Minimum standard for improving ICT resilience

Version May 2023, with update NIST SP 800-53 Rev. 5 and ISO 27001:2022

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
Federal Office for
National Economic Supply FONES

Preface

Digitalisation demands defensive action

Increasing levels of IT penetration and networking in almost all areas of life opens up both economic and social potential that a highly developed and industrialised nation like Switzerland cannot fail to act upon. At the same time, however, increasing digitalisation also gives rise to new threats to which we must respond quickly and decisively. The particular danger of targeted cyber attacks on IT infrastructures affects public-sector bodies, operators of critical infrastructures, and other businesses or organisations to the same degree.

These individual businesses and organisations have a fundamental responsibility to protect themselves. However, wherever the functioning of critical infrastructures is affected the state also has a responsibility, based on its remit as laid down in the Federal Constitution, and on the National Economic Supply Act. This Minimum ICT Standard is an expression of the responsibility of the state to protect its citizens, its economy, and its institutions and public administrations.

The Minimum ICT Standard comes into play in those areas in which a modern society can least afford outages: in those ICT systems that are important to the functioning of critical infrastructures. It is recommended that operators of critical infrastructures apply this Minimum ICT Standard or comparable requirements (e.g. ISO, Cobit, etc.). This document nonetheless offers any interested business or organisation a guide and specific instructions for action to improve its own ICT resilience.

Management Summary

This Minimum ICT Standard serves as a recommendation and potential guide to improving ICT resilience. It is aimed in particular at operators of critical infrastructures, but is essentially applicable to any business or organisation, and is freely available.

The Minimum ICT Standard is aimed in particular at ICT officers and members of the senior management of the operators of critical infrastructures.

This document is structured into three sections:

1. Background information: this part serves as a reference work and is intended to give readers a basic knowledge of ICT security.

2. Framework: the 'Framework' section gives users a set of specific activities to implement. These are structured under five headings: 'Identify', 'Protect', 'Detect', 'Respond' and 'Restore'. A total of 106 activities are set out here.

3. Assessment: businesses and organisations can use the 'Assessment' section and the associated scoring tool in Excel to evaluate their progress with implementing the measures, or have this progress audited by an external company. The findings can be used as a basis for benchmarking across organisations.

Contents

1 Section 1 – Introduction

1.1 Overview

Section 1 defines the foundations for and objectives of ICT security, sets out what this comprehensive topic covers and what it does not, and explains how the Minimum ICT Standard is to be used.

1.2 Legal foundations

The following underlying laws form the basis for NES action.[1]

- Federal Act on the National Economic Supply (National Economic Supply Act, NESA; SR 531)
- Ordinance on the Organisation of National Economic Supply (Organisation of National Economic Supply Ordinance; SR 531.11)
- Ordinance on Preparatory Measures for National Economic Supply (SR 531.12)

1.3 Background and objectives

Cybersecurity demands a risk-based approach and the use of secure systems within the individual operator's own area of responsibility. Many cyber attacks can be repelled at reasonable cost simply by taking the tried-and-tested precautions set out in this Minimum ICT Standard. Its aim is to give businesses and organisations a versatile tool that enables them to take independent action to improve the resilience of their ICT infrastructures. By taking a risk-based approach, the standard permits the implementation of different levels of defence, adjusted to the particular needs of the organisation.

1.4 Scope

This Minimum ICT Standard has been drawn up by the National Economic Supply (NES) organisation in cooperation with external cybersecurity experts.

A number of internationally recognised cybersecurity standards already exist. Most of these extend well beyond the present document (see section 1.4.1). This Minimum Standard explicitly does not seek to compete with the existing international standards. Rather, it is compatible with them while being more reduced in scope. It is intended to provide a more entry-level introduction to the issues, and yet ensure a high degree of protection.

As a complement to the present Minimum ICT Standard, NES has drafted further, sector-specific standards,[2] which go into greater (technical) detail. It is recommended that, as soon as they become available, operators of critical infrastructures base their actions on these detailed, sector-specific requirements in addition to this Minimum Standard.

If a sector already has its own standards, or if international standards such as ISO or NIST are used, businesses can use the checklist in Section 3, 'Assessment' to determine whether or not they already meet this Minimum Standard.

1.4.1 Foundation documents and standards

There are many different standards and sources of information around the world on dealing with cyber risks. Some of these are already recognised by businesses and are in use. The present Minimum ICT Standard is based on the NIST Cybersecurity Framework Core.[3] It has been supplemented with other internationally recognised industry standards where appropriate. The most important of these are the following:

1. NIST Guide to Industrial Control Systems (ICS) Security
   This guide is also issued and updated by the National Institute of Standards and Technology, and extends the NIST Cybersecurity Core Framework by specific requirements for handling industrial control systems (ICS), in particular, NIST Special Publication 800-82, revision 2, May 2015.[4]

[1] All of these legal texts can be found in the classified compilation of federal law. They can be found online at:
https://www.admin.ch/gov/en/start/federal-law.html.
The National Economic Supply Act is available in English. The ordinances are available in German, French and Italian

[2] These are currently available for the power supply and food supply sectors. Standards for other sectors are in progress and will be published upon completion.

[3] https://www.nist.gov/cyberframework

[4] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

2. ISO 2700x
   The International Organization for Standardization (ISO) publishes around a dozen mutually complementary standards on cybersecurity. These are referred to as the '2700x family'. The best-known of these is ISO 27001. It specifies the requirements for setting up, implementing, maintaining and continuously improving a documented information security management system compatible with the context of the organisation concerned.[5]

3. COBIT
   Control Objectives for Information and Related Technology (COBIT)[6]

4. ENISA Good Practice Guide on National Cyber Security Strategies.[7]

5. Federal Office for Information Security (Germany), BSI 100-2.[8]

1.4.2 Principles

1. Independent responsibility: operators of critical infrastructures have a fundamental independent responsibility to maintain their critical ICT processes.

2. Business continuity management: all aspects of cybersecurity should be integrated into an overarching business continuity management structure.

3. Risk management: those applying these standards must assess possible cyber risks – such as impairments to availability, integrity and confidentiality – on an ongoing basis. The business must judge which risks should be mitigated, and which it is willing to bear.

1.4.3 Measures and references in this document

Wherever possible, the authors have avoided duplicating information. Instead, they refer to other cybersecurity standards. Those applying this Standard are advised to consult the stated sources where necessary.

[5] https://www.iso.org/standard/66435.html

[6] http://www.isaca.org/COBIT/Pages/default.aspx

[7] https://www.enisa.europa.eu/topics/national-cyber-security-strategies

[8] https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html;jsessionid=2012D9CA020E153625E39AFEE673D910.1_cid341

1.5 Introducing the Minimum ICT Standard

This section presents the key issues addressed by the Minimum ICT Standard.

1.5.1 Principles of cybersecurity

A business must first define its cybersecurity principles before it can put them into effect in its operations. Specifically, it must answer the following questions:

- What is to be done?
- How is it to be done?
- Who is responsible?
- How will the outcome be measured?

Cybersecurity principles set out the rules, procedures, metrics and organisational structures which are required for effective planning and control.

1.5.2 Organisation and responsibilities

As a basis for cybersecurity, a business must have a general security organisation which defines clear tasks, responsibilities and authorities. This should also provide the framework for defining and implementing the defence-in-depth strategy. Cyber risks should form part of global risk management. This is key to recognising potential cyber threats and to defining the appropriate action. The security organisation must enable senior management to decide on the necessary resources. This level of management must also equip the security organisation with the proper powers to perform their core tasks without limitation in close cooperation with the various areas of the business.

1.5.3 Policy, directives and guidelines

Before a cybersecurity strategy (such as a defence-in-depth strategy) can be put into effect, the policy, procedures and working directives of an organisation must be identified, or in some cases defined.

Those responsible for cybersecurity must be notified of the business requirements of the various business units. These requirements must also be documented. They might be legal, financial, strategic or operational in nature, for example.

1.5.4 Risk management

Active risk management is a crucial element of improving ICT resilience by means of a defence-in-depth strategy. This should take the business's appetite for risk into account. It is therefore important that the organisational unit in charge of operating and maintaining ICT systems is familiar with the methods and procedures of risk management within the organisation, and is able to apply these to cyber risks. The aim of the cyber risk process is to identify potential threats to the ICT systems, applications and data that are to be protected, to assess them, and to define how the identified risks are to be dealt with. The overall risk process is broken down into three sub-processes: risk analysis, risk assessment and risk response (taking the appropriate action). To review the effectiveness of this action, risks are re-evaluated all the time, and any changes reported. Where necessary, action may then be amended accordingly.

There is no such thing as absolute security. That is why the management of the business must determine its appetite for risk.

1.6 Elements of a defence-in-depth strategy

1.6.1 The defence-in-depth concept

A business's cybersecurity strategy must be geared to protecting the critical ICT assets that are required for its business processes. This demands a multi-layered approach that is known internationally as 'defence in depth'. It refers to the coordinated use of multiple security measures to protect the ICT assets within the business. The strategy is based on the military principle that it is more difficult for an enemy to penetrate a complex, multi-layered system of defence than a single barrier. At the same time, the methods and modus operandi of potential attackers are observed as a basis for the corresponding defence plan. In a cybersecurity context, a defence-in-depth concept is designed to recognise breaches in ICT security, to respond to them, and to minimise or mitigate the consequences of those security breaches. Defence in depth takes an holistic approach which seeks to protect all (ICT) assets against all types of risk. The company's resources should be deployed to ensure effective protection against known risks, as well as comprehensive monitoring of potential future risks. The resulting measures must cover ICT systems in their entirety. This includes people, procedures, properties, data and devices. An attacker only poses a threat to an ICT system if they succeed in exploiting a vulnerability in one of these elements. Organisations and businesses must monitor their security measures continuously, and adapt them to new threats where necessary.

1.6.2 Industrial control systems (ICS)

The complex architecture of ICS means that, in the worst case, vulnerabilities can remain undetected for a very long time, and the corresponding exploits represent what is known as an advanced persistent threat (APT). Implementing a defence-in-depth concept, as described above, offers appropriate protection against these threats.

The following are typical methods of attacking ICS:

- Attacks via the internet to an ICS that is accessible online, with the aim of establishing permanent remote access.
- Remote access to the ICS using stolen access data.
- Attacks on ICS by exploiting vulnerabilities in the web interface.
- Planting malware in the ICS via compromised data carriers (e.g. USB sticks, smartphones, etc.)
- Attacks on office systems (e.g. via phishing mails, drive-by infections, etc.) with the aim of penetrating the ICS via any interface.

When implementing defence-in-depth concepts, it must be remembered that there are important differences between office systems and an ICS. Table 1 shows the security issues and their differing importance with regard to ICT and ICS.

Security topic	ICT (e.g. office systems)	ICS (e.g. nuclear power station management)
Anti-virus	Very common. Easily deployed and updated. Users have control over customisation. Anti-virus protection can be asset-based or enterprise-based.	Memory requirements and delays in data exchange caused by anti-virus software scans can impact negatively on an ICS system. Organisations can only protect legacy ICS elements with after-market solutions. In an ICS context, anti-virus solutions usually required 'exclusion' folders to avoid programs quarantining critical files.
Update management	Clearly defined, enterprise-wide, remote and automated.	Long lead and planning time to successful patch installation; OEM-specific; may (temporarily) halt ICS functionality. The acceptable risk in this regard must be defined.
Technology support life cycle	2–3 years, multiple providers, ongoing development and upgrades.	10–20 years, usually same vendor/service provider over the entire life cycle, product end-of-life creates new security threats.
Testing and audit methods	Use modern (poss. automated) methods. Systems are usually resilient and reliable enough to handle assessments during normal operation.	Automated assessment may be unsuitable, e.g. owing to the high degree of individual development. There is a greater probability of failure during testing, so assessments during normal operation tend to be more difficult.
Change management	Regular and scheduled. Geared to the organisation's requirements, to minimum/maximum period of use.	A complex procedure with a potential impact on the organisation's business activities. Strategic, individual planning required.
Asset classification	Common and performed annually. Results drive expenditure/investment.	Performed only when necessary/mandatory. Without an inventory, countermeasures may be out of proportion to the importance of the system elements.
Incident response and forensics	Easily developed and deployed. May be regulatory requirements (data protection) to observe.	Focused primarily on system resumption. Forensic procedures are immature.
Physical security	Ranges from poor (office systems) to excellent (secure data centres).	Physical security is typically excellent.
Secure software development	An integral part of the development process.	Historically, ICS have generally been designed as physically isolated systems. As a result, little thought was given to security as an integral part of system development. ICS vendors are maturing, but at a slower rate than in ICT. Core elements of ICS can be difficult to retrofit with security solutions, or none are available.
Security compliance	General regulatory requirements, depending on sector (and not in all sectors).	Specific regulatory guidance, depending on sector (and not in all sectors)

Table 1: Differences between ICT and ICS

The following factors must be taken into account when implementing a defence-in-depth concept in an ICS

- The cost of securing legacy systems according to contemporary needs
- The growing trend of connecting ICS with business networks
- The ability to offer users remote access, in both the ICT and ICS environments
- The need to trust the business's own supply chain
- Modern methods of monitoring and protecting ICS-specific protocols
- The ability to stay up to date on intelligence about emerging threats to ICS.

The defence-in-depth approach makes it more difficult to conduct direct attacks on ICT systems, and makes it more likely that conspicuous or unusual behaviour within the system will be detected at an early stage. This approach also makes it possible to create separate zones in which to implement intrusion detection technology. Table 2 shows the typical elements of a defence-in-depth strategy.

Elements of a defence-in-depth strategy	
Risk management programme	• Identify security threats • Risk profile • Detailed management of ICT asset inventory
Cybersecurity architecture	• Standards/recommendations • Policy • Procedures
Physical security	• Protection for field devices • Control centre access controls • Video surveillance, access controls & barriers
Network architecture	• Typical secure zones • Demilitarised zones (DMZ) • Virtual LANs
Network perimeter security	• Firewalls • Remote access & authentication • Jump servers/hosts
Host security	• Patch and vulnerability management • Field devices • Virtual machines • Hardening
Security monitoring	• Intrusion detection systems • Security audit logging • Security incident and event monitoring • System Monitoring • EDR/XDR
Vendor management	• Supply chain monitoring & management • Managed services & outsourcing • Use of cloud services
The human element	• Policy • Procedures • Training and awareness

Table 2: Elements of a defence-in-depth strategy

1.6.3 Risk management

1.6.3.1 Risk management programme

Before any defence-in-depth strategy can be implemented, the business risks to an organisation that are associated with cyber threats must be understood. These risks must be managed in accordance with the appetite for risk across the business as a whole. Those responsible for managing and maintaining ICT systems must be able to recognise, assess and address cyber risks. To do this, they must understand how these methods must be applied to their particular system landscape. This in turn requires a clear understanding of threat scenarios, operational and technical processes, and the technologies used. Only then can a defence-in-depth strategy be integrated in to normal day-to-day business. Management is responsible for ensuring a secure environment as fundamental to all computer-based activities within the organisation.

The principles for handling risk that are described above also apply in general. A number of ICT applications are nonetheless especially important owing to their criticality. These include industrial control systems (ICS) in particular. Designing an effective ICS security architecture demands that business risks be placed in relation to the functional (operational) requirements of the ICS. This may also relate to the physical world, such as perimeter defences around data centres. Decision-makers at all levels of the organisation must be aware of the importance of cyber risks and must play an active role in the risk management process. It is essential that selected systems, applications and processes, including the associated networks, are subject to regular risk analyses. Set strict specifications for these analyses, and take a structured and systematic approach.

1.6.3.2 Risk management framework

ICT risk analyses should be embedded in a risk management framework and conducted regularly on clearly defined subjects. Examples of scope include business-critical facilities, processes and applications (including those currently in development), as well as their dependencies on further systems, networks and services.

The objective of this risk management framework is to allocate the risks that are identified to responsible individuals or functions, who/which then monitor and assess them and take appropriate action to keep them within the limits that have previously been defined as acceptable (=risk appetite).

1.6.3.3 Risk analysis

The scope that the ICT risk analysis should cover should be defined clearly. The business processes that are affected and the technical elements concerned must be described along with possible external factors. Their weighting within the analysis should also be defined. These factors then determine the content and boundaries of the analysis.

1.6.4 Business impact analysis

A business impact analysis should identify the potential realistic and the potential worst-case impacts (on business operations) of ICT components (incl. individuals, data, processes, services and networks) being compromised. This should cover a range of areas, such as finance, operations, legal affairs, reputation and health.

Ultimately, the business must determine what effects on its operations it is willing to bear if the necessary ICT assets are not available as planned. Thus, the requirements and defence levels necessary to ensure the availability, integrity and usability of the identified ICT resources, as determined by acceptable risk, must be defined.

1.6.5 Action

Action to counter the risks described in the business impact analysis should be identified, reviewed, and approved. It should be released together with the plans for the exact steps that senior management will take.

Attention should also be paid here to establishing the residual risk to all assets in their relevant environments, and to dealing with that risk appropriately (e.g. mitigation, avoidance, transfer or acceptance) in line with the business's risk appetite.

In this way, the maximum permitted risk should be determined for each individual asset, so that (cumulated) ICT risks can be calculated.

1.6.6 Cybersecurity architecture

Cybersecurity architecture encompasses the specific measures taken and their strategic placement within the network to establish a layer of security in the sense of the defence-in-depth strategy. It should also permit information to be gathered on the data flow between all systems and their connections. The cybersecurity architecture should also be aligned with the physical inventory of facilities and ICT assets, to ensure an holistic understanding of the flows of information within the organisation.

The cybersecurity architecture should comply with the NIST Framework Core. It must offer protection for the confidentiality, integrity and availability of data, services and systems. An implementation plan should be drawn up for the cybersecurity architecture. This should be designed with the specific corporate culture and the business's strategic objectives in mind, but at the same time pay appropriate heed to the need for security, and the resources that this requires. The cybersecurity architecture is generally accompanied by an integrated task list which identifies expected outcomes (indications and triggers for further review and orientation), determines project timelines, supplies estimates of the required resources, and pinpoints significant project dependencies.

1.6.7 Physical security

Physical security measures reduced the risk of accidental or deliberate loss or damage to ICT assets belonging to the organisation or the surrounding environment. The assets to be protected include physical assets such as tools and plant equipment, the environment, the surrounding community and intellectual property, including proprietary data, such as process settings and customer information. In many cases, physical security controls must meet specific environmental, safety, regulatory, legal and other requirements. Organisations should tailor physical security controls, such as technical controls, to the type of protection needed. To ensure comprehensive defences, physical protection also covers the security of ICT components and data from the surrounding environment which is connected with the ICT. With many ICT infrastructures, security is closely linked to plant safety. This is to keep employees out of dangerous situations, without obstructing them in their work, or emergency procedures. Physical security controls are both active and passive measures which limit physical access to all elements of the ICT infrastructure. Below are a few examples of the incidents that such defences are intended to prevent:

- Unauthorised physical access to sensitive locations
- Physical modification, manipulation, theft or other removal or destruction of existing systems, infrastructure, communications interfaces or physical locations
- Unauthorised observation of sensitive facilities through visual observation, photographs, or any other means of recording information
- The unauthorised introduction or installation of new systems, infrastructure, communications interfaces or other hardware
- The unauthorised introduction of devices (USB sticks, wireless access points, bluetooth or mobile devices) designed to manipulate hardware, listen in on communications, or have any other damaging effect.

To meet the requirements for information security, physical assets, including systems and network equipment, office equipment (e.g. network printers and multifunction devices), as well as special equipment (e.g. industrial control systems) must be protected for their entire life cycle, from acquisition (purchase or lease), through maintenance, to their disposal.

Mobile devices (including laptops, tablets and smartphones) and their data must also be protected against unauthorised access, loss and theft, by configuring their security settings appropriately, limiting access to them, installing security software, and managing all devices centrally.

1.6.8 Hardware life cycle management

The acquisition (purchase or lease) of durable, reliable hardware should always conform to security requirements. Possible vulnerabilities in the hardware should always be identified.

The aim is to ensure that the hardware always offers the required level of functionality, and does not impair the security of critical or sensitive information and systems for the whole of its life cycle.

1.6.9 Mobile device configuration

To protect data from unauthorised access, loss and theft, mobile devices (including laptops, tablets and smartphones) should always have a standard configuration which confirms to the security requirements.

The aim of this standard configuration is to guarantee the information security of stored or transmitted data on the mobile device, even if it is lost or stolen.

1.6.10 Industrial control systems

Industrial control systems must be monitored and controlled in accordance with the level of protection that they require. These systems demand particular technological and physical protection, specifically in order to guarantee that supply-related processes continue to run.

1.6.11 ICS network architecture

When designing a network architecture, it is generally worth separating ICS networks from the wider corporate network. There is a difference in the type of data traffic that these two networks carry: internet access, FTP, email and remote access are generally permitted within the corporate network, but not within the ICS network. ICS data that is carried via the corporate network could be intercepted or exposed to DDoS or man-in-the-middle attacks. Separating the corporate network and the ICS network, or severely restricting connectivity, can minimise security and performance problems with the ICS network.

1.6.12 ICS network perimeter security

The costs of installing an ICS and the need to maintain a homogeneous network infrastructure often mean that a connection is required between the ICS and the corporate network. This connection presents a considerable security risk, and should be protected by technical means. If the networks have to be connected, it is urgently recommended that only minimal connections are permitted (single ones, if possible) and that the connection is made via a firewall and DMZ (a separate network segment). ICS servers which receive data from the corporate network must be placed in a DMZ. External connections must be known, and limited to minimal access via the firewall. Data exchange can be monitored and subject to plausibility testing by means of additional systems which are able to detect anomalies.

1.6.13 Host security

A further layer of security must be implemented at host or workstation level. Firewalls protect most devices against intrusion from outside. That said, a good security model requires multiple layers of defence. For the network to be comprehensively secured, all hosts must also be secured. This type of host security layer should allow a user to use a variety of operating systems and applications, while also affording the devices themselves suitable protection.

A set of password rules must be drawn up for all users on a system, and known accounts (such as 'Administrator') must be renamed. Users may circumvent restrictive password rules by keeping their passwords in a non-secure way (e.g. noting them down), or by repeatedly using similar passwords. The complexity of how passwords are determined should reflect the particular user's level of authority. Password change cycles are another option here.

Organisations should implement the following general recommendations for each ICS host and each device that has access to the corporate network. These apply irrespective of operating system:

- Install and configure a host-based firewall
- Use screen savers with short intervals and with a password requirement to log in, if possible
- Operating systems must be patched and firmware kept up to date
- Configure logs on all devices
- Deactivate services and accounts that are not used
- Insecure services, such as telnet, remote shell and rlogin must be replaced by secure alternatives such as SSH
- Users should not be able to disable services
- Make and test system backups, especially if they are not controlled centrally
- Security modules provided by the operating system, such as security scanners, should be activated or replaced by suitable software
- The same policy applies to laptops and other mobile devices which are not continuously connected to the corporate network. In addition, the hard disks of mobile devices should be encrypted.

1.6.14 Security monitoring

The use of monitoring systems and network components which detect anomalous behaviours and attack signatures add further complexity to an IT or ICS environment. These monitoring and detection functions are vital to a defence-in-depth concept of protecting critical assets. An electronic boundary around an ICS network is not enough to protect those critical assets from unauthorised access. According to the defence-in-depth concept, a monitoring system should give an organisation an early warning of any security incident. Most organisations have a certain standard form of monitoring for their IT environment – but most do not have the same for their ICS networks.

The following are essential:

- Conduct regular, thorough and independent audits of security status (critical business environments, processes, applications and supporting systems and networks)
- Monitor information risks, comply with the security-related elements of legal, regulatory and contractual requirements, and report regularly to senior management about information security

1.6.15 Information security strategy

Defining, maintaining and monitoring a comprehensive information security strategy enables senior management to determine a clear policy and helps them enforce those requirements, as well as in risk management.

1.6.16 Vendor management

Vendor management involves identifying and managing information risks connected with external providers (i.e. vendors of hardware and software, providers of outsourced services, and cloud service providers, etc.). The inclusion of information security requirements in formal contracts should minimise risk here.

1.6.17 The human element

Organisations face a range of challenges in handling the mistakes and deliberate actions of people within the ICT environment. Technical measures can never fully rule out incorrect operation, whether malicious or not. The more inexperienced or untrained staff within a business, the more susceptible it is to having its systems manipulated. Combating the activities of insiders with malicious intentions is a further challenge. When dealing with these challenges, businesses must address the following issues:

1.6.17.1 Staff employment cycles

Information security should form part of the entire employment cycle, from appointment until departure. This includes security-related measures, such as the surrender of working tools (hardware, access to systems), or for access to buildings and other premises, and the attendant security responsibility. An appropriate training programme for staff should not only raise their awareness of security matters, but also define 'secure' conduct. The organisation should document the status and conduct of such training courses.

The aim is to ensure that staff are equipped with the skills, knowledge and tools that they need to uphold the organisation's values and to comply with information security policy.

1.6.17.2 Directives/policies

Clear, practicable directives and policies for staff govern their conduct when dealing with security-related issues. They provide a framework and permit controls to be carried out in order to protect systems and enforce those policies. They also lay down the procedures that staff must follow, and define what the organisation expects of them. Policies and directives set the rules of compliance, and what sanctions apply in the event of an infringement.

1.6.17.3 Procedures

Security management falls within the responsibility of IT security, and is organised in terms of procedures. Its role is to protect corporate information and data. Organisations are also required to apply security management procedures to industrial control systems. This means defining procedures, the steps that must be taken, or how a certain system should be configured. These procedures should be standardised and repeatable. In this way, new staff are always trained to the same, consistent level of security, and it can be ensured that they are familiar with all of the necessary regulations and standards. The intrusion detection procedure is particularly important. Meanwhile, network-based security procedures take on a special significance in connection with manufacturer-specific protocols and legacy systems.

1.6.17.4 Roles and responsibilities in critical business environments

Roles and responsibilities in critical business environments, procedures, applications (including supporting systems/networks) and information should be clearly defined and allocated to capable individuals.

The aim is to foster a sense of independent responsibility among staff. The corporate culture that this creates helps to ensure that staff have information security in mind when going about their work.

1.6.17.5 Communications/security awareness programme

A security awareness programme and the associated communications encourages awareness and the desired behaviour of all staff at all hierarchical levels of the business.

The aim is to achieve a corporate culture which encourages the desired secure conduct on the part of the individual. Each of these individuals should be enabled to take risk-based decisions within their particular sphere of influence.

1.7 The NIST Framework

The objective of the NIST Framework and its recommendations is to provide operators of critical infrastructures and other organisations which are dependent on ICT with a tool enabling them independently and on their own responsibility to improve their resilience in the face of cybersecurity risks. The Framework is based on a selection of existing standards, guidelines, and best practice specifications, and is technology-neutral.

1.7.1 The NIST Framework Core

The NIST Framework Core is risk-based. It consists of five functions:

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

1.7.2 Implementation tiers

The NIST Framework has four implementation tiers. These describe the practices that a business has instituted, in other words its level of protection. They range from partial (tier 1) to adaptive (tier 4). To determine its own tier level, an organisation should have a thorough knowledge of its risk management practices, the threat environment, legal and regulatory requirements, business objectives, and organisational requirements.

2 Part 2 – Implementation

2.1 Overview

This section describes the tasks that must be completed to implement the minimum ICT standard. It is structured according to to the five functions of the NIST Framework Core (see 1.7.1). These five functions are: Identify, Protect, Detect, Respond and Recover. The tasks that must be completed (see table below) are categorised as follows:

In each case, the first two letters (e.g. 'ID' = 'Identify) refer to one of the five functions. The second pair of letters then refers to the category (e.g. 'AM' = 'Asset Management'). Finally, the number designates the individual task. They are numbered sequentially within the category. For example, 'ID.AM-1' corresponds to the first task in the asset management category under the Identify function.

An additional table of references to other international ICT standards has been added to each table listing tasks from the NIST Framework Core. These tables each reference a particular category, such as asset management. They are intended to make it easier for users which organise their ICT security according to other standards to map the present standard against their own.

2.2 Identify

2.2.1 Asset management

The data, individuals, devices, systems and facilities of an organisation are identified, catalogued and rated. Their rating should correspond to their criticality in the business processes that must be completed, and the organisation's risk strategy.

Description	Task
ID.AM-1	Draw up an inventory-taking process which ensures that you have a complete inventory of all your ICT assets at all times.
ID.AM-2	Produce an inventory of all of the software platforms/licences and applications within your organisation.
ID.AM-3	Catalogue all of your internal communication and data flows.
ID.AM-4	Catalogue all external ICT systems that are relevant to your organisation.
ID.AM-5	Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.
ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.

Table 3: ID.AM tasks

Standard	Reference
CCS CSC 1	1, 2
COBIT 5	BAI09.01, BAI09.02, BAI09.05, DSS05.02, APO02.02, APO03.03, APO03.04, PO01.02, DSS06.03
ISA 62443-3:2013	SR 7.8
ISO 27001:2022	A.5.2, A.5.3, A.5.9, A.7.9, A.5.12, A.5.14 A.5.32, Clause 7.1, Clause 7.2
NIST-SP-800-53 Rev. 5	AC-4, CA-3, CA-9, PL-8, CM-8, AC-20, SA-9, CP-2, RA-2, SA-20, PS-7, PM-2, PM-5, PM-29, SA-17, SC-6, RA-9
BSI 100-2	M 2.225, M 2.393, B 2.10, M 2.193

Table 4: ID.AM references

2.2.2 Business environment

The business's objectives, tasks and activities are rated and prioritised. This information is used as a basis for allocating responsibilities.

Description	Task
ID.BE-1	Identify, document and communicate the exact role of your business within the (critical) supply chain.
ID.BE-2	The importance of the organisation as a critical infrastructure operator, and its position within the critical sector, is identified and communicated.
ID.BE-3	Objectives, tasks and activities within the organisation are prioritised and rated.
ID.BE-4	Catalogue all external ICT systems that are relevant to your organisation.
ID.BE-5	Prioritise the resources that you have inventoried (devices, applications, data, etc.) based on their criticality

Table 5: ID.BE tasks

Standard	Reference
CCS CSC 1	1, 2
COBIT 5	BAI09.01, BAI09.02, BAI09.05, DSS05.02, APO02.02, APO03.03, APO03.04, PO01.02, DSS06.03
ISA 62443-3:2013	SR 7.8
ISO 27001:2022	A.5.19, A.5.21, A.5.23, A.5.24, A.5.28, A.5.29, A.5.30, A.5.31, A.5.33, A.5.37, A.6.2, A.7.11, A.7.12, A.7.5, A.8.14, A.8.6, A.8.30, Clause 4.1
NIST-SP-800-53 Rev. 5	CP-2, CP-8, PM-8, PM-11, PE-9, PE-11,RA-9, SA-20, SR-1, SR-2, SR-3
BSI 100-2	B 1.11, M 2.256, B 2.2, B 2.12, M 2.214

Table 6: ID.BE references

2.2.3 Governance

Governance determines responsibilities, monitors, and ensures compliance with regulatory, legal and operational requirements from the business environment.

Description	Task
ID.GV-1	Organizational cybersecurity policy is established and communicated.
ID.GV-2	Information security roles and responsibilities are coordinated with internal roles (e.g. those in risk management) and external partners.
ID.GV-3	Ensure that your organisation complies with all statutory and regulatory cybersecurity requirements, including those applicable to data protection.
ID.GV-4	Ensure that cybersecurity risks are embedded in business-wide risk management structures.

Table 7: ID.GV tasks

Standard	Reference
COBIT 5	APO01.03, EDM01.01, EDM01.02, APO13.02, MEA03.01, MEA03.04, DSS04.02
ISA 62443-3:2013	
ISO 27001:2022	A.5.1, A.5.19, A.5.30, A5.31, A.6.2, A.6.6, A.8.27, A.8.30 A15.1.1, Clause 6
NIST-SP-800-53 Rev. 5	AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PM-1, PM-2, PS-1, PT-1, RA-1, SA-1, SC-1, SI-1, SR-1, PM-3, PM-7, PM-9, PM-10, PM-11, PM-28, PM-29, RA-1, RA-2, RA-3, SA-2, PS-7, PS-9
BSI 100-2	M 2.192, M 2.193, M 2.336, B 1.16

Table 8: ID.GV references

2.2.4 Risk assessment

The organisation understands the effects of cybersecurity risks on business operations, assets and individuals, including reputational risks.

Description	Task
ID.RA-1	Identify the (technical) vulnerabilities of your assets, and document them.
ID.RA-2	Share intelligence regularly in fora and other bodies to stay up to date about cybersecurity threats.
ID.RA-3	Identify and document internal and external cybersecurity threats.
ID.RA-4	Identify the possible business impacts of cybersecurity threats, and calculate the probability of their occurring.
ID.RA-5	Rate the risks to your organisation based on threats, vulnerabilities, impacts (on business activity) and probabilities.
ID.RA-6	Define possible immediate responses should a risk occur, and prioritise these measures.

Table 9: ID.RA tasks

Standard	Reference
COBIT 5	APO12.01, APO12.02, APO12.03, APO12.04, APO 12.05, APO 13.02, DSS04.02
ISA 62443-3:2013	4.2.3, 4.2.3.9, 4.2.3.12
ISO 27001:2022	A.5.37, A.5.6, A.5.7, A.6.1, A.8.12, A8.14, A.8.16, A,8.2, A.8.3, A.8.7, A.8.8, Clause 6.1.2, Clause 6.1.3, Clause 8, Clause 8.3, Clause 9.3
NIST-SP-800-53 Rev. 5	CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5, PM-15, PM-16, SI-5, RA-3, SI-5, PM-12, RA-2, PM-9, PM-11, SA-14
BSI 100-2	M 2.35, M 2.199, M 2.546

Table 10: ID.RA references

2.2.5 Risk management strategy

Determine the priorities, constraints and maximum risk tolerances of your organisation.
On this basis, assess your operational risks.

Description	Task
ID.RM-1	Establish risk management processes, manage them actively and have them confirmed by the persons/stakeholders concerned.
ID.RM-2	Define and communicate your organisation›s maximum risk tolerance.
ID.RM-3	Ensure that maximum risk tolerance is calculated taking into account your organisation's importance as an operator of a critical infrastructure. This calculation should also be informed by sector-specific risk analyses.

Table 11: ID.RM tasks

Standard	Reference
COBIT 5	APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02, APO12.06
ISA 62443-3:2013	4.3.4.2, 4.3.2.6.5
ISO 27001:2022	A.6.1, A.8.2, A.8.3, Clause 6.1.3, Clause 8.3, Clause 9.3
NIST-SP-800-53 Rev. 5	PM-8, PM-9, PM-11, PM-28, RA-9

Table 12: ID.RM references

2.2.6 Supply chain risk management

Determine priorities, constraints, and the maximum risks that your organisation is willing to accept in connection with supplier-related risks.

Description	Task
ID.SC-1	Establish clear procedures to manage supply chain risks. Have these procedures reviewed and agreed by all of the stakeholders involved.
ID.SC-2	Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.
ID.SC-3	Place your suppliers and service-providers under a contractual obligation to develop and implement appropriate measures to meet the objectives and requirements of the supply chain risk management process.
ID.SC-4	Establish a system of monitoring to ensure that all of your suppliers and service-providers are fulfilling their obligations as required. Have this confirmed on a regular basis by audit reports or technical test results.
ID.SC-5	Work with your suppliers and service-providers to define response and recovery procedures following cybersecurity incidents. Conduct drills to test these procedures.

Table 13: ID.SC tasks

Standard	Reference
COBIT 5	APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05
ISA 62443-3:2013	4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14, 4.3.2.6., 4.3.2.5.7, 4.3.4.5.11 7
ISO 27001:2022	A.5.19, A.5.20, A.5.21, A.5.22, A.5.29, A.6.6, A.8.30, Clause 8.3
NIST-SP-800-53 Rev. 5	AU-6, CA-2, CA-7, CP-2, CP-4, IR-3, IR-4, IR-8, IR-9, PS-7, PM-9, PM-30, RA-3, SA-4, SA-9, SA-11, SA-15, SR-1, SR-2, SR-3, SR-5, SR-6
BSI	B 1.11, B 1.17, M 2.256, B 1.3

Table 14: ID.SC references

2.3 Protect

2.3.1 Access management

Ensure that physical and logical access to ICT assets and facilities is restricted to authorised individuals, processes and devices, and that they can be used only for permitted activities.

Description	Task
PR.AC-1	Establish a clearly defined procedure for granting and managing permissions and access data for users, devices and processes.
PR.AC-2	Ensure that only authorised individuals have physical access to ICT assets. Take action (on building security, for example) to ensure that ICT assets are protected from unauthorised physical access.
PR.AC-3	Establish procedures by which to manage remote access.
PR.AC-4	Define permission levels according to the principle of least privilege, as well as separation of functions.
PR.AC-5	Ensure that the integrity of your network is protected. Segregate your network both logically and physically where necessary and sensible.
PR.AC-6	Ensure that digital identities are allocated to unambiguously authenticated individuals or processes.
PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).

Table 15: PR.AC tasks

Standard	Reference
COBIT 5	DSS05.04, DSS06.03, DSS01.04, DSS05.05, APO13.01, DSS01.04, DSS05.03, DSS05.04, DSS05.05, DSS05.07, DSS06.03, BAI08.03
ISA 62443-3:2013	SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.13, SR 2.1, SR 2.6, SR 3.1, SR 3.8, SR 2.2, SR 2.3
ISO 27001:2022	A.5.14, A.5.15, A.5.16, A.5.17, A.5.18, A.5.21,A.5.22, A.5.23, A.5.3, A.5.34, A.6.1, A.6.7, A.7.1, A.7.2. A.7.3, A.7.4, A.7.5, A.7.6, A.7.9, A.8.1, A.8.5, A.8.11, A.15, A.8.16, A.8.18, A.8.2, A.8.3, A.8.5, A.8.20, A.8.22, A.8.27, A.8.31
NIST-SP-800-53 Rev. 5	AC-1, AC-2, AC-3, AC-4, AC-5, AC-6, AC-10, AC-14, AC-16, AC-17, AC-19, AC-20, AC-24, SC-15, IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, IA-8, IA-9, IA-10, IA-11, IA-12, PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, PE-9, SC-7, SC-10, SC-20, PS-3
BSI	M 2.30, M 2.220, M 2.11, M 4.15, M 1.79, M 2.17, B 2.2, B 2.12, B 5.8, B 4.1, M 2.393, M 2.5, B 1.18, M 2.220, M 2.8, M 4.135, B 4.1, M 5.77, M 2.393, M 2.5, M 3.33, M 2.31, M 2.586, M 4.135

Table 16: PR.AC references

2.3.2 Awareness and training

Ensure that your staff and external partners receive appropriate, regular training on all cybersecurity matters. Ensure that your staff and external partners perform their security-related tasks in accordance with the related requirements and procedures.

Description	Task
PR.AT-1	Ensure that all members of staff are informed and trained on cybersecurity.
PR.AT-2	Ensure that higher-level users are particularly aware of their role and responsibility.
PR.AT-3	Ensure that all third-party stakeholders (suppliers, customers and partners) are aware of their role and responsibility.
PR.AT-4	Ensure that all managers are aware of their particular role and responsibility.
PR.AT-5	Ensure that those in charge of physical security and information security are aware of their particular role and responsibility.

Table 17: PR.AT tasks

Standard	Reference
COBIT 5	APO07.03, BAI05.07, APO07.02, DSS06.03, APO07.03, APO10.04, APO10.05
ISA 62443-3:2013	4.3.2.4.2, 4.3.2.4.3
ISO 27001:2022	A.5.19, A.5.2, A.5.4, A.6.2, A.6.3, A.6.6, A. 7.2, A.7.3, A.7.6, A.8.18, A.8.2, A.8.3, A.8.30, Clause 5.1, Clause 5.3
NIST-SP-800-53 Rev. 5	AT-2, AT-3, CP-3, IR-2, PM-13, PM-14, PS-7, SA-9
BSI	M 2.193, B 1.13

Table 18: PR.AT references

2.3.3 Data security

Ensure that information, data and data carriers are managed in a way which protects the confidentiality, integrity and availability of the data in accordance with the organisation's risk strategy.

Description	Task
PR.DS-1	Ensure that stored data is protected (against violations of confidentiality, integrity and availability).
PR.DS-2	Ensure that data is protected while in transit (against violations of confidentiality, integrity and availability).
PR.DS-3	Ensure that you have a formal procedure in place for your ICT assets which protects data upon removal, transfer or the replacement of those assets.
PR.DS-4	Ensure that your ICT assets have sufficient capacity to ensure data availability is maintained.
PR.DS-5	Ensure that appropriate action has been taken to prevent data leaks.
PR.DS-6	Establish a procedure to check the integrity of firmware, operating systems, application software and data.
PR.DS-7	Provide a development and testing IT environment which is completely separate from productive systems.
PR.DS-8	Establish a procedure to check the integrity of the hardware you use.

Table 19: PR.DS tasks

Standard	Reference
COBIT 5	APO01.06, BAI02.01, BAI06.01, DSS06.06, BAI09.03, APO13.01, BAI07.04, BAI03.05.4
ISA 62443-3:2013	SR 3.4, SR 4.1, SR 3.1, SR 3.8, SR 4.1, SR 4.2, SR 7.1, SR 7.2, SR 5.2
ISO 27001:2022	A.5.7, A.5.10, A.5.13, A.5.14, A.5.15, A.5.23, A.5.24, A.5.29, A.5.33, A.5.34, A.6.1, A.6.2, A.6.5, A.6.6, A.7.5, A.7.8, A.7.9, A.7.10, A.7.14, A.8.1, A.8.11, A.8.12, A.8.13, A.8.14, A.8.16, A.8.18, A.8.19, A.8.2, A.8.20, A.8.22, A.8.23, A.8.24, A.8.26, A.8.28, A.8.29, A.8.31, A.8.34, A.8.3, A.8.4, A.8.6, A.8.7, A.8.8
NIST-SP-800-53 Rev. 5	AC-4, AC-5, AC-6, AU-4, AU-13, CM-2, CM-8, MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, CP-2, PE-11, PE-16, PE-19, PE-20, PS-6, SA, 10, SC-5, SC-7, SC-8, SC-11, SC-28, SI-4, SI-7, SI-10
BSI	M 2.217, B 4.1, M 2.393, B 5.3, B 5.4, B 5.21, B 5.24, B 1.7, M 2.3, B 1.15, M 5.23, M 3.33, M 2.226, M 3.2, M 3.6, B 1.18, M 2.220, M 2.8, M 4.135, M 4.494, M 5.77, M 2.393, B 5.3, M 3.55, B 5.4, B 5.21, B 5.24, B 1.7, B 1.6, B 1.9, B 5.4, B 5.21, B 5.24, M 2.62, M 2.4

Table 20: PR.DS references

2.3.4 Information protection processes and procedures

Draw up policies to protect information systems and assets. Apply these policies to protect those information systems and assets.

Description	Task
PR.IP-1	Draw up a baseline configuration for your information and communication infrastructure, as well as for industrial control systems. Ensure that this baseline configuration complies with typical security principles (e.g. N-1 redundancy, least-functionality configuration, etc.).
PR.IP-2	Establish a life cycle procedure for the use of ICT assets.
PR.IP-3	Establish a procedure to monitor configuration changes.
PR.IP-4	Ensure that backups of your information are conducted, maintained and tested on a regular basis (check that you are able to revert to your backups).
PR.IP-5	Ensure that you comply with all (regulatory) requirements and policies concerning your physical assets.
PR.IP-6	Ensure that data is destroyed according to requirements.
PR.IP-7	Ensure that your information security procedures are enhanced and improved continuously.
PR.IP-8	Share information about the effectiveness of various protection technologies with your partners.
PR.IP-9	Establish response procedures for any cyber incidents that may occur. (Incident response planning, business continuity management, incident recovery, disaster recovery.)
PR.IP-10	Test response and recovery plans.
PR.IP-11	Embed aspects of cybersecurity in the staff recruitment process at an early stage (e.g. by conducting background checks and individual security checks).
PR.IP-12	Develop and implement a procedure for dealing with identified vulnerabilities.

Table 21: PR.IP tasks

Standard	Reference
COBIT 5	BAI10.01, BAI10.02, BAI10.03, BAI10.05, APO13.01, BAI06.01, BAI01.06, APO13.01, DSS01.04, DSS05.05, BAI09.03, APO11.06, DSS04.05, DSS04.03, APO07.01, APO07.02, APO07.03, APO07.04, APO07.05
ISA 62443-3:2013	SR 7.6
ISO 27001:2022	A.5.10, A.5.11, A. 5.19, A.5.24, A.5.26, A.5.27, A.5.29, A.5.30, A.5.31, A.5.33, A. 5.35, A.5.36, A.5.37, A.5.5, A.5.6, A.5.7, A.6.1, A.6.2, A.6.4, A.6.5, A.6.6, A.6.8, A.7.10, A.7.11, A.7.12, A.7.13, A.7.14, A.7.5, A.7.8, A.5.8, A. 8.1, A.8.13, A.8.19, A.8.25, A.8.27, A.8.29, A.8.32, A.8.7, A.8.8, A.8.9, A.8.13, Clause 9, Clause 10
NIST-SP-800-53 Rev. 5	AC-21, CA-2, CA-7, CA-8, CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, CP-1, CP-2, CP-4, CP-6, CP-7, CP-9, CP-10, IR-1, IR-3, IR-7, IR-8, IR-9, MP-6, PE-1, PL-2, PM-6, PM-14, PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, RA-1, RA-3, RA-5, SA-3, SA-4, SA-8, SA-10, SA-11, SA-21, SI-2, SI-4, SR-12
BSI	B 1.4, B 1.3, M 2.217, B 1.14, B 1.9, M 2.62, B 5.27, M 4.78, M 2.9, B 1.0, M 2.80, M 2.546, B 5.27, B 5.21, B 5.24

Table 22: PR.IP references

2.3.5 Maintenance

Ensure that maintenance and repair work to components of the ICT system and/or the ICS are conducted in accordance with policies and procedures.

Description	Task
PR.MA-1	Ensure that the operation and maintenance of, and any repairs to assets are logged. Ensure that such work is conducted promptly and uses only those means which have been tested and approved.
PR.MA-2	Ensure that maintenance work on your systems that is carried out via remote access is logged. Ensure that no unauthorised access is possible.

Table 23: PR.MA tasks

Standard	Reference
COBIT 5	BAI09.03, DSS05.04, APO11.04, DSS05.02, APO13.01
ISA 62443-3:2013	
ISO 27001:2022	A.5.14, A.5.15, A.5.19, A.5.22, A.6.7, A.7.13, A.8.2, A.8.9, A.8.15, A.8.16
NIST-SP-800-53 Rev. 5	MA-1, MA-2, MA-3, MA-4, MA-5, MA-6
BSI	M 2.17, M 2.4, M 2.218, M 2.4, B 1.11, B 1.17, M 2.256

Table 24: PR.MA references

2.3.6 Protective technology

Install technical security solutions in accordance with requirements and procedures to ensure the security and resilience of your ICT systems and their data.

Description	Task
PR.PT-1	Define requirements for audits and log records. Produce and check the regular logs in accordance with those requirements and policies.
PR.PT-2	Ensure that removable media are protected, and that they are used only in accordance with policy.
PR.PT-3	Ensure that your system is configured so that a minimum level of functionality is guaranteed at all times.
PR.PT-4	Ensure that your communications and control networks are protected.
PR.PT-5	Ensure that mechanisms (e.g. failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.

Table 25: PR.PT tasks

Standard	Reference
COBIT 5	APO11.04, DSS05.02, APO13.01, BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05
ISA 62443-3:2013	SR 2.3, SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.4, SR 2.5, SR 2.6, SR 2.7, SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.2, SR 7.6
ISO 27001:2022	A.5.14, A.5.15, A.5.18, A.5.29, A.5.30, A.5.34, A.5.37, A.8.11, A.8.13, A.8.14, A.8.15, A.8.16, A.8.20, A.8.21, A.8.22, A.8.2, A.8.3, A.8.34, A.8.5, A.8.6, A.8.9, A.9.2, A.5.10, A.6.7, A.7.10, A.7.14, A.8.13, A.8.24
NIST-SP-800-53 Rev. 5	AC-3, AC-4, AC-17, AC-18, AU-1, AU-2, AU-3, AU-6, AU-7, AU-12, AU-13, AU-14, AU-16, CM-7, CP-7, CP-8, CP-11, CP-12, CP-13, MP-1, MP-2, MP-3, MP-4, MP-5, MP-7, MP-8, PE-11, PL-8, SC-6, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43
BSI	B 5.22, M 2.500, M 2.220, M 2.64, M 4.227, M 2.64, B 1.18, B 4.1, M 2.393, B 1.3, B 2.4, B 2.9

Table 26: PR.PT references

2.4 Detect

2.4.1 Anomalies and events

Ensure that anomalies (abnormal behaviours) and security-related events are detected swiftly and that the potential impact of incidents is understood.

Description	Task
DE.AE-1	Define a baseline for permitted network operations and expected data flows for users and systems. Manage these values continuously.
DE.AE-2	Ensure that detected cybersecurity incidents are analysed to understand their targets and methods.
DE.AE-3	Ensure that information on cybersecurity incidents is aggregated and correlated from multiple sources and sensors.
DE.AE-4	Determine the impact of possible events.
DE.AE-5	Define the thresholds above which cybersecurity incidents trigger an alert.

Table 27: DE.AE tasks

Standard	Reference
COBIT 5	DSS03.01, APO12.06
ISA 62443-3:2013	SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2
ISO 27001:2022	A.5.24, A.5.25, A.5.27, A.5.28, A.5.37, A.8.1, A.8.12, A.8.15, A.8.16, A.8.20, A.8.21, A.8.7, A.8.8
NIST-SP-800-53 Rev. 5	AC-4, AU-6, CA-3, CA-7, CM-2, CP-2, SI-4, AU-6, IR-4, IR-5, IR-8, SC-16, SI-4, RA-3, RA-5
BSI	B 1.8

Table 28: DE.AE references

2.4.2 Security continuous monitoring

Ensure that ICT systems, including all assets, are monitored at regular intervals to detect cybersecurity incidents, and also to verify the effectiveness of protective measures.

Description	Task
DE.CM-1	Monitor networks continuously to detect potential cybersecurity events.
DE.CM-2	Continuous monitoring/surveillance of all physical assets and buildings to detect cybersecurity incidents.
DE.CM-3	Establish a system to monitor ICT use on the part of your staff, to detect potential cybersecurity incidents.
DE.CM-4	Ensure that malware can be detected.
DE.CM-5	Ensure that malware can be detected on mobile devices.
DE.CM-6	Ensure that the activities of external service providers can be monitored so that cybersecurity incidents can be detected.
DE.CM-7	Monitor your system continuously to ensure that activities or access by unauthorised persons, devices and software are detected.
DE.CM-8	Vulnerability scans are performed.

Table 29: DE.CM tasks

Standard	Reference
COBIT 5	DSS05.01, DSS05.07, APO07.06, BAI03.10
ISA 62443-3:2013	SR 6.2, SR 3.2, SR 2.4
ISO 27001:2022	A.5.14, A.5.15, A.5.18, A.5.19, A.5.21, A.5.23, A.5.7, A.6.7, A.7.1, A.7.2, A.7.4, A.7.8, A.7.9, A.8.1, A.8.11, A.8.12, A.8.15, A.8.16, A.8.19, A.8.2, A.8.20, A.8.21, A.8.23, A.8.28, A.8.3, A.8.30, A.8.5, A.8.7, A.8.8
NIST-SP-800-53 Rev. 5	AC-2, AU-12, AU-13, CA-7, CM-3, CM-8, CM-10, CM-11, PE-6, PE-20, PS-7, RA-5, SA-4, SA-9, SC-5, SC-7, SC-18, SC-44, SI-3, SI-4, SI-8
BSI	B 5.22, M 2.500, B 1.6, B 2.9, B 1.9, B 5.25, B 1.11, M 2.256, M 2.35

Table 30: DE.CM references

2.4.3 Detection processes

Processes and instructions for detecting cybersecurity incidents are cultivated, maintained and tested.

Description	Task
DE.DP-1	Define clear roles and responsibilities so that there is no doubt about who is responsible for what, and who holds what authority.
DE.DP-2	Ensure that detection processes comply with all requirements and conditions.
DE.DP-3	Test your detection processes.
DE.DP-4	Communicate detected incidents to the relevant actors (e.g. suppliers, customers, partners, authorities, etc.).
DE.DP-5	Improve your detection processes continuously.

Table 31: DE.DP tasks

Standard	Reference
COBIT 5	DSS05.01, APO13.02, APO12.06, APO11.06, DSS04.05
ISA 62443-3:2013	SR 3.3, SR 6.1
ISO 27001:2022	A.5.2, A.5.26, A. 5.27, A.5.3, A.5.35, A.5.4, A.6.3, A.6.8, A.7.4, A.8.12, A.8.15, A.8.16, A.8.17, A.8.27, A.8.6, A.8.7, A.8.8, A.8.9, Clause 5.3, Clause 7.2, Clause 9.2, Clause 10.1
NIST-SP-800-53 Rev. 5	AC-1, AT-1, AU-1, AU-6, CA-1, CA-2, CA-7, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PL-2, PM-1, PM-14, PS-1, PT-1, RA-1, RA-5, SA-1, SC-1, SI-1, SI-3, SI-4, SR-1, SR-9, SR-10
BSI	M 2.193, M 2.568, B 1.8

Table 32: DE.DP references

2.5 Respond

2.5.1 Response planning

Draw up a response plan to address detected cybersecurity incidents. Ensure that this response plan is executed promptly and properly in any incident.

Description	Task
RS.RP-1	Ensure that the response plan is executed promptly and properly during or after a detected incident.

Table 33: RS.RP tasks

Standard	Reference
COBIT 5	BAI01.10
ISA 62443-3:2013	
ISO 27001:2022	A.5.26, A.5.28, A.5.29
NIST-SP-800-53 Rev. 5	CP-2, CP-10, IR-4, IR-8
BSI	B 1.8

Table 34: RS.RP references

2.5.2 Communications

Ensure that your response procedures are coordinated with internal and external stakeholders. Ensure that, should an event occur, you receive support from public-sector bodies if necessary and appropriate.

Description	Task
RS.CO-1	Ensure that all individuals are familiar with their response and the sequence of their actions if and when a cybersecurity incident occurs.
RS.CO-2	Define reporting criteria and ensure that cybersecurity incidents are reported and processed in accordance with these criteria.
RS.CO-3	Share information and findings about detected cybersecurity incidents in accordance with the defined criteria.
RS.CO-4	Coordination with stakeholders occurs consistent with response plans.
RS.CO-5	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.

Table 35: RS.CO events

Standard	Reference
COBIT 5	
ISA 62443-3:2013	
ISO 27001:2022	A.5.2, A.5.24, A.5.26, A.5.3, A.5.30, A.5.37, A.5.5, A.5.6, A.6.3, A.6.8, A.7.4
NIST-SP-800-53 Rev. 5	AU-6, CP-2, CP-3, IR-3, IR-4, IR-6, IR-8, PM-15, SI-5
BSI	B 1.3, B 1.8, M 2.193

Table 36: RS.CO references

2.5.3 Analysis

Ensure that regular analyses are conducted to permit an effective response to cybersecurity incidents.

Description	Task
RS.AN-1	Ensure that notifications from detection systems are noted and investigated.
RS.AN-2	Ensure that the impact of a cybersecurity incident is properly understood.
RS.AN-3	Conduct a forensic analysis after any incident that occurs.
RS.AN-4	Categorise incidents that occur in accordance with the requirements of the response plan.
RS.AN-5	Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers).

Table 37: RS.AN tasks

Standard	Reference
COBIT 5	DSS02.07
ISA 62443-3:2013	SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1
ISO 27001:2022	A.5.19, A.5.25, A.5.26, A.5.27, A.5.28, A.5.35, A.5.5, A.5.6, A.6.3, A.8.15, A.8.16, A.10.2
NIST-SP-800-53 Rev. 5	AU-6, AU-7, CA-1, CA-2, CA-7, CP-2, IR-4, IR-5, IR-8, PE-6, PM-4, PM-15, RA-1, RA-3, RA-5, RA-7, SI-4, SI-5, SR-6
BSI	B 5.22, M 2.500, M 2.64, B 1.8

Table 38: RS.AN references

2.5.4 Mitigation

Act to prevent the further spread of a cybersecurity incident and to limit the potential damage.

Description	Task
RS.MI-1	Ensure that cybersecurity incidents can be contained and their further spread blocked.
RS.MI-2	Ensure that the impact of cybersecurity incidents can be mitigated.
RS.MI-3	Ensure that newly identified vulnerabilities are reduced or documented as accepted risks.

Table 39: RS.MI tasks

Standard	Reference
COBIT 5	
ISA 62443-3:2013	SR 5.1, SR 5.2, SR 5.4, A.12.2.1, A.16.1.5
ISO 27001:2022	A.5.26, A.8.23, A.8.8
NIST-SP-800-53 Rev. 5	IR-4, CA-2, CA-7, RA-3, RA-5, RA-7
BSI	B 1.6, B 1.8, M 2.35

Table 40: RS.MI references

2.5.5 Improvements

Ensure that your organisation's capacity to respond to cybersecurity incidents improves continuously by learning lessons from previous incidents.

Description	Task
RS.IM-1	Ensure that the findings and lessons of previous cybersecurity incidents are incorporated into your response plans.
RS.IM-2	Update your response strategies.

Table 41: RS.IM tasks

Standard	Reference
COBIT 5	BAI01.13
ISA 62443-3:2013	
ISO 27001:2022	A.5.27, A.10.1, Clause 10
NIST-SP-800-53 Rev. 5	CP-2, IR-4, IR-8
BSI	B 1.8

Table 42: RS.IM references

2.6 Recover

2.6.1 Recovery planning

Ensure that recovery procedures are (can be) maintained and executed to guarantee that systems can be restored swiftly.

Description	Task
RC.RP-1	Ensure that recovery plans can be executed properly after any cybersecurity incident.

Table 43: RC.RP tasks

Standard	Reference
COBIT 5	DSS02.05, DSS03.04
ISA 62443-3:2013	
ISO 27001:2022	A.5.29, A.5.30, A.5.37
NIST-SP-800-53 Rev. 5	CP-10, IR-4, IR-8

Table 44: RC.RP references

2.6.2 Improvements

Ensure that your recovery procedures improve continuously by learning lessons from previous recoveries.

Description	Task
RC.IM-1	Ensure that the findings and lessons of previous cybersecurity incidents are incorporated into your recovery plans.
RC.IM-2	Update your recovery strategy.

Table 45: RC.IM tasks

Standard	Reference
COBIT 5	BAI05.07
ISA 62443-3:2013	
ISO 27001:2022	A.5.27, A.10.1, Clause 10
NIST-SP-800-53 Rev. 5	CP-2, IR-4, IR-8

Table 46: RC.IM references

2.6.3 Communications

Coordinate your recovery activities with internal and external partners, such as internet service providers, CERT, the authorities, system integrators, etc.

Description	Task
RC.CO-1	Ensure that public perceptions of your organisation are addressed actively.
RC.CO-2	Ensure that your organisation is perceived positively once again after any cybersecurity incident.
RC.CO-3	Communicate all of your recovery activities to internal stakeholder groups, and especially also to (senior) management.

Table 47: RC.CO tasks

Standard	Reference
COBIT 5	EDM03.02
ISA 62443-3:2013	
ISO 27001:2022	A.5.24, A.5.26, A.5.5, A.6.3, Clause 7.4
NIST-SP-800-53 Rev. 5	CP-2, IR-4

Table 48: RC.CO references

3 Section 3 – Assessment

3.1 Introduction

This section describes the steps to be taken in a periodic review of the completeness and effectiveness of the action that has been taken. The outcome of this review should be a statement about the maturity of the organisation's own cybersecurity. It should permit a comparison within a given sector, or across sectors.

The measures presented here to improve ICT resilience (see Section 2) remain useless if they are not implemented at company level. It is important that those in charge understand the importance of cybersecurity issues, that the awareness of staff and partners is raised, and that sufficient resources are planned and made available to implement these measures. It is recommended that an assessment of this minimum standard be conducted at least annually, and action needed to improve resilience taken as quickly as possible.

Security is not a static state that can be achieved. Security is a process which must be conducted, evaluated, amended and improved continually. Cybersecurity can no longer be ignored. There is no time like the present to take appropriate action to improve the resilience of your critical ICT assets.

Each of the tasks presented in Section 2 must be scored on a scale of 0 to 4 (please refer to the scoring system set out below in 3.2.1). These scores form the basis for an evaluation of an organisation's tier level (see Section 3.3).

3.1.1 Task scoring system

0 = Not implemented
1 = Partially implemented, not fully defined and adopted
2 = Partially implemented, fully defined and adopted
3 = Implemented, fully or largely implemented, static
4 = Adaptive, implemented, continuously reviewed, improved

3.2 Description of an organisation's tier level

Tiers range from partial (tier 1) to adaptive (tier 4), and describe a growing degree of maturity. Organisations should determine their target tier level, ensuring that their chosen level meets their particular organisational goals.

The next section presents detailed descriptions of the four tier levels.

3.2.1 Tier 1: partial

Tier level 1 reflects risk management processes and organisational cybersecurity requirements which have not been formalised. Thus, cybersecurity risks are generally managed on an ad-hoc or reactive basis. There is an integrated risk management programme at the organisational level, but no institutionalised awareness of cybersecurity risks or an organisation-wide approach to managing them. Typically, the organisation will not have procedures in place to make coordinated use of information on cybersecurity. Similarly, in many cases, where cybersecurity risks occur the organisation will not have standardised procedures by which to share information or to coordinate collaboration with external partners.

3.2.2 Tier 2: risk informed

Organisations which classify themselves into tier 2 typically have risk management procedures in place to counter cybersecurity risks. However, they are not implemented in the form of specific instructions that staff must follow. At the organisational level, cybersecurity risks are integrated into the company-wide risk management system, and there is a certain awareness at all levels of the business. That said, such organisations usually lack company-wide approaches to managing and improving awareness of current and future cybersecurity risks. Approved procedures and processes are defined and implemented. Staff have sufficient resources to fulfil their roles in connection with cybersecurity. Cybersecurity information is shared within the organisation on an informal basis. The organisation understands its role in the broader environment and communicates with external partners (e.g. customers, suppliers, service providers, etc.) on cybersecurity issues. There are no standardised procedures for cooperating or for sharing information with these partners, however.

3.2.3 Tier 3: repeatable

Organisations at tier level 3 have formally approved risk management plans, as well as requirements for their implementation throughout the business. Policies applicable to the company as a whole define how cybersecurity risks are to be handled. The cybersecurity risks that are recorded as standard, as well as the requirements for dealing with them, are updated regularly. These updates factor in changes to business needs, technical developments and a changing threat landscape – as a result of new actors, for example – or political shifts.

Procedures and processes for dealing with these new risks are defined in writing. The organisation uses standardised methods to respond to changes in risk. Staff have the knowledge and skills they need to fulfil their roles.

The organisation understands its dependencies upon external partners, and regularly shares information with them that enables its management to take decisions in response to incidents.

3.2.4 Tier 4: adaptive

Tier level 4 means that an organisation meets all of the requirements for tier levels 1–3 in full, and also reviews its own procedures, methods and capabilities continuously, improving them where necessary. This continuous improvement is based on the complete documentation of all cybersecurity incidents. The organisation analyses past incidents and learns the necessary lessons, adapting its own procedures and the security technologies it uses dynamically to advances in cybersecurity technologies or changing threat situations. Cybersecurity risk management is an integral part of the corporate culture. Findings from previous incidents, and information from external sources and from the business's ongoing monitoring of its own systems and networks is integrated continually into the risk management process. The organisation shares information with partners all the time, for which it has standardised procedures in place.

3.3 Interpreting the assessment – an example

The figure below shows an example of a notional interpretation of all of the tasks described earlier in this document. The assessment can be conducted using the Excel file that can be downloaded from the website of the Federal Office for National Economic Supply.[9]

The diagrams shown below tell users about their organisation's degree of cybersecurity maturity in each of the five categories (ID-Identify, PR-Protect, DE-Detect, RS-Response, RC-Recover). All of the tasks in each of the five categories are scored between 0 and 4 (the coloured line). The dotted line shows the average for each category. The diagram to the top left (the cybersecurity maturity score) shows the overall score formed by the average figures for the individual categories.

Please note that these diagrams are examples only, and do not show guideline or target values. Each organisation must determine its own appetite for risk, and thus define the corresponding level of defence (for each category).

[9] https://www.bwl.admin.ch

Example of how an assessment is evaluated.

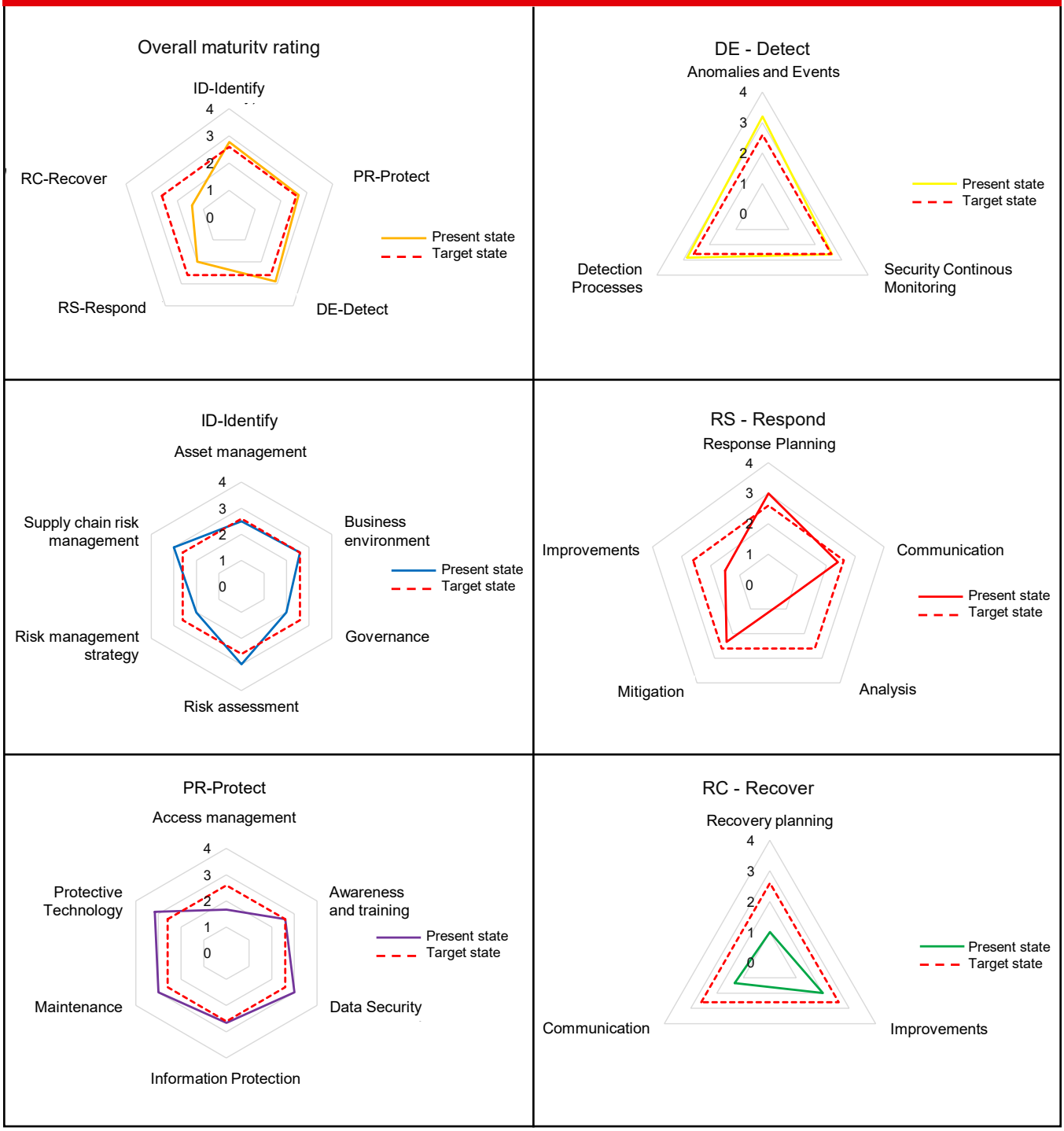

Figure 1: Example of how an assessment is evaluated.

4 Appendix

4.1 List of figures

4.2 List of tables

4.3 Glossary

This glossary lists terms that have a specific meaning in the context of this document. It does not list terms that are in common use in the ICT field, such as hardware, software, backup, etc.

Term	Definition
Benchmarking	A benchmark is a measure of comparison. 'Benchmarking' thus describes a comparative analysis of processes or outcomes. In this document, it explicitly refers to a comparison with organisations targeting a similar level of defence.
Cyber attack	Cyber attacks refer to all deliberate activities designed to impair the availability, integrity or confidentiality of data.
Drive-by infection	A drive-by infection refers to a computer being infected by malware (e.g. viruses, trojans, etc.), simply by visiting a website. Calling up such a website is sufficient to infect the computer.
Hardware life cycle management	Hardware life cycle management is a comprehensive approach to managing ICT hardware throughout its useful life.
Host security	Host security comprises all security measures implemented on the field device. These include firewalls and anti-virus software, for example.
ICS network perimeter security	Perimeter security refers to security at the point at which data is transferred from the corporate network to a public network such as the internet. Perimeter security is achieved by means of perimeter firewalls, which offer a strategic first line of defence against attacks.
ICT infrastructure	All elements of information and communications technology equipment which an organisation requires to perform its business processes. Examples include desktop PCs, mobile telephones, data centres, etc.
Industrial control systems	'Industrial control systems' is a collective term for all of elements that are used to control and monitor facilities or industrial processes. An industrial control system typically comprises sensors, data centres, control centres, communication lines and industrial facilities. 'Supervisory control and data acquisition system' (SCADA) is used as a synonym for 'industrial control system' (ICS).
Information security management system (ISMS)	An information security management system (ISMS) is a company-wide management system which effectively ensures that the organisation's target information security and continuity levels are maintained in the long term.
Intrusion detection systems	An intrusion detection system is a system which detects attacks on a computer system or network. The IDS may back up a firewall, or also run directly on the computer system being monitored.

Term	Definition
Compromised	A system, database or even an individual data set is regarded as compromised if it is possible that data could have been manipulated and if the owner (or administrator) of the system has lost control over correct functioning or correct content.
Critical infrastructure	The spectrum of critical infrastructures spans nine sectors, divided into 27 sub-sectors (industries). The full list is available online at: https://www.babs.admin.ch/en/aufgabenbabs/ski/kritisch.html
Legacy systems	Legacy systems are out-of-date systems that, for whatever reason, can no longer be replaced. Such systems may present a particular risk, and thus require the appropriate action to ensure their security.
Man-in-the-middle attacks	A man-in-the-middle attack (MITM attack) is a form of attack used on ICT networks. The attacker places themselves either physically or – in most cases today – logically between the two communication partners, and their system takes complete control of the data traffic between two or more network users. They are thus able to read any information they choose, and even manipulate it.
Mobile device configuration	'Mobile device configuration' refers to all technical measures and settings designed to protect data on mobile devices (smartphones, laptops, etc.), even if the device is physically lost.
Phishing mail	'Phishing', derived from 'fishing' refers to attempts to collect a user's personal data via fake websites, e-mails or text messages, the ultimate aim being identity theft.
Security awareness programme	The objective of a security awareness programme is to improve awareness of security issues, and the appropriate behaviours, among staff, partners, suppliers, etc.
Security monitoring	Security monitoring describes the process by which data flows and network activity in an organisation's own network are observed continuously. The aim is to detect conspicuous behaviour at an early stage. Dedicated security monitoring systems are used to this end.

Project structure

Project Principal
Werner Meier, Federal Office for National Economic Supply
Delegate NES

Project lead
Daniel Caduff, Hans-Peter Käser
Federal Office for National Economic Supply
Deputy Head of Secretariat ICT Division

Strategic Lead
Marcel von Vivis, National Economic Supply

Authors

Operational Lead
- Reto Häni, National Economic Supply
  Head, Infrastructure Operators Department

Experts
- Urs Küderli, National Economic Supply
  Expert Infrastructure Operators Department, PwC
- Christian Weigele, National Economic Supply
  Expert Infrastructure Operators Department, SAP
- Candid Wüest, National Economic Supply
  Expert Infrastructure Operators Department, Symantec
- Marc Holitscher, National Economic Supply
  Expert Infrastructure Operators Department, Microsoft
- Markus Pfyffer, National Economic Supply
  Expert Infrastructure Operators Department, IBM
- Hansruedi Münger, National Economic Supply
  Expert Infrastructure Operators Department, ATOS

Contact information

Federal Department of Economic Affairs,
Education and Research EAER
Federal Office for National Economic Supply FONES

Bernastrasse 28, CH-3003 Bern
info@bwl.admin.ch, www.bwl.admin.ch
Tel. +41 58 462 21 71

Licence

Please cite the document as follows:

Federal Office for National Economic Supply FONES:
Minimum standard for improving ICT resilience', Bern, 2018.
Revision May 2023, NIST SP 800-53 Rev. 5 and ISO 27001:2022