security solutions themselves.

OBJECTIVES

To provide a coordinated support system for systematic information security work for priority activities, which at the same time facilitates coordination in the event of a wider crisis.

MEASURES

Activities must be implemented to increase information security in the field of healthcare, municipalities and small and medium-sized enterprises. This includes developing networks for information sharing and cooperation within respective areas of activity.

IMPLEMENTATION

The MSB is coordinating priority activities in cooperation with central stakeholders, such as the Swedish National Board of Health and Welfare, SKL and the Confederation of Swedish Enterprise.

1.6 Self-measurement of information security

An organisation's level of information security should at least correspond to its internal and external requirements. It is important for an organisation to be able to compare its information security level with other similar organisations so it can assess its own level. Being able to assess its own organisation's level of information security contributes to a large extent to management awareness and motivation.

Estimations of the level of implemented security measures are important to ensure the individual organisation is able to make the right priorities as well as develop an overall capacity assessment. The assessment of other organisations' level of information security is also an important factor for risk and vulnerability analyses implemented within the public sector.⁵

It is also not possible to assess information security in one sector to obtain an overall picture of Sweden's information security.

A tool is very urgently needed within the public sector which will enable stakeholders to measure the level of information security in their own organisations. A number of specific questions can help create a measurement (self-measurement) which the organisation can compare with other organisations (benchmarking). This also applies if the activities clearly differ from agency to agency, municipality to municipality, etc. Standardised self-measurements also make it possible to provide a basis for assessments of the security level within different sectors and also an overall picture of Sweden's information security.

OBJECTIVES

Organisations can assess their own level of information security by comparing it with other organisations in the same sector. It should also be possible to create an overall picture of the level of organisations' information in sectors and in society in general.

MEASURES

Develop a tool for self-measurement of information security for agencies, councils and municipalities. The tool must allow the various stakeholders to securely input information on their security level and compare their level with others. The tool must also make it possible to compile different anonymous reports in order to create a picture of Sweden's information security.

IMPLEMENTATION

The MSB is coordinating the work and developing a tool for self-measurement of information security which will be available from 2013.

5. MSBFS 2010:7 regulations on governmental agencies' risk and vulnerability analyses, and MSBFS 2010:6 regulations on municipalities' and county councils' risk and vulnerability analyses.

1.7 Enhance the protection of privacy as part of information security

One of the strategic objectives of Strategy for Sweden's information security 2010-2015 is to protect freedoms and rights and privacy. Today, many organisations handle large quantities of personal data and other information of a sensitive nature. A prerequisite for these organisations being able to retain a high degree of trust amongst citizens is that they are able to protect this sensitive information from unauthorized access. The privacy aspect has been identified as being central to the development of functioning security solutions in the field of healthcare and is also a foundation of the new e-government work.

The concept of privacy is not unambiguous and cannot only be defined in legal terms. Insofar as a conflict arises, for example, between availability and privacy, this situation must be highlighted and openly discussed to ensure well-founded priorities can be made. From a social perspective, it must also be clear that privacy is the central factor in ensuring citizens and other stakeholders have confidence in the functions of society. If this confidence is not forthcoming, it will have the same consequences as an interruption to availability, i.e. the function will cease functioning.

In the field of information security, the concept of integrity is often used to describe a property of an information asset. This use of the concept is not synonymous with "personal privacy". In order to facilitate information security work, it is important to clarify central concepts and this applies particularly to concepts such as privacy.

OBJECTIVES

Support for systematic information security work is available which also includes privacy aspects in a way which creates confidence in the essential functions of society.

MEASURES

Examine and clarify how personal privacy should be safeguarded within information security work. Privacy must be a driving factor, for example, in the selection of protection levels and measures.

Clarify how a balance can be created between privacy on the one hand and security measures, which may be considered a violation, for example logging and other forms of monitoring on the other.

IMPLEMENTATION

The MSB is carrying out work in cooperation with the Swedish Data Inspection Board.

1.8 National terminology for information security

Uniform terminology within the information security field is becoming more and more important as more organisations work actively to improve and manage their information security. Increasing levels of information exchange across organisational borders require uniform definitions which can be used in contracts and other types of agreement. Terminology is also vital to the strategic knowledge building and to communicating on matters of information security within different sectors of society. This does not only apply to practical information security work within individual organisations but is also a prerequisite for a number of other items in the Action Plan, such as awareness-raising measures, research and support for e-government, for example.

SIS HB 550 Terminology for information security is a basic document establishing joint and uniform terminology which should now be revised with the support of experts from the authorities included in SAMFI and other relevant parties. An all-encompassing terminology model should form the basis for the work to ensure consistent terms and relationships between terms.

The work to revise terminology must be conducted in the long-term and focus strongly on accessibility. A proposal should therefore also be developed for how the terminology should be administered and constantly revised in a quality-assured manner. It should also be available electronically.

OBJECTIVES

Quality-assured terminology for the field of information security that is continuously developed and accessible to those working in information security.

MEASURES

In cooperation with relevant specialists, SIS/TK 318 Information security and SIS Förlag AB, develop a revised version of SIS HB 550 Terminology for information security, and safeguard terminology administration in the long term.

IMPLEMENTATION

FMV/CSEC are leading the work in cooperation with SIS and other authorities included in SAMFI.

Competence

2. Competence

Development within the IT sector has been and will continue to be a strong, positive force within society. The technology provides opportunities for communication, knowledge development, economic growth and enhanced options for participation in democratic processes. Ensuring that society is able to make optimum use of the development's positive effects requires both competence and awareness of the risk associated with IT usage. Knowledge of the risks associated with IT and electronic communications, for example, via the Internet, should be taught early on and form an integral and natural part of first IT usage. This knowledge and these skills should then be included in all further schooling, including higher education, not least as an integrated part of academic programmes that lead to careers with significant elements of information handling.

The human factor is critical in many organisations. Large incidental costs can be attributed to deficiencies in the awareness and competency of managers, users and IT personnel. It is people who develop, install, configure and use technical systems. It is people who formulate, communicate and monitor administrative systems. An especially important group from an information security perspective is the organisations' management bodies. This is because they have the ultimate responsibility for organisational quality and security, and make decisions on protective measures. There is therefore a huge need for knowledge of information security matters and measures to raise levels of competence must be adapted to different roles and activities.

A field as multi-faceted as information security must be studied in more depth. Research and research studies are necessary to maintain both general knowledge and expert knowledge in the field. National research and research studies also improve teaching skills in the field - from elementary school to colleges and universities.

2.1 Study training and competence needs in the field of information security

Ensuring that information security can be developed requires a large number of stakeholders with different types of competency in the field. These range from specialist competency to the competency which enables individual home users to securely manage their information handling.

Today, there are various types of training programmes available, for example courses at universities and colleges, agencies and private training enterprises, as well as Internet courses which many organisations conduct in-house. As the information security field itself is so large, it encompasses everything from training courses which relate to the management and control of information security to technical security measures. From the perspective of society, it is important to create, and proceed from, an overall picture of both the need for, and availability of, training courses to ensure it is possible to prioritise training and research initiatives in an appropriate and long-term way. It is particularly important to be able to prioritise the need for competency in functions which are vital to society, such as healthcare for example, and within sectors with specific tasks, such as Internet providers. When it comes to the need for competency, it is also important to identify professional bodies with a high degree of relevance to information security, such as teachers at various levels, lawyers, systems engineers and professionals within the information security field.

How to develop training initiatives of a cross-sectoral nature aimed at the management level, is another area which should be analysed in greater depth. This should happen at the same time as ongoing work to develop so-called CIAO training⁶.

OBJECTIVES

To be able to raise competency levels in an effective and coordinated manner in the field of information security on the basis of a common needs assessment.

MEASURES

Examine society's need for competency within the information security field from a five-year perspective.

FRA, PTS and the MSB are cooperating with the Swedish National Defence College on developing CIAO training in 2012.

IMPLEMENTATION

The MSB is taking the initiative to examine the need for training and competency within the information security field. The examination is being carried out in close cooperation with other authorities included in SAMFI and other relevant stakeholders.

6. Chief Information Assurance Officer (CIAO)

2.2 Increase awareness about Sweden's information security

Development in society places high demands on security awareness. The public sector should take responsibility in this area by providing information and instruction in security matters. Information security is a large and complex area comprising many different components and functions. In terms of technical requirements, individuals and how they choose to handle their information, play a vital role in the work to achieve effective information security. Many security incidents today have a human rather than a technical cause, grounded in many cases on a lack of knowledge. In spite of this, resources and research are more often concentrated on development of the technical environment rather than on understanding the considerations of the individual. Knowledge and awareness amongst the general public of why information security is important and how they can protect their information are central components of information security work. Strategic considerations and target awareness are required to build up awareness and knowledge of information security issues in society. Knowledge of how awareness of information security issues affects modern day society is now almost a prerequisite for working effectively with awareness-raising measures.

Various measures are being implemented on an ongoing basis to increase the awareness level with regard to information security, for example, information initiatives aimed at specially selected target groups and development of training tools, for example the computer-based information security training for end-users developed by the MSB (DISA). To be effective in the long term, these measures should be coordinated in a programme with a strategic orientation.

OBJECTIVES

To ensure that a relevant and up-to-date understanding of the risks associated with various types of IT usage is widely available. This applies to usage both at work and at home.

MEASURES

Develop and implement a programme for raising awareness of information security in society.

IMPLEMENTATION

The MSB is responsible for developing a programme to coordinate awareness-raising measures together with the authorities included in SAMFI and other relevant stakeholders.

2.3 Announcement of framework research programme on information security

A national initiative on research and research studies in the field of information security is necessary to maintain both general and expert knowledge in the field. Increased national research and research studies also improve teaching skills in the field at colleges and universities.

Research in information security should lead – directly or indirectly – to benefits for society, and it is therefore important that the research conducted be firmly established in society as a whole. Research in information security should be

conducted from a broad perspective and not solely focus on technical research, even if this is, naturally, an important element. Social, cultural, legal, economic and criminological aspects are examples of other areas that require study in the field of information security to achieve comprehensive knowledge. The field's multi-faceted nature means that knowledge development should be conducted in cross-disciplinary environments and in cooperation with society in general.

Research based on international cooperation should be encouraged. This does not, however, contradict the need for a clearer national coalition for research conducted in Sweden.

Mapping and coordination are required to ensure that resources given to research give the maximum benefit. It is therefore important to work towards continued cooperation on research financing within the information security field.

OBJECTIVES

Increased cooperation between research-funding bodies and society in general with regard to information security research. The long-term objective is to coordinate Swedish research within the information security field at a national and international level and to have a clear orientation towards society-related needs.

MEASURES

Develop a framework research programme in the field of information security and collaborate more in the field of information security research and development in society. The first step is to launch a call for research funding in the information security field for 2012.

IMPLEMENTATION

The MSB is responsible for work carried out in cooperation with the relevant authorities.

2.4 Information campaign on signal protection

Signal protection is traditionally defined as measures aimed at ensuring confidentiality and preventing manipulation of our country's telecommunications. These measures can include systems with in-built encryption or systems for protection against interception, jamming or false signalling. For a system to be called a signal protection system it must be approved by the Swedish Armed Forces. Signal protection systems are constructed and adapted to meet a threat from other countries' general intelligence services and therefore require comprehensive protective measures, regulations, training and handling. The systems are mainly used to protect information subject to confidentiality which relates to national security but can also be used to protect other information where there is a perceived significant threat.

Swedish agencies responsible for signal protection and encryption and Swedish companies which develop encryption products possess significant knowledge and competency. This knowledge can have a broader use in society. Consultation with the responsible authorities can raise the level of security in vital societal functions. Work can also be carried out to ensure that these organisations have

the ability to protect their information assets and achieve secure cross-sector exchanges of information that are subject to confidentiality and relate to national security. This can occur at central, regional and local levels.

An information base which relates to the relevant stakeholders in the public sector should be developed and disseminated to increase awareness and use and to demonstrate the benefit of using signal protection. The information base should indicate how information can be protected from disclosure and manipulation with the aid of signal protection, primarily to protect information subject to confidentiality and relating to national security.

OBJECTIVES

Authorities at national, county and municipal level should have knowledge of what signal protection is and how it can be applied.

MEASURES

Develop an information base relating to signal protection and make this available to authorities at national, county and municipal level.

IMPLEMENTATION

The work is being carried out in cooperation with the Swedish Armed Forces, the MSB and FRA and other relevant government agencies.

**Information sharing,
collaboration and response**

3. Information sharing, collaboration and response

Sharing information is important for safeguarding and disseminating knowledge and experience in the information security field. Such knowledge and experience are found everywhere in society; both in the public and private sector. To enhance Sweden's information security, it is important that effective networks exist within and between the private and public sectors. This is particularly important when it comes to vital societal functions and critical infrastructure operated both publicly and privately.⁷ Both the public sector and the business community therefore benefit from enhanced information and experience exchange.

It is not unusual for IT-based disruptions and attacks to spread quickly over organisations' and countries' borders. Society needs to have the ability to prevent these events, and if they occur nonetheless, it must be able to handle them effectively. An important prerequisite as regards vital societal functions and critical infrastructure is that they possess adequate resilience - i.e. the ability to quickly recover after IT incidents. Increased cooperation and coordination is also required within and between all sectors of society and levels of responsibility. A global world with cross-border risks and threats also requires increased levels of cooperation. Sweden is therefore actively contributing to international co-operation at multiple levels; within the EU, with the Nordic countries and with individual states.

Traditional criminality such as fraud, extortion, slander and sabotage now also exists on the Internet. It is a threat to society and these new forms of criminality must be countered. IT incidents, including criminal acts, fall within the Police's area of responsibility and should be handled by the Police on the basis of a Police report. However, handling the consequences - i.e. not the criminal investigation - is a matter for the organisation affected and other stakeholders in society. The basis for this work is the so-called principles of Responsibility, Equality and Proximity.⁸

Large-scale IT incidents can constitute a severe threat to Sweden's security and Swedish interests. Where advanced antagonistic attacks are involved, responsibility lies with the Swedish security and intelligence services, and in most cases, the Swedish Criminal Investigation Department as well.

7. See also "A functioning society in a changing world" which the MSB has developed on behalf of the government, <https://www.msb.se/RibData/Filer/pdf/26084.pdf>.

8. *Responsibility principle*: Those responsible for an activity under normal conditions should also be responsible in a crisis situation. *Equality principle*: In a crisis situation, the organisation should, as far as possible, function as it would under normal conditions. If possible, the organisation should also be managed in the same location as under normal conditions. *Proximity principle*: The subsidiarity principle means that a crisis should be handled where it occurs and by those who are most closely affected and responsible. The affected municipality and the relevant county therefore have primary responsibility for operations. Then, if local resources prove inadequate, regional and national efforts come into play.

3.1 Increased collaboration to prevent and manage serious it-incidents

A large-scale IT incident can have serious consequences for vital societal functions and critical infrastructure. To improve Sweden's ability to prevent and manage serious IT incidents, the government believes that "a more coherent structure is required in the field. An important means for achieving this is the establishment of a national cooperation function for information security. The government therefore believes that the MSB, in cooperation with the relevant authorities, should work towards establishing such a function".⁹

On 14 April 2010, the government commissioned the MSB to develop a national plan clarifying how serious IT incidents should be handled (Fö2010/701/SSK). On 1 March 2011, the MSB presented its plan. The aim of the national management plan for serious IT incidents is to improve conditions for limiting and averting the direct consequences of a serious IT incident in society through cooperation and coordinated decision-making. Broad cooperation between different stakeholders will be required to complete this task. The management plan focuses exclusively on managing serious IT incidents. It proceeds from the basic conditions that exist within the Swedish crisis management system, i.e. guiding principles and the responsibility of individual stakeholders. The management plan is interim in nature until it has been tested and revised in line with the findings.

OBJECTIVES

To enhance the ability to prevent and manage serious crises with an IT element. Serious IT incidents must be countered by effective coordination of resources without changing current responsibilities.

MEASURES

Continue work with national cooperation in the information security field within the framework of relevant responsibilities and roles.

Continue development of a national cooperation function for information security.

Continue work between the security and intelligence services to further strengthen the ability to manage serious antagonistic cyber attacks.

Establish a national management plan for serious IT incidents after testing and revision.

9. Proposition 2010/11:1 expenditure area 6, page 83, and *IT in the service of mankind - a digital agenda for Sweden* (Ministry of Industry, Employment and Communications).

IMPLEMENTATION

The authorities included in SAMFI are continuing to work with national cooperation to prevent and manage IT incidents within the framework of relevant responsibilities and roles.

The MSB, in cooperation with SAMFI and other stakeholders in society, is continuing work to develop a national cooperation function for information security.

The MSB, in cooperation with SAMFI and relevant stakeholders, is revising the management plan as required in connection with the NISÖ 2012 exercise and establishing the management plan.

The security and intelligence services are continuing with work to strengthen their ability to manage serious antagonistic cyber-attacks.

3.2 IT incident reporting

An important component of effective information security work is the continuous gathering of knowledge about which incidents occur since they can affect information assets critical to the continuity of operations. Many stakeholders have already recognised the importance of analysing IT incidents that have occurred and transferring this knowledge back to their own organisations. In specific terms, this means that many organisations have now introduced some form of reporting and management system for IT incidents. There is great benefit to be had from not merely learning from our own mistakes and incidents but also from those of others. This applies both within the individual organisation and at the national level. It is therefore important to create conditions for an advanced flow of information between individual stakeholders and centralised national agencies. A more systematic IT incident reporting system in society does not however replace routines for reporting crimes to the Police and it is important that reporting is not carried out in such a way as to compromise criminal investigations.

On 14 April 2010, the government gave the MSB the task of submitting proposals relating to a system for mandatory IT incident reporting for government agencies. On 1 March 2011, the MSB presented its proposal for creating a coherent structure for such IT incident reporting. The proposal can be described in short as a bidirectional reporting process for reporting to the MSB/CERT-SE and providing feedback to relevant parties. It was proposed that the system be mandatory for government agencies and voluntary for other stakeholders in society. When presenting its findings the MSB identified the need for careful analysis of the legal requirements for collating passing on and handling information.

In Proposition 2011/12:1 (Expenditure area 6), the government indicates the need for a closer analysis of which type of information an agency should be required to collate and report, which agency should be the recipient of reporting and how the proposal should be financed. The legal requirements also need to be clarified. The government also writes that "as well as the MSB's need for IT incident infor-

mation on the basis of the agency's coordinating role in the event of accidents and crises and the management of IT incidents, the Swedish National Police Board (RPS) may also require IT incident reporting". In the proposition, the government also stresses that an IT incident which involves criminal activity falls within the police area of responsibility. On 12 April 2012, the MSB was commissioned by the government to perform an in-depth analysis of mandatory IT incident reporting for government agencies. The findings will be presented by 1 December 2012 at the latest.

OBJECTIVES

To create a good understanding of the extent and focus of IT incidents affecting government agencies and other stakeholders in society.

MEASURES

Carry out an in-depth analysis of mandatory IT incident reporting, primarily for government agencies.

IMPLEMENTATION

The MSB is carrying out an in-depth analysis of mandatory IT incident reporting in accordance with the commission from the government.

3.3 Technical detection and warning system

Many stakeholders use protective mechanisms, such as intrusion detection systems, firewalls and anti-virus systems, to increase their information and IT security. IT intrusion detection and warning systems are an important tool in the work to construct a national situational assessment of actual and potential IT incidents and deviations from the norm. Such an information security-related situational assessment is a prerequisite for coordinated management of serious IT incidents. It is vital to be able to quickly detect and present the chain of events in the event of an IT incident. Should the national information security-related situational assessment indicate that a number of central stakeholders in society are simultaneously affected by coordinated intrusions, actual or potential, a different approach is required compared to an intrusion where only a single stakeholder is affected. Multiple different detection and warning systems with different tasks and requirements may be needed to build up a national information security-related situational assessment and also protect vital societal functions against attacks.

On 14 April 2010, the government commissioned FRA to submit proposals on how a technical detection and warning system for vital societal functions and critical infrastructure could be designed and introduced. On the same day, the MSB was commissioned by the government to develop a proposal defining which stakeholders would be able to introduce a technical detection and warning system for vital societal functions and critical infrastructure.

FRA and the MSB presented their findings on 1 March 2011. In Proposition 2011/12:1, the government states that both MBS's and FRA's reports constitute a basis for continued work and that the starting point should be that "those

agencies with a particular responsibility as regards crisis management in accordance with the appendix to Ordinance (2006:942) on emergency management and heightened alert should primarily be part of a national detection and warning system”.

On 10 November 2011, FRA was commissioned by the government to provide further information on the technical detection and warning system which the agency presented on 1 March 2011. FRA presented its in-depth examination of technical detection and warning systems on 2 April 2012. The commission was carried out in consultation with the Swedish Security Services and also entailed developing a pilot version of the proposed system.

OBJECTIVES

To establish a better national situational assessment of IT incidents and deviations from the norm - an information security-related situational assessment - by introducing different types of technical detection and warning systems. This creates conditions for coordinated action at the national level, which in turn makes it possible to avert or limit the consequences of serious IT incidents.

MEASURES

The work with technical detection and warning systems continues within the framework of the ordinary activities of the authorities included in SAMFI and other stakeholders. A particular requirement is the development of systems which can securely safeguard and manage information from the security and intelligence services.

IMPLEMENTATION

FRA is continuing work to develop a technical detection and warning system in accordance with the proposal presented to the government on 2 April 2012.

Other stakeholders are continuing work with the technical detection of IT incidents and warning systems within the framework of ordinary activities.

3.4 National cooperation on work with information security in the EU

In the digital agenda for Sweden, the government states that ”Sweden’s participation in international cooperation in the information security field should be further supported and developed”.¹⁰

Work carried out within the framework of the EU is of vital importance for the work to improve Sweden’s information security. As Sweden is a member of the EU, the union constitutes an important arena, amongst other things in regard to research and technology development, and normalisation, or in other words, various forms of legislation and other means of regulation, such as standardisation. It is therefore vital that Sweden is able to exert a constructive influence on the EU’s work with information security. For government agencies to be able support

10. *IT in the service of mankind – a digital agenda for Sweden* (Ministry of Industry, Employment and Communications), page 41.

Swedish actions, both expertise and experience of how EU's policies are formed and implemented are required. To influence the EU's work with information security, it is necessary to choose which issues and processes to prioritise. It is also important to coordinate available resources to achieve maximum effectiveness.

OBJECTIVES

Through increased national cooperation and active participation in information security work within the EU, Sweden can have a constructive influence on the EU's work in the information security field.

MEASURES

Active participation in information security work taking place within the framework of the EU and increased national cooperation in the EU's work with information security.

IMPLEMENTATION

The authorities included in SAMFI are working to enhance cooperation by means of their participation in the information security work being conducted by the EU. Work on these issues is taking place in close dialogue with the relevant agencies and departments at the Government Offices.

3.5 Plan, implement and evaluate information security exercises

Regular information security exercises within and between different sectors and at different levels of responsibility, are a prerequisite for developing and evaluating structures for managing IT incidents. The aim of the exercises can be, for example, to develop public-private partnerships and examine how joint situational assessments can be created and maintained. The European Commission encourages EU Member States to organise regular exercises to hone actions and practice restoring systems after large-scale IT incidents.¹¹

Information security exercises are an important part of national and international cooperation aimed at preventing and managing serious IT incidents. In November 2011, the exercise Cyber Atlantic was carried out involving the EU and the USA. In November 2010, the pan-European exercise Cyber Europe was carried out. Information security exercises are also carried out within the framework of Nato/PfP. In May 2010 and February 2008, technical information security exercises, so-called Cyber Defence Exercises (CDX) were carried out involving cooperation between stakeholders in Sweden (SAMFI, Swedish Defence Research Agency (FOI), FHS, etc.) and abroad. On 29-30 September 2010, the MSB, in cooperation with SAMFI, Svenska kraftnät [the Swedish national grid] and private stakeholders from the energy sector, carried out the first national information security exercise, named NISÖ 2010.

11. European Commission communication COM (2011)163.

OBJECTIVES

To develop Sweden's capacity for managing serious IT incidents through regular information security exercises within and between different sectors at different levels of responsibility, nationally and internationally.

MEASURES

Plan, implement and evaluate the national information security exercise NISÖ 2010 and a technical information security exercise during 2013, as well as future exercises.

Participate actively in work being carried out with information security exercises within the EU and Nato/PfP.

IMPLEMENTATION

The MSB is responsible for the exercise NISÖ 2010 and the technical information security exercise in 2013. The work is being carried out in cooperation with SAMFI, sector-specific agencies and private stakeholders.

The work with exercises related to critical information infrastructure protection (CIIP) and IT security within the EU is being carried out in close cooperation between PTS and the MSB.

Exercises within the framework of Nato/PfP are primarily being carried out in cooperation between the Swedish Armed Forces and the MSB.

Communications security

4. Communications security

Information management regularly occurs between multiple stakeholders which requires secure communications over telecommunications and data networks. For example, the Internet carries a large percentage of society's information flow. In this context, it is important to have robust critical functions in the infrastructure for electronic communications as well as secure cryptographic functions and signal protection. To ensure trust in information exchange, it is also vital that electronic services are based on well-functioning and secure systems.

4.1 Preventive measures to increase security in electronic communications

It is the responsibility of the telecommunications and Internet providers to ensure that the communication network is functioning and secure. Sometimes, however, society requires even greater operational security than that which businesses, having fulfilled legal requirements, can justify commercially. In these circumstances, society can act to finance preventive measures, such as strengthening electronic communications against serious disruptions and crises, for example sabotage, accidents and natural disasters. In many cases, work with preventive activities is an example of successful public-private partnerships. There have recently been a number of examples where financing has been provided, for example, for mobile base stations, back-up electrical power, dual connections and geological repositories. The measures undertaken are in line with the national strategy for robust electronic communications.

OBJECTIVES

To reduce the number of operational disruptions in the field of electronic communications and strengthen the ability of stakeholders within the sector to manage serious operational disruptions.

MEASURES

The following preventive measures with regard to physical and logical threats, training courses and information systems must be implemented to increase operational security in electronic communications.

- Map vulnerabilities in support systems and network components of providers within the electronic communications sector.
- Carry out function checks on protected installations within the electronic communications sector.
- Enhance access protection at installations for electronic communications.
- Plan, implement and evaluate a national crisis management exercise (Telö) for stakeholders within the electronic communications sector.
- Further develop the national system for robust and traceable time.
- Further develop the information systems Ledningskollen [cable check], Gemensam lägesuppfattning (GLU) [shared situational awareness] and Driftinformation för operatörer (DIO) [operational information for providers].
- Implement special training initiatives in the field of operational security in urban networks.
- Carry out a pilot study of the electronic communications requirements of vital societal functions.

IMPLEMENTATION

PTS is responsible for work in cooperation with relevant authorities and other stakeholders.

4.2 Measures for Steps to follow up security in the electronic communication sector

The amendments which came into force in the Swedish Electronic Communications Act (SFS 2003:389) on 1 July 2011 have introduced a new supervisory tool. Providers must now report significant operational security and privacy incidents to PTS. Within this framework, PTS has issued regulations for creating a clear regulatory framework for reporting these events.¹² This establishes an improved basis for supervisory work in the sector.

OBJECTIVES

To reduce the number of operational disruptions in the field of electronic communications and strengthen the ability of stakeholders within the sector to manage serious operational disruptions.

MEASURES

Important measures which must be taken to increase security in electronic communications include:

- Continue to develop routines for daily monitoring of operational disruptions and management of incident reports.
- Carry out an analysis of supervisory methodology when new mandates and tools have been added.
- Carry out a planned supervision of operational security at the Swedish top level domain .SE.
- Replace guidelines with regulations on operational security.
- Develop a regulation on security protection for electronic communications.

IMPLEMENTATION

PTS is responsible for work in cooperation with relevant authorities and other stakeholders.

4.3 Special initiative on the introduction of DNSSEC

A central function of the Internet is the so-called domain name system (DNS). In simple terms, it translates the addresses used (for example `www.myndigheten.se`) to IP addresses of the servers where the requested information is available or where the e-mail recipient can be found, etc.

When the DNS was originally designed, the focus was on issues other than security, for example the need to be able to easily and quickly connect further computers to the Internet. In later years, the need for security has come to the fore and a special addition to DNS, called DNSSEC, has been developed. DNSSEC is based on the answer in the form of, for example, an IP address which the domain name system provides being digitally signed. This prevents incorrect addresses being submitted without authorisation, which is a risk to which the original DNS is vulnerable. A secure DNS within all public organisations is fundamental to ensuring crisis management capacity in a digital world.

12. See PTSFS 2012:01 and PTSFS 2012:02.

DNSSEC is today considered to be an obvious benefit to website operators when information credibility requirements are high. In spite of this, and in spite of the guidelines developed by the eGovernment Delegation and the Swedish Association of Local Authorities and Regions (SKL), amongst others, the number of websites using DNSSEC within the public sector is surprisingly low. In 2011, municipalities have been able, via the county administrative boards, to apply for funding from the so-called emergency management allowance in the national budget to assist with the introduction of DNSSEC into its IT infrastructure. The work has had a significant impact and around a third of the country's municipalities have asked to take part. The work will be evaluated in 2012 but it is clear even now that further steps need to be taken to introduce DNSSEC in the remaining municipalities, as well as in authorities and agencies at the national, regional and county levels.

OBJECTIVES

To introduce DNSSEC into the majority of public organisations by the end of 2014.

MEASURES

Follow up the initiatives implemented in 2011 and continue work to introduce DNSSEC for the remaining domains within the public sector.

IMPLEMENTATION

The MSB and PTS in cooperation with .SE (Internet Infrastructure Foundation) and SKL.

4.4 Encryption for classified data

Agencies, municipalities, county councils and organisations need to protect their sensitive and classified information. If the information relates to national security, it must be protected by signal protection systems approved by the Swedish Armed Forces.¹³ The Encryption for classified data (KSU) system is available for other classified information. The KSU system has been approved by the Swedish Armed Forces after review. The purpose of KSU is to ensure that quality-assured and commercially available products, together with a regulatory framework developed by the Swedish Armed Forces and a management structure adapted to the organisation, will be able to increase the level of security as it currently stands. By using KSU systems approved by the Swedish Armed Forces, organisations can easily ensure that components and recommended management structures provide secure and effective protection for the data the organisation is aiming to protect.

One file encryption is currently KSU approved. KSU-level encryption systems approved by the Swedish Armed Forces and intended, for example, for mobile, voice and data communications, connection encryption over Virtual Private Networks (VPNs) and for USB memory encryption, should be further developed.

13. In accordance with Article 13 of the Security Protection Ordinance (1996:633)

OBJECTIVES

To expand and develop KSU such that classified information handled by agencies, county councils, municipalities and other organisations is protected by encryption for classified data.

MEASURES

Propose solutions to economic and legal aspects of introducing KSU.

IMPLEMENTATION

The Swedish Armed Forces in cooperation with the MSB, FRA and other relevant agencies.

4.5 Develop Swedish Government Secure Intranet (SGSI)

To enable secure communications with EU Member States and bodies via the European Commission's TESTA (Trans-European Service for Telematics between Administrations) network, a national network, SGSI (Swedish Government Secure Intranet) has been established in Sweden. SGSI can also be used for secure information exchange between Swedish agencies. Communications between the agencies are encrypted with a nationally approved signal protection system. The MSB is the system owner of SGSI.

SGSI today provides added value for connected agencies. The number of agencies connected to SGSI should increase without an increase in costs. This should be made possible by more effective control of network administration.

OBJECTIVES

To increase the number of agencies connected to SGSI, to operate the network more efficiently and to future-proof network security.

MEASURES

Maintain and in certain respects develop security work on the SGSI. Develop network services requested by users.

IMPLEMENTATION

The MSB is responsible for implementation, partly in cooperation with the relevant authorities in SAMFI.

4.6 Accessible and protected communications infrastructures for the public sector

For over a decade, the ability to create and exchange digital information in ever greater quantities has been of fundamental importance to Swedish authorities. That the changes involve a gradual escalation from local solutions to more joint solutions is characteristic of this digital development. For Swedish e-government, it is becoming more and more evident that local solutions are not appropriate, either in terms of function or security.

In its activities, each agency must by law strive for high efficiency and good housekeeping with government funds. In accordance with the Government

Agencies Ordinance (SFS 2007:515), the agency must also develop its activities and, through cooperation with agencies and others, work to safeguard the benefits to be gained by the individual and the state as a whole. Global changes also create significant pressure of public administration and place great demands on efficiency.¹⁴

The eGovernment Delegation is working to develop a basis for joint solutions in which an essential starting point is viewing public administration in its entirety. As e-government gradually becomes accepted, certain agencies will need to communicate large quantities of sensitive information between themselves electronically. This requires not only confidentiality and secrecy, but also availability, integrity and traceability.¹⁵

Accessible and protected communications infrastructures for the public sector should be based on existing conditions in society. Amongst other things, this involves the use of existing infrastructure, adjustment to a vibrant and rapidly developing market and utilisation of the high technical competency that exists in both the private and public sector.

OBJECTIVES

Accessible and protected communications infrastructures for the public sector.

MEASURES

Continue work with accessible and protected communications infrastructures for the public sector.

IMPLEMENTATION

Work with accessible and protected communications infrastructures for the public sector is continuing within the framework of the mandates of the various stakeholders and in accordance with an upcoming government commission.¹⁶

14. *IT within public administration – have the agencies made reasonable efforts to ascertain whether outsourcing contributes to increased efficiency?* RiR 2011:4, Swedish National Audit Office, 2011.

15. *Strategy for the agencies' work with e-government.* Report by the eGovernment Delegation, SOU 2009:86.

16. In Proposition 2011/12.1 (Expenditure area 6), the government states that the Swedish Agency for Public Management will be commissioned to present a needs assessment in relation to accessible and protected communications infrastructures for the public sector.

**Security in
products and systems**

5. Security in products and systems

The long-term supply of secure IT products requires formal frameworks for evaluating and certifying security capabilities. These frameworks should be accepted nationally and internationally.

For example, in the fields of electricity and water distribution, rail transport and the petrochemical industry, IT systems are used to control and monitor physical processes. It is vital that industrial control systems have high levels of information security.

5.1 Develop encryption audit regulations for commercial products

The Swedish Certification Body for IT Security (CSEC) at FMV has a system for evaluating and certifying IT security in products and systems within the framework of the international agreement CCRA. The Swedish Armed Forces also have special responsibility with regard to approval of Encryption for classified data (KSU) for the individual agency, the national defence forces and international cooperation.

On behalf of the Swedish Armed Forces, FMV/CSEC has developed complementary regulations for encryption auditing within the framework of CSEC's certification scheme. These encryption audit regulations can form the basis for enabling commercial products to obtain KSU approval from the Swedish Armed Forces through CSEC certification in accordance with these encryption regulations.

OBJECTIVES

To create a Common Criteria-based system for encryption auditing in Sweden which can form the basis for enabling more commercial products to obtain KSU approval from the Swedish Armed Forces.

MEASURES

Develop encryption audit regulations within the FMV/CSEC certification scheme. Develop data and documentation, for example protocols, which can be used within the framework of KSU approval from the Swedish Armed Forces. License evaluation companies to carry out encryption auditing according to encryption audit regulations developed by FMV/CSEC and approved by the Swedish Armed Forces.

IMPLEMENTATION

FMV/CSEC is carrying out work with the support of the Swedish Armed Forces and the MSB.

5.2 Increased use of CC evaluated products

Increased application of Common Criteria (CC) as method support in specifying requirements can contribute to more secure IT products and systems. However, this requires that the standard's method package is also developed in a way that simplifies the application as much as possible.

It is reasonable to specify requirements for the utilisation of certified products, for example, within critical areas in the IT infrastructure with significant importance for communications security or for the security products that are used in organisations with stringent demands on confidentiality. A gradual escalation of the requirement methods used in procurement can be a path towards utilisation of CC. Simply requiring that the government agencies that participate in procurement must define their organisations' security requirements linked to that which is to be procured can be worthwhile as an initial measure. Object-oriented information measures are also of substantial value. Today, many CC-evaluated protection profiles (PP) have been made public. Increased access to protection profiles for requested security products should also enhance the requirements for effective security in IT products and systems.

OBJECTIVES

To provide support for Swedish agencies and other organisations procuring IT security products, through protection profiles developed by the authorities included in SAMFI. The protection profiles form the basis for minimum requirements for security functions and auditing products which are critical to organisations' information security.

MEASURES

Develop and certify protection profiles. Develop regulation from the MSB governing requirements for IT products' security capabilities based on the requirements in certified protection profiles. Develop guidelines and instructions for how organisations can use certified products to achieve effective information security.

IMPLEMENTATION

The work with protection profiles is being carried out by the MSB supported by FMV/CSEC and experts from other authorities included in SAMFI.

The work with regulations governing requirements for IT products' security capabilities is being carried out by the MSB in cooperation with FMV/CSEC and the Swedish Armed Forces and other stakeholders.

5.3 National evaluation laboratory

One of the main challenges in the information security field today is the extremely large amounts of information that can be stored on different types of portable computer equipment, e.g. USB sticks, mobile telephones and laptop computers. One of the most common causes of major losses of confidential data is theft or loss of such equipment. Encryption of information stored on portable computer equipment can prevent loss of confidential data in the majority of cases. However, encryption protection of this kind requires the ability to resist attackers with physical access to the found equipment. Such attackers can use different types of physical attack to reveal the encryption key, thereby gaining access to the encrypted information.

As knowledge of how to carry out these physical attacks is becoming more widespread and, at the same time, the equipment needed to carry out the attacks in many cases has become much cheaper, the risk of attacks of this kind has increased significantly. If the physical protection afforded by the encryption keys is incorrectly configured, there is an increased risk that a motivated attacker may successfully compromise the protection in found or stolen portable data equipment, even though the information is encrypted. There are many examples of where various forms of data protection in portable units have had serious deficiencies, resulting in the information being able to be read with no great effort.

Unlike other leading IT security countries (for example Great Britain, Germany, the Netherlands and Spain), Sweden currently lacks a national centre of excellence for analysing how such attacks are carried out and how such attacks can be prevented through appropriate technical solutions, even in cases where the

attacker has access to the data equipment. The consequence of this is that, in many cases, Swedish agencies and suppliers have to use other countries' facilities to get products tested. The lack of national competency in the field also means there is a significant risk that information in portable equipment does not have the promised protection.

A national centre of excellence in the field should be established. This centre of excellence should also be able to carry out evaluations of specific products to ensure that stored data has adequate physical protection. Evaluations should be recognised internationally by means of certification.

OBJECTIVES

Sweden must have the ability itself to analyse how physical attacks on information in portable data equipment can be carried out and prevented. National competency and the ability to evaluate and certify products to show they have adequate protection against physical attacks must also be available. Sweden must cooperate with other countries in Europe in the fields and be able to carry out internationally recognised certifications of this kind.

MEASURES

Analyse requirements for a national evaluation laboratory with the necessary competence and equipment to analyse physical attacks on information in computer equipment.

IMPLEMENTATION

FMV/CSEC are examining the requirements for a national evaluation laboratory in cooperation with the Swedish Armed Forces and FRA.

5.4 Increased security in industrial information and control systems (SCADA)

Industrial information and control systems (SCADA) are used in vital societal functions and critical infrastructure to control and monitor physical processes. Information and control systems are becoming increasingly accessible via public networks (for example, the Internet), are based more and more on commercially produced and available standard products and integrated to an ever greater extent into business systems. The ongoing development significantly modifies the risk assessment. In summary, the ability to prevent and manage, at the national level, IT-related risks and threats to industrial information and control systems in vital societal functions and critical infrastructure needs to be enhanced.

Security in industrial information and control systems is a cross-sector area where the responsibility of Swedish authorities lies with multiple agencies and supervisory authorities and extends to both normal activities and crisis situations. The security problems are similar in all sectors of society and there is no natural sector financing.

Cooperation between the private and the public sectors is a prerequisite for increasing security in industrial information and control systems. Where prac-

tical measures to increase security must be considered part of a natural commercial commitment to system users and owners, the private sector will bear the majority of the costs. However, the more qualified security issues have a bearing on national security and in this case central government plays a decisive role.

There are currently few Swedish stakeholders with more in-depth competency in the field and a clear commitment is required on the part of the government to guarantee sufficient resources and competency. National and international information sharing and cooperation requires an ability on the part of the Swedish government to develop its own unique knowledge, as well as an ability to evaluate and adapt knowledge developed by other stakeholders. Previous experience at both the national and international levels shows that practical activities are necessary to create the necessary partnership between the public and private sector. For the central government to be a leading stakeholder and cooperation partner, it has to show coordinated leadership, technical competency and continuity.

OBJECTIVES

To enhance an ability to prevent and manage, at national level, IT-related risks and threats to industrial information and control systems in vital societal functions and critical infrastructure.

MEASURES

Continue to implement the programme for increased security in industrial information and control systems (SCADA) initiated by the MSB in 2010 and concluding at the end of 2012. The programme is a coordinated national, cross-sectoral initiative which enables an efficient use of resources and enhances conditions for utilising initiatives implemented by responsible authorities in different sectors. Particularly important areas include information security in power supply and in transport systems.

Plan, implement and evaluate a programme for increased security in industrial information and control systems 2013-15.

IMPLEMENTATION

The MSB continues to carry out work in cooperation with the authorities included in SAMFI, agencies and supervisory authorities and private stakeholders who own and manage vital societal functions and critical infrastructure.

In 2012, the MSB is developing a proposal for a programme for 2013-15 in cooperation with relevant parties.

