Swedish Civil Contingencies Agency

Critical infrastructure protection

Increased resilience through risk management, business continuity management, information and cybersecurity, and managing unwanted events

Critical infrastructure protection – Increased resilience through risk management, business continuity management, information and cybersecurity, and managing unwanted events

Civil Preparedness Department

Cover photographs: Mikael Svensson/Johnér
Production: Advant

Publication number: MSB2536 – December 2024
ISBN: 978-91-7927-589-1

Content

Introduction

Introduction

The changing world and security policy developments place increased demands on society's actors to be able to maintain vital societal functions. In order for vital societal functions to be maintained, critical infrastructure needs to aim to, as far as possible, function in everyday life, during a peacetime crisis, during threat of war, and ultimately during war.

In order for Sweden to function and be defended in war, all actors, both public and private, need to take responsibility for strengthening society's resilience and have the ability to continue operating their critical infrastructure even during a crisis and ultimately during war.[1] Those who provide critical infrastructure need to create a resilience in the organisation and it's activities as this is a basic condition for Sweden's preparedness. This may involve reducing the probability of risks occurring or ensuring access to resources in the form of staff, goods, services, and information.

The need to work with resilience in critical infrastructure has increased in recent years, not least as part of the development of civil preparedness. Efforts to strengthen the resilience of critical infrastructure have also accelerated as part of EU cooperation. Member States shall implement two EU directives, CER[2] and NIS2[3], which provide for clearer regulation in this area. The two directives are aimed at the actors providing critical infrastructure and require increased resilience.

1. Government Bill 2020/21:30 Total Defence 2021–2025.

2. **Directive (EU) 2022/2557 of the European Parliament and of the Council** of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

3. **Directive (EU) 2022/2555 of the European Parliament and of the Council** of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

Fact box on CER and NIS2

CER Directive: The Critical Entities (providers of critical infrastructure) Resilience Directive. The CER Directive requires Member States to ensure that operators of critical infrastructure have the capability to prevent, withstand, and manage disruptions or interruptions in the activities.

NIS2 Directive: Directive on measures for a high common level of cybersecurity across the Union. The NIS2 Directive requires Member States to protect network and information systems used to provide essential services and ensure the continuity of such services when they are exposed to incidents, thereby contributing to the security of the Union and to the efficient functioning of its economy and society.

The support will be updated when the CER and NIS2 directives are implemented in Swedish legislation.

Fundamental areas to work with to build resilience are risk management, business continuity management, information and cybersecurity, and managing unwanted events. These areas intersect, have complementary perspectives and form a foundation for an organisation's preparedness and security work. The work not only contributes to a more robust organisation, but also strengthens the resilience of society as a whole.

Purpose

The purpose of this supporting document is to describe in greater detail what actors providing critical infrastructure, at a minimum, need to work on in order to increase resilience and what is included in this work.

Target group

The support is aimed at all private and public actors who provide critical infrastructure, but can be used by anyone who wants to create conditions for continuing their organisation's activities during crises and wars.

How the support is intended to be used

The support consists of checklists based on national and international standards and sector-specific guidance on risk management, business continuity management, information and cybersecurity, and managing unwanted events. They are intended to provide support for what an actor providing critical infrastructure, at minimum, needs to work on to create the conditions to be able to maintain the activities. The support is generic so it can be used by all types of organisations.

The support is also intended to be used to better coordinate work with the different areas.

The appendix contains a cross-reference to the standards and sector-specific guidance on which the checklists are based, as well as a link to the relevant regulations.

The support does not describe how the work can be carried out, but guides what needs to be included to create resilience in critical infrastructure. The support does not contain any dimensions or capability requirements for the critical infrastructure.

Support for the development of resilience is available in the publication *Planeringsinriktning för civil beredskap – Ett underlag till stöd för fortsatt planering* (MSB2194).

List of terms

Critical infrastructure
'Critical infrastructure' refers to activities, services or infrastructure that maintain or ensure societal functions necessary for the basic needs, values or safety of society.[4] In this context, activities are to be understood as a broader concept. Activities, services or infrastructure also include facilities, processes, systems and nodes.

Vital societal function
'Vital societal function' refers to a societal function necessary for the basic needs, values or safety of society[5], such as Care of children and pupils, payment services, and land transport. These are maintained and ensured by critical infrastructure.

Resilience
The ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident.[6]

4. Ordinance (2022:524) on Central Government Authorities' Preparedness.
5. Identification of critical infrastructure: list of vital societal functions (MSB1844 – October 2021).
6. **Directive (EU) 2022/2557 of the European Parliament and of the Council** of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

Resilience in critical infrastructure

Resilience in critical infrastructure

To create a foundation and to provide a complementary perspective for an organisation's security and preparedness work, it is necessary to work with risk management, business continuity management, information and cybersecurity, and managing unwanted events. Systematic work is key to creating resilience in critical infrastructure.

By working systematically, conditions are created for preventing, preparing, resisting and managing unwanted events. The work with:

- Risk management is based on managing the risks that can affect the activities of the organisation. By systematically identifying, analysing, evaluating and addressing risks, the organisation can manage uncertainties in its environment.[7] The work contributes to minimising financial, staff, functional or information losses, and to a more effective recovery when an unwanted event occurs.
- Business continuity management is based on what is to be delivered and the resources needed for it. The work focuses on planning to maintain operations at an acceptable level, regardless of the type of disruption an organisation is exposed to. By working with business continuity management, organisations can more quickly recover from and reduce the consequences of an unwanted event. The work also contributes to a less vulnerable society.[8]
- Information and cybersecurity is based on protecting information and the information systems needed for operations and permeates all preparedness work. All operations depend on accurate and complete information being available to authorised users at the right time for operations to function. Systematic information security work means that the organisation needs to identify the information on which the critical infrastructure depend and where it is processed in order to ensure appropriate protection for the information and its confidentiality, accuracy and availability.[9]

7. ISO 31000:2018 – Risk management – Guidance.

8. SS 22304:2023 – Security and resilience – Business continuity management systems – Business continuity management manual according to SS EN ISO 22301.

9. ISO 27000: 2020 – Information technology – Security techniques – Information security management systems – Overview and vocabulary.

- Managing unwanted events includes incident and crisis management as well as cooperation and management during societal disruptions. It is based on the fact that organisations need to be prepared to manage unwanted events of varying degrees of severity when they occur. By planning for various unwanted events, conditions are created for an event to be managed effectively, for the consequences to be limited, and for critical infrastructure to be maintained.

The work needs to be systematic, be integrated into the organisation's existing work practices and permeate the entire organisation, for example as part of the organisation's management system. There are great advantages in coordinating this for more efficient work. Among other things, they all contain elements of analysis and assessments based on the activities of the organisation and potential risks but from different perspectives. The work will also generate the need for actions that need to be coordinated to create the best effect within the organisation. Not seeing this work as isolated processes also reduces the risk of duplication.

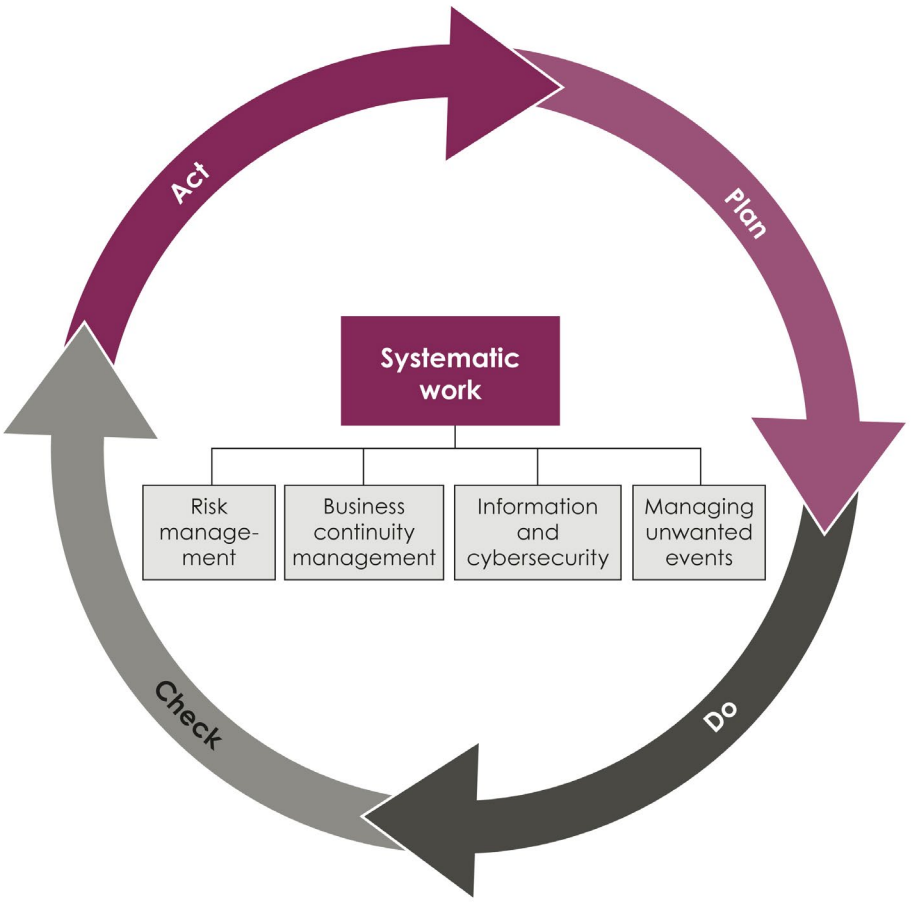
Examples of links between the different work practices are given below:

- The work with risk management provides, among other things, knowledge about the risks that the organisation and its activities may be exposed to. The data can be used to support the risk assessment of resources in business continuity management and can also be used to assess risks to information and, with that, appropriate measures as part of information and cybersecurity work.
- The work with business continuity management provides, for example, a basis for what resources are needed to maintain the critical infrastructure. It provides, among other things, knowledge about the information and information systems on which the organisation depends and is a basis for the activities' information protection requirements.
- Measures identified to provide protection as part of risk management or information and cybersecurity work may be the same in all areas.
- Lessons learned from managing unwanted events, especially incident and crisis management, are important input for improvement work in all areas.

The next section describes *risk management, business continuity management, information and cybersecurity*, and *managing unwanted events* with associated checklists.

There is also a checklist called *systematic work* that describes common work practices.

Figure 1. Systematic work on resilience in critical infrastructure



Systematic work

The checklist aims to create a systematic approach to the work on resilience in critical infrastructure. It has sections on governing documents, external monitoring, training and exercise, information and communication, follow-up and improvement, and lessons learned.

Table 1. Checklist – Systematic work

Number	Description
S1	The management of the organisation has in governing documents determined the overall conditions and objectives for the implementation of risk management, business continuity management, information and cybersecurity work and managing unwanted events based on the organisation's circumstances. *The objectives shall be based on requirements imposed on the organisation, measurable, communicated and updated*.
S2	The organisation has documented in governing documents and work practices what is needed to plan, implement, use, follow up and improve the organisation's work with risk management, business continuity management, information and cybersecurity, and managing unwanted events planning for critical infrastructure.
S3	The organisation works with external monitoring to identify events that affect the critical infrastructure in order to make effective decisions on priorities for risk management, business continuity management, information and cybersecurity and in managing events.
S4	The organisation educates and trains staff affected by the work on critical infrastructure.
S5	The organisation has established methods and plans for internal and external communication and reporting for risk management, business continuity management, information and cyber security and for event management.
S6	The organisation has established work practices to follow up and evaluate work with risk management, business continuity management, information and cybersecurity, and managing unwanted events. *This includes work practices to evaluate past events and exercises and to follow up compliance with internal and external requirements.*
S7	The organisation draws on the experience gained from follow-ups and audits of the work with risk management, business continuity management and information and cybersecurity, past events and exercises.

Risk management

The risk management work practices can take different forms but can generally be summarised in the checklist below.

Table 2. Checklist – Risk management

Number	Description
R1	A policy has been drawn up and the organisation has implemented and documented descriptions of roles and responsibilities regarding risk management.
R2	Objectives have been developed for the work and the organisation works with risk management in the strategic work. *Working with risk management in strategic work can mean, for example, including it in the organisation's governing processes such as planning and budgeting processes and having it as a recurring item on the management agenda.*
R3	The organisation has sufficient resources to meet the risk management objectives set out in the governing documents. *For example, customer and legal requirements. These resources can also be allocated to staff, technology, methodology and tools, financing and information to manage vulnerabilities and enable adaptation to changing circumstances.*
R4	The organisation works with risk management in its day-to-day activities. *For example, by integrating risk management into existing processes in the organisation and by ensuring that everyone within the organisation is responsible for managing risks.*
R5	The organisation has decided and communicated the level of risk acceptance of the activities, which is used as a starting point for managing the risks (see also K5 and IC5). *The organisation's level of risk acceptance, sometimes also called risk tolerance, is the level that the organisation/management has decided should apply in order to accept a risk, i.e. retain the risk without taking any further action. Note that even accepted risks must be monitored continuously*.
R6	The organisation regularly conducts assessments of risks and vulnerabilities (see also K6 and IC7) in the activities and these include, among other things: • Identification of risks, vulnerabilities and capabilities of the activities. • The probability and consequence of risks occurring. • Valuation and prioritisation of risks in relation to the activities' objectives/ requirements. • Risk management action plan. *The assessments aim to give the organisation a sufficiently good picture of the internal and external risks associated with the activities. These assessments can be carried out in a variety of areas, including risk analysis for internal governance and control, actuarial risk analyses and risk and vulnerability analyses.*
R7	The organisation decides and implements measures according to the agreed risk action plan.
R8	The organisation follows up and evaluates implemented measures to ensure that they have reduced the risks as expected.

Business continuity management

Business continuity management can take different forms but can generally be summarised in the checklist below.

See www.msb.se/kontinuitetshantering for more support in the work.

Table 3. Checklist – Business Continuity Management

Number	Description
K1	A policy has been drawn up and the organisation has implemented and documented descriptions of roles and responsibilities regarding business continuity management.
K2	Objectives have been developed for the work and the organisation works with business continuity management in the strategic work. *For example, by it being an integral part of the organisation's overall management system and a recurring item on the management agenda*.
K3	The organisation has sufficient resources to meet the business continuity management objectives/requirements set out in governing documents.
K4	The organisation works with business continuity management in its day-to-day activities. *This can be done by implementing business continuity management in existing processes in the organisation.*
K5	The organisation has conducted and documented a business impact analysis if disruptions occur in the organisation's delivery of vital/critical products and services that may include: • a criteria model (or equivalent) for assessing the consequences of disruptions (see also R5 and IC5). • What activities are needed to deliver products and services. • What consequences a disruption of these activities have for the organisation through assessment using the criteria model. • Definition of how long the activity can be down without the consequences being unacceptable for the organisation (acceptable downtime). • Identified priority activities • Determined resources (dependencies) including partners and suppliers needed to perform the priority activities. • Identified recovery times for the resources.
K6	The organisation has carried out and documented a risk assessment of which risks may interfere with vital/critical products and services (see also R6 and IC7). The risk assessment may include an identification and assessment of: • Risks that could lead to a disruption of resources or priority activities • Existing redundancy or other protective measures • The probability of exceeding recovery time objectives if the risk occurs • What risks need to be addressed *The risk assessment can cover priority activities or the resources on which they depend*.
K7	The organisation has one or more adopted action plans with draft measures.
K8	The organisation has chosen and documented business continuity solutions, i.e. how to manage disruptions in operations, before, during and after an event. *Business continuity solutions may include hiring new staff, signing agreements with multiple suppliers, reallocating staff and enabling stockpiling of input goods and spare parts.*

Number	Description
K9	The organisation has established and documented one or more business continuity plans which may include: • Document owner • Purpose and objectives • Scope • Responsibilities and roles • Powers • Activation procedures • Fallback procedure • Recovery procedure • Return procedure • Required contact details • Exercise and training • Procedure for revision of the plan The business continuity plan is available and anchored in the organisation. *A business continuity plan contains documented information that guides an organisation to manage a disruption and resume, restore, and recreate the delivery of products and services in accordance with its business continuity management objectives.*
K10	The organisation follows up and evaluates implemented measures and business continuity solutions to ensure that they have had the intended effect.

Information and cybersecurity

Work practices for information and cybersecurity can take different forms as it needs to be integrated with the organisation's way of leading and managing its activities, but can generally be summarised in the checklist below.

See www.msb.se/informationssakerhet for more support in designing information and cyber security work in your organisation.

Table 4. Checklist – Information and cyber security

Number	Description
IC1	A policy has been drawn up and the organisation has implemented and documented descriptions of roles and responsibilities regarding information and cybersecurity work.
IC2	Objectives have been developed for the work and the organisation works with information and cybersecurity in the strategic work. *This means working systematically to plan, implement, maintain and improve information and cybersecurity in the activities. For example, by it being an integral part of the organisation's overall management system and a recurring item on the management agenda*.
IC3	The organisation has sufficient resources to meet the information and cybersecurity objectives/requirements set out in the governing documents.
IC4	The organisation works with information and cybersecurity in its day-to-day activities based on governing documents and work practices. *This can be done by implementing information and cybersecurity in existing processes in the organisation*.

Number	Description
IC5	The organisation has decided and communicated the level of risk acceptance of the activities, which is used as a starting point for managing the risks (see also R5 and K5). *The organisation's level of risk acceptance, sometimes also called risk tolerance, is the level that the organisation/management has decided should apply in order to accept a risk, i.e. retain the risk without taking any further action. Note that even accepted risks must be monitored continuously*.
IC6	The organisation conducts and documents information classifications. This means that the information is valued based on confidentiality, accuracy and availability. *This document identifies the consequences that arise if the information is not available, accurate or if it is disclosed to unauthorised persons*.
IC7	The organisation conducts and documents risk assessments by identifying and analysing risks to information processing, for example based on where it is processed, stored or communicated (see also R6 and K6). *Risk assessment is the approach that includes risk identification, risk analysis and risk evaluation*.
IC8	The organisation chooses the security measures that need to be taken to protect the information based on the results of the information classification and risk assessment. The implementation of the measures includes the development of an action plan describing: • Who will implement the security measure. • When it should be implemented. • How the organisation checks that the measure is implemented and provides the necessary protection. *The security measures can be of various kinds, e.g. organisational, staff-related, technical, or physical*.
IC9	The organisation has introduced sufficient security measures to protect the information by placing requirements on resources that process information during information management. *For example, by imposing requirements on staff management, physical protection, and technical measures*.
IC10	The organisation works to ensure continuity of its information and information systems, see business continuity management checklist. *See in particular K5-K9*.
IC11	The organisation has governing documents for how information and cybersecurity incidents should be reported and work practices for incident management. This includes communicating established work practices, roles and areas of responsibility for information security incident management.
IC12	The organisation follows up and evaluates implemented measures to ensure that they have had the intended effect.

Managing unwanted events

Managing unwanted events can take different forms but can generally be summarised in the checklist below. The checklist below applies to all types of events and can be customised accordingly.

See www.msb.se/samverkanledning for more support in thet work.

Table 5. Checklist - Managing unwanted events

Number	Description
H1	A policy regarding incident and crisis management is established and known in the organisation.
H2	Objectives have been developed for the organisation's work with managing unwanted events.

Number	Description
H3	The organisation has sufficient resources to meet the objectives/requirements regarding the organisation's work with managing unwanted events.
H4	The organisation has established and documented work practices for how to handle an unwanted event, including clear roles and responsibilities: • Internally within the own organisation. • In cooperation with other actors.
H5	The organisation has established contacts, networks, or forums with relevant actors.
H6	The organisation has a contact point for: • Alerts and coordination internally within the organisation. • To cooperate with other actors. *For example TiB, official on standby, responsible manager, direction and coordination contact (ISK) or equivalent*.
H7	The organisation conducts external monitoring for the purpose of strengthening its management capabilities. *External monitoring is conducted to actively collect, analyse, evaluate and convey information that helps organisations create a knowledge of the surrounding world to support better decision-making in an event/crisis*.
H8	The organisation has methods for drawing up and communicating situational pictures internally and externally. *A situational picture is a selection of information compiled in the form of descriptions or assessments of the situation. The purpose is to provide an overview, understanding or basis for decisions and measures.*
H9	The organisation has appropriate technical systems and equipment in place to deal with an unwanted event that may affect critical infrastructure.
H10	The organisation has procedures in place to document the handling, analysis and decision before, during and after an unwanted event occurs.
H11	The organisation has drawn up one or more plans for managing unwanted events. These plans may include: • Roles, responsibilities and mandates. • Owner and administrator of plan. • Objective and purpose. • Procedure for alerts and activation of plan. • Contact details, both internally and to other actors. • Methods and forms for how unwanted events should be managed internally and in cooperation with other actors. • Procedures for sharing information and creating situational pictures. • Internal and external communication procedures. • Crisis communication procedures. • External monitoring procedures. • Premises and technical equipment. • Procedures for lessons learned. • Procedures for training and exercise of plan. • Recovery plan. *Plans can consist of one or more procedures, checklists, etc. They are used when there is a need to draw up a crisis management organisation to deal with the event. These plans may be called contingency plans, crisis management plans, etc.*
H12	The organisation has made plans to be able to provide psychological and social care of its own staff.

Appendix

Appendix – Standards and guidance

Table 6. Standards and guidance

Type	Reference	Year
Systematic work		
Standard	**ISO 22301** – Societal Security – Business continuity management systems – Requirements	2019
Standard	**SS 22304** – Security and resilience – Business continuity management systems – Business continuity management manual according to SS EN ISO 22301	2023
Standard	**ISO 22313** – Security and resilience – Business continuity management systems – Guidance for ISO 22301 implementation	2020
Standard	**ISO 22316** – Security and resilience – Organisational resilience – Principles	2020
Standard	**ISO 22318** – Business continuity management systems – Guidelines for supply chain continuity management (ISO/TS 22318:2021, IDT)	2022
Standard	**ISO 22320** – Emergency management – Requirements for Collaboration	2019
Standard	**ISO 22331** – Business continuity management systems – Guidelines for selecting a business continuity strategy	2018
Standard	**ISO 22332** – Business continuity management systems – Guidelines for developing business continuity plans and procedures (ISO/TS 22332:2021)	2021
Standard	**ISO 27000** – Information technology – Security techniques – Information security management systems – Overview and vocabulary	2020
Standard	**ISO 27001** – Information security, cybersecurity and privacy protection – Information security management systems – Requirements	2022
Standard	**ISO 27002** – Information security, cybersecurity and privacy protection – Information security controls	2022
Standard	**ISO 27003** – Information technology – Security techniques – Information security management system implementation guidance	2018
Standard	**ISO 27005** – Information security, cybersecurity and privacy protection – Guidance on managing information security risks	2022
Standard	**ISO 31000** – Risk management – Guidance	2018
Standard	**BSI-Standard 100-4** – Business Continuity Management	2009
Standard	**NFPA 1600** – Standard on Disaster/Emergency Management and Business Continuity Programs	2013

Type	Reference	Year
Guidance	**COSO Compliance Risk Management, Applying the Coso ERM Framework**	2020
Guidance	**FSPOS Vägledning för kontinuitetshantering** (based on the standard SS-ISO 22301:2012 – Societal Security – Business Continuity Management System)	2024
Guidance	**FSPOS Vägledning för Krishantering**	2017
Guidance	**MSB 30128** – Säkerhetsåtgärder i informationssystem	2022
Guidance	**MSB 1447** – Utvärdering av hantering av inträffade händelser	2019
Risk management		
Standard	**ISO 31000** Risk management – Guidance	2018
Standard	**ISO 22316** Security and resilience – Organisational resilience – Principles	2020
Standard	**ISO 27001** – Information security, cybersecurity and privacy protection – Information security management systems – Requirements	2022
Standard	**ISO 27003** – Information technology – Security techniques – Information security management system implementation guidance	2018
Standard	**ISO 27005** – Information security, cybersecurity and privacy protection risk management – Guidance	2022
Guidance	**COSO Compliance Risk Management, Applying the Coso ERM Framework**	2020
Guidance	**FSPOS Vägledning för kontinuitetshantering** (Addresses how organisations can work with risk assessment and risk management)	2024
Business continuity management		
Standard	**ISO 22301** – Societal Security – Business continuity management systems – Requirements	2019
Standard	**SS22304** – Säkerhet och resiliens – Ledningssystem för kontinuitetshantering – Handbok för kontinuitetshantering enligt SS EN ISO 22301	2023
Standard	**ISO 22313** – Security and resilience – Business continuity management systems – Guidance for ISO 22301 implementation	2020
Standard	**ISO 22316** – Security and resilience – Organisational resilience – Principles	2020
Standard	**ISO 22317** – Business continuity management systems – Guidelines for business impact analysis (ISO/TS 22317:2021, IDT)	2022
Standard	**ISO 22318** – Business continuity management systems – Guidelines for supply chain continuity management (ISO/TS 22318:2021, IDT)	2022

Type	Reference	Year
Standard	**ISO 22332** – Business continuity management systems – Guidelines for developing business continuity plans and procedures (ISO/TS 22332:2021)	2021
Standard	**ISO 27002** – Information security, cybersecurity and privacy protection – Information security controls	2022
Standard	**BSI-Standard 100-4** – Business Continuity Management	2009
Standard	**NFPA 1600** – Standard on Disaster/Emergency Management and Business Continuity Programs	2013
Guidance	**FSPOS Vägledning för kontinuitetshantering** (based on the standard SS-ISO 22301:2012 – Societal Security – Business Continuity Management System)	2024
Information and cybersecurity		
Standard	**ISO 27000** – Information technology – Security techniques – Information security management systems – Overview and vocabulary	2020
Standard	**ISO 27001** – Information security, cybersecurity and privacy protection – Information security management systems – Requirements	2022
Standard	**ISO 27002** – Information security, cybersecurity and privacy protection – Information security controls	2022
Standard	**ISO 27003** – Information technology – Security techniques – Information security management system implementation guidance	2018
Standard	**ISO 27005** – Information security, cybersecurity and privacy protection – Guidance on managing information security risks	2022
Standard	**ISO 22316** – Security and resilience – Organisational resilience – Principles	2020
Standard	**SS-EN IEC 62443-3-2** – IT-säkerhet i industriella automationssystem – Del 3–2: Riskbedömning och systemkonstruktion	2020
Standard	**SS-EN IEC 62443-3-3** – IT-säkerhet i industriella automationssystem – Del 3–3: IT-säkerhet i nät och system – Fordringar på systemets säkerhet och på säkerhetsnivåer	2019
Guidance	**MSB 30128** – Säkerhetsåtgärder i informationssystem	2022
Managing unwanted events		
Standard	**ISO 22320** – Emergency management – Requirements for Collaboration	2019
Standard	**ISO 22316:2020** Security and resilience – Organisational resilience – Principles	2020
Guidance	**FSPOS Vägledning för Krishantering**	2024
Guidance	**Gemensamma grunder –** ramverk för samverkan och ledning	2024

Systematic work

Table 7. Checklist – Systematic work

Number	Description	Help text	Reference to standard or guidance	Link to statutes
S1	The management of the organisation has in governing documents established overall conditions and objectives for how risk management, business continuity management, information and cyber security and planning for managing unwanted events shall be implemented based on the organisation's circumstances.	The objectives should be based on requirements imposed on the organisation, measurable, communicated and updated.	**ISO 22301:2019** Section 5.2. **SS 22304:2023** Section 5.2. **ISO 22313:2020** Section 5.2. **ISO 22316:2020** Section 4.1, 4.2. **ISO 22318:2022** Section 5.2.1. **ISO 22320:2019** Section 5.2.1 and 5.3.1. **ISO 27000:2020** Section 3.75, 4.2.1 and 4.6. **ISO 27001:2022** Section 4.4, 5.1–5.2, 6.2, 8.1, 9.3 and 10. **ISO 27002:2022** Section 0.1–0.2, 5.1–5.2, 5.4 and 5.36. **ISO 27003:2018** Section 4.4, 5.1–5.2, 6.2, 8.1, 9.3 and 10. **ISO 31000:2018** Section 5.2 and 5.4.2. **MSB 30128** Section 2.1.3. **COSO** page 11 and 14. **BSI-Standard-100-4** Section 3.2. **FSPOS guidance for business continuity management** Section 3.1.	6§ **i Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter.**
S2	The organisation has in governing documents and work practices documented what is needed to plan, implement, use, follow up, and improve the organisation's risk management work, business continuity management, information and cyber security and planning for managing unwanted events for critical infrastructure.		**ISO 22301:2019** Section 5.2. **SS 22304:2023** Section 5.2. **ISO 22313:2020** Section 5.2. **ISO 22320:2019** Section 5.3. **ISO 22316:2020** Section 4.1 and 4.2. **ISO 27000:2020** Section 4.6. **ISO 27001:2022** Section 5.1 and 5.2. **ISO 27003:2018** Section 5.3, 6.1 and 6.2. **ISO 31000: 2018** Section 6.3.2, 5.2, 5.4.2, 5.4.3, 5.4.5, 6.2, and 6.5.3.	6§ i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter**.

Number	Description	Help text	Reference to standard or guidance	Link to statutes
S3	The organisation works with external monitoring to identify events that affect the critical infrastructure in order to make effective decisions on priorities for risk management, business continuity management, information and cybersecurity and in managing events.		**SS 22304:2023** Section 8.2.1. **ISO 22316:2020** Section 5.3. **ISO 27001:2022** Section 4.1 and 4.3. **ISO 27003:2018** Section 4.1. **ISO 27005:2022** Section 7.2.1. **ISO 22316:2020** Section 3.4, 4.1, 5.3, 5.10, 6.3.2 and 6.4. **ISO 27005:2022** Section 5.2. **ISO 31000:2018** Section 5.7.1. **COSO** page 11. **MSB 30128** Section 2.2.	5 § punkt 4 i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter**. 2 kap. 2 § i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:7) om säkerhetsåtgärder i informationssystem för statliga myndigheter**.
S4	The organisation educates and trains staff affected by the work on critical infrastructure.		**ISO 22301:2019** Section 7.2 and 8.5. **SS 22304:2023** Section 7.2 and 8.5. **ISO 22313:2020** Section 7.2 and 8.5. **ISO 22320:2019** Section 6.3.1. **ISO 27001:2022** Section 7.2b. **ISO 27002:2022** Section 6.3. **ISO 31000:2018** Section 5.4.4. **COSO** page 33. **MSB 30128** Section 2.1.6. **FSPOS Business Continuity Management Guidance** Sections E.2 and E.3. **FSPOS Crisis Management Guidance** Section 3.4.	9 § punkt 5 i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter**. 2 kap. 4 § i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:7) om säkerhetsåtgärder i informationssystem för statliga myndigheter**. 2 kap. 8 § i **Lag (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap**. 8 § och 20 § punkt 11 i **Förordning (2022:524) om statliga myndigheters beredskap**. 5 kap. 1 § i **Säkerhetsskyddsförordning (2021:955)**.

Number	Description	Help text	Reference to standard or guidance	Link to statutes
S5	The organisation has established methods and plans for internal and external communication and reporting for risk management, business continuity management, information and cybersecurity, and event management.		**ISO 22301:2019** Section 7.4, 8.4.3 and 9.2. **SS 22304:2023** Section 8.4.2 and 9.2. **ISO 22313:2020** Section 7.4, 8.4.3 and 9.2. **ISO 22320:2019** Section 6.2:4. **ISO 27001:2022** Section 7.4. **ISO 27002:2022** Section 6.8. **ISO 27003:2018** Section 7.4. **ISO 31000:2018** Section 5.4.5, 6.2, 6.4.and 6.5. **FSPOS Crisis Management Guidance** Section 3.4.	8 § och 9 § i **Lag (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap**. 19 § och 22 § i **Förordning (2022:524) om statliga myndigheters beredskap**.
S6	The organisation has established work practices to follow up and evaluate work with risk management, business continuity management, information and cybersecurity, and managing unwanted events.	This includes work practices to evaluate past events and exercises and to follow up compliance with internal and external requirements.	**ISO 22301:2019** Section 8.6 and 9. **SS 22304:2023** Section 8.6 and 9. **ISO 22313:2020** Section 9.1.1 and 9.3.3. **ISO 22316:2020** Section 5.9, 6.2.2, 6.3.1, and 6.6. **ISO 22318:2022** Section 6.5 and Appendix B4. **ISO 22331:2018** Section 7.1 and 7.2. **ISO 27000:2020** Section 4.5.6 and 4.5.7. **ISO 27001:2022** Section 4.4, 5.2d, 9.1 and 10. **ISO 27003:2018** Section 9.1 and 10.2. **ISO 27005:2022** Section 10.5–6. **ISO 31000:2018** Section 5.6 and 6.6. **BSI-Standard-100-4** Chapter 8. **NFPA 1600**, Chapter 8. **FSPOS Business Continuity Management Guidance** Section 3. **FSPOS Crisis Management Guidance** Section 3.2–3.3. **MSB1447** Evaluation of handling of past events.	

Number	Description	Help text	Reference to standard or guidance	Link to statutes
S7	The organisation draws on the experience gained from follow-ups and audits of the work with risk management, business continuity management and information and cybersecurity, past events and exercises.		**ISO 22301:2019** Section 9.2 and 10. **SS 22304:2023** Section 9.2 and 10. **ISO 22313:2020** Section 9.2–9.3 and 10. **ISO 22316:2020** Section 5.6 and 5.9. **ISO 22318:2022** Appendix B4. **ISO 22332:2021** Section 12. **ISO 27005:2022** Section 10.6–10.8. **ISO 31000:2018** Section 5.7.2 and 6.1. **COSO** page 22–26. **BSI-Standard-100-4** Chapter 9. **NFPA 1600** Chapter 9. **FSPOS Crisis Management Guidance** Section 3.3. **MSB1447** Evaluation of handling of past events.	

Risk management

Table 8. Checklist – Risk management

Number	Description	Help text	Reference to standard or guidance	Link to statutes
R1	A policy has been drawn up and the organisation has implemented and documented descriptions of roles and responsibilities regarding risk management.		**ISO 27005:2022** Section 6.1. **ISO 31000:2018** Section 5.3, 5.4.2, 5.4.3.	
R2	Objectives have been developed for the work and the organisation works with risk management in the strategic work.	Working with risk management in strategic work can mean, for example, including it in the organisation's governing processes such as planning and budgeting processes and having it as a recurring item on the management agenda.	**ISO 27003:2018** Section 6.3, 8. **ISO 31000:2018** Section 4, 5.1–5.3 and 6.1. **COSO** page 11.	7 § och 17 § i **Förordning (2022:524) om statliga myndigheters beredskap**.
R3	The organisation has sufficient resources to meet the risk management objectives set out in the governing documents.	For example, customer and legal requirements. These resources can also be allocated to staff, technology, methodology and tools, financing and information to manage vulnerabilities and enable adaptation to changing circumstances.	**ISO 22316:2020** Section 4.2, 5.2, 5.5 and 5.7–5.8. **ISO 27005:2022** Section 6.1. **ISO 31000:2018** Section 5.4.2 and 5.4.4. **COSO** page 8.	
R4	The organisation works with risk management in its day-to-day activities.	For example, by integrating risk management into existing processes in the organisation and by ensuring that everyone within the organisation is responsible for managing risks.	**ISO 27001:2022** Section 8. **ISO 27003:2018** Section 6.3. **ISO 31000:2018** Section 4, 5.1–5.3 and 6.1.	

Number	Description	Help text	Reference to standard or guidance	Link to statutes
R5	The organisation has decided and communicated the level of risk acceptance of the activities, which is used as a starting point for managing the risks (see also K5 and IC5).	The organisation's level of risk acceptance, sometimes also called risk tolerance, is the level that the organisation/ management has decided should apply in order to accept a risk, i.e. retain the risk without taking any further action. Note that even accepted risks must be monitored continuously.	**ISO 27005:2022** Section 6.4.2. **ISO 31000:2018** Section 6.3.4. **FSPOS guidance for business continuity** Section 2.4.2.	
R6	The organisation regularly conducts assessments of risks and vulnerabilities in the activities and these include, among other things: • Identification of risks, vulnerabilities and capabilities of the activities. • The probability and consequence of risks occurring. • Valuation and prioritisation of risks in relation to the activities' objectives/requirements. • Risk management action plan.	The assessments aim to give the organisation a sufficiently good picture of the internal and external risks associated with the activities. These assessments can be carried out in a variety of areas, including risk analysis for internal governance and control, actuarial risk analyses and risk and vulnerability analyses.	**ISO 27005:2022** Section 7. **ISO 31000:2018** Section 6.4.2–6.4.4 and 6.5. **COSO** page 15–25.	7 § och 17 § i **Förordning (2022:524) om statliga myndigheters beredskap**. 3 § i **Förordning (2018:1343) om intern styrning och kontroll**.
R7	The organisation decides and implements measures according to the agreed risk action plan.		**ISO 27005:2022** Section 8.6. **ISO 31000:2018** Section 6.5.3. **COSO** page 22–26.	
R8	The organisation follows up and evaluates implemented measures to ensure that they have reduced the risks as expected.		**ISO 22316:2020** Section 6.3.1, 6.2.2. **ISO 27005:2022** Section 10.5. **ISO 31000:2018** Section 5.6, 6.6. **COSO** page 22–26.	

Business continuity management

Table 9. Checklist – Business Continuity Management

Number	Description	Help text	Reference to standard or guidance	Link to statutes
K1	A policy has been drawn up and the organisation has implemented and documented descriptions of roles and responsibilities regarding business continuity management.		**ISO 22301:2019** Section 5.2–5.3, 7.3, 8.4.2 and 8.4.4. **SS 22304:2023** Section 5.2–5.3, 7.3, 8.4.2 and 8.4.4. **ISO 22313:2020** Section 5.2–5.3, 7.1.2, 7.3, 7.5 and Table 3. **ISO 22317:2022** 4.3.1. **ISO 22318:2022** 5.2.1 and 5.2.3. **ISO 22331:2018** 4.4.1. **BSI-Standard-100-4** Section 3.2, 4.5 and 4.6. **FSPOS Business Continuity Management Guidance** Section 3.1 and Appendix A.	
K2	Objectives have been developed for the work and the organisation works with business continuity management in the strategic work.	For example, by it being an integral part of the organisation's overall management system and a recurring item on the management agenda.	**ISO 22301:2019** Section 6.2 and 7.3. **SS 22304:2023** Section 6.2 and 7.3. **ISO 22313:2020** Section 6.2.2 and 7.3. **ISO 22316:2020** Section 5.2. **ISO 22331:2018** Section 4.4.2–4.4.4, 4.5 and 5.6.4. **BSI-Standard-100-4** Section 4.6. **FSPOS Business Continuity Management Guidance** Section 3.1 and Appendix A.	10 § och 19–20 §§ i **Förordning (2022:524) om statliga myndigheters beredskap**.
K3	The organisation has sufficient resources to meet the business continuity management objectives/ requirements set out in governing documents.		**ISO 22301:2019** Section 5.1, 6.2.2 and 7.1. **SS 22304** Section 5.1, 5.3, 6.2.2 and 7.1. **ISO 22316:2020** Section 4.2, 5.5 and 5.7. **ISO 22318:2022** Section 5.2.2.	

Number	Description	Help text	Reference to standard or guidance	Link to statutes
K4	The organisation works with business continuity management in its day-to-day activities.	This can be done by implementing business continuity management in existing processes in the organisation.	**ISO 22301:2019** Section 7.2–7.3. **SS 22304:2023** Section 7.2–7.3. **ISO 22313:2020** Section 5.1.3, 7.2 and 7.3. **ISO 22316:2020** Section 5.8. **ISO 22318:2022** Section 4.2.2. **NFPA 1600**, Section 8.1.1. **BSI-Standard-100-4** Section 4.6.	10 § och 19–20 §§ i **Förordning (2022:524) om statliga myndigheters beredskap**. 13 § i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter MSBFS 2020:6**.
K5	The organisation has conducted and documented a business impact analysis if disruptions occur in the organisation's delivery of vital/critical products and services that may include: • a criteria model (or equivalent) for assessing the consequences of disruptions (see also R5 and IC5). • What activities are needed to deliver products and services. • What consequences a disruption of these activities have for the organisation through assessment using the criteria model. • Definition of how long the activity can be down without the consequences being unacceptable for the organisation (acceptable downtime). • Identified priority activities. • Determined resources (dependencies) including partners and suppliers needed to perform the priority activities. • Identified recovery times for the resources.		**ISO 22301:2019** Section 4.3.2 and 8.2.2. **SS 22304:2023** Section 4.3.2 and 8.2.2. **ISO 22313:2020** Section 4.3.2 and 8.2.2. **ISO 22317:2022** Table 3, 5.5-5.6 and Appendix D. **ISO 22318:2022** Section 5.4.2. **ISO 22331:2018** Section 5.2 and 4.7. **ISO 27002:2022** Section 5.30. **FSPOS Business Continuity Management Guidance** Appendix B and B.1-2.	7 § punkt 1 och 3 i **Förordning (2022:524) om statliga myndigheters beredskap**.

Number	Description	Help text	Reference to standard or guidance	Link to statutes
K6	The organisation has carried out and documented a risk assessment of which risks may interfere with vital/critical products and services (see also R6 and IC7). The risk assessment may include an identification and assessment of: • Risks that could lead to a disruption of resources or priority activities. • Existing redundancy or other protective measures. • The probability of exceeding recovery time objectives if the risk occurs. • What risks need to be addressed.	The risk assessment can cover priority activities or the resources on which they depend.	**ISO 22301:2019** Section 8.2.3. **SS 22304:2023** Section 8.2.3. **ISO 22313:2020** Section 8.2.3. **FSPOS Business Continuity Management Guidance** Appendix B and B3–4.	7 § punkt 2 i **Förordning (2022:524) om statliga myndigheters beredskap**.
K7	The organisation has one or more adopted action plans with draft measures.		**ISO 22301:2019** Section 8.3. **SS 22304:2023** Section 8.3. **ISO 22313:2020** Section 8.3.	
K8	The organisation has chosen and documented business continuity solutions, i.e. how to manage disruptions in operations, before, during and after an event.	Business continuity solutions may include hiring new staff, signing agreements with multiple suppliers, reallocating staff and enabling stockpiling of input goods and spare parts.	**ISO 22301:2019** Section 4.4, 8.3.2 and 8.4.4–8.4.5. **SS 22304:2023** Section 4.4, 8.3 and 8.4.4–8.4.5. **ISO 22313:2020** Section 8.3.2. **ISO 22331:2018** Section 5.2, 5.5.4 and 5.6. **NFPA 1600** Section 6.7.1.	

Number	Description	Help text	Reference to standard or guidance	Link to statutes
K9	The organisation has established and documented one or more business continuity plans which may include: • Document owner. • Purpose and objectives. • Scope. • Responsibilities and roles. • Powers. • Activation procedures. • Fallback procedure. • Recovery procedure. • Return procedure. • Required contact details. • Exercise and training. • Procedure for revision of the plan. The business continuity plan is available and anchored in the organisation.	A business continuity plan contains documented information that guides an organisation to manage a disruption and resume, restore, and recreate the delivery of products and services in accordance with its business continuity management objectives.	**ISO 22301:2019** Section 8.4.3–8.4.5. **SS 22304:2023** Section 8.4.3–8.4.5. **ISO 22313:2020** Section 8.4.4.3. **ISO 22332:2021** Section 9,10 and 11. **NFPA 1600** Section 6.1.1 and 6.7.1. **BSI-Standard-100-4** Section 7.4.4, 7.4.5 and Appendix A. **FSPOS Business Continuity Management Guidance** Section 3.4, Appendix D and H.	
K10	The organisation follows up and evaluates implemented measures and business continuity solutions to ensure that they have had the intended effect.		**ISO 22301:2019** Section 8.5, 8.6. **SS 22304:2023** Section 8.5, 8.6. **ISO 22313:2020** Section 8.5, 8.6. **FSPOS Business Continuity Management Guidance** Appendix H.	

Information and cybersecurity

Table 10. Checklist – Information and cybersecurity

Number	Description	Help text	Reference to standard or guidance	Link to statutes
IC1	A policy has been drawn up and the organisation has implemented and documented descriptions of roles and responsibilities regarding information and cybersecurity work.		**ISO 27000:2020** Section 4.2.1. **ISO 27001:2022** Section 5.1h, 5.2–5.3, 7.2. and 7.3a. **ISO 27002:2022** Section 5.2-5.3, 5.4d, 5.12 and 6.1. **ISO 27003:2018** Section 5.3, 7.2 and Appendix A. **ISO 27005:2022** Section 10.2. **MSB 30128** Section 2.1.3–2.1.4 and 2.1.6.	2 kap. 2 § och 5 kap. i **Säkerhetsskyddsförordning (2021:955)**. 4–6 §§ i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter**. 2 kap. 1 § i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:7) om säkerhetsåtgärder i informationssystem för statliga myndigheter**.
IC2	Objectives have been developed for the work and the organisation works with information and cyber security in their strategic work.	This means working systematically with planning, implementing, maintaining and improving information and cyber security in the activities. For example by it being an integral part of the organisation's overarching management system and that it is a recurring item on the management agenda.	**ISO 22316:2020** Section 4.2, 5.2, 5.4–5.5. and 5.7–5.8. **ISO 27000:2020** Section 3.75, 4.2.1 and 4.6. **ISO 27001:2022** Section 4.4, 5.1–5.2, 6.2, 8.1, 9.3 and 10. **ISO 27002:2022** Section 0.1–0.2, 5.1–5.2, 5.4. and 5.36. **ISO 27003:2018** Section 4.4, 5.1–5.2, 6.2, 8.1, 9.3 and 10. **MSB 30128** Section 2.1.3.	4–6 §§ och 14–15 §§ i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter**.

Number	Description	Help text	Reference to standard or guidance	Link to statutes
IC3	The organisation has sufficient resources to meet the information and cybersecurity objectives/ requirements set out in the governing documents.		**ISO 27001:2022** Section 5.1C. **ISO 27003:2018** Section 7.1.	5 § punkt 3 i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter**.
IC4	The organisation works with information and cybersecurity in its day-to-day activities based on governing documents and work practices.	This can be done by implementing information and cybersecurity in existing processes in the organisation.	**ISO 27001:2022** Section 8. **ISO 27005:2022** Section 6.3.	8 § i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:8) om informationssäkerhet för leverantörer av samhällsviktiga tjänster**. 6 § i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter**.
IC5	The organisation has decided and communicated the activities' level of risk acceptance, which used as a basis when handling the risks (see also R5 and K5).	The organisation's level of risk acceptance, called risk tolerance and is the level which the organisation/management has decided should apply in order to accept a risk, i.e. retain the risk without taking any further action. Note that even accepted risks must be monitored continuously.	**ISO 27000:2020** Section 3.62, 4.5.4. **ISO 27001:2022** Section 6.1.2a1. **ISO 27003:2018** Section 6.1.2a1. **ISO 27005:2022** Section 6.4.1–2.	

Number	Description	Help text	Reference to standard or guidance	Link to statutes
IC6	The organisation conducts and documents information classifications. This means that the information is valued based on confidentiality, accuracy and availability.	This document identifies the consequences that arise if the information is not available, accurate or if it is disclosed to unauthorised persons.	**ISO 27002:2022** Section 5.12.	8 § punkt 1 i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:8) om informationssäkerhet för leverantörer av samhällsviktiga tjänster**. 6 § punkt 1 i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter**.
IC7	The organisation conducts and documents risk assessments by identifying and analysing risks to information processing, for example based on where it is processed, stored or communicated (see also R6 and K6).	Risk assessment is the approach that includes risk identification, risk analysis and risk evaluation.	**SS-EN IEC 62443-3-2:2020** Section 4.3.1, 4.5.2, 4.6. **ISO27000:2020** Section 3.64, 4.2.3 and 4.5.3. **ISO 27001:2022** Section 6.1.1–6.1.2, 6.1.3, 7.5.2 and 8.2. **ISO 27002:2022** Section 5.7, 5.9 and 5.12. **ISO 27003:2022** Section 6.1.2. **ISO 27005:2022** Section 6.3 and 7–9. **MSB 30128** Section 2.3.	2 kap. 1 § i **Säkerhets-skyddsförordning (2021:955)**. 7 § och 17 § i **Förordning (2022:524) om statliga myndigheters beredskap**. 8 § punkt 2 i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:8) om informationssäkerhet för leverantörer av samhällsviktiga tjänster**. 4–5 §§ och 6 § punkt 1 i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter**. 2 kap. 1 § och 3 § i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:7) om säkerhetsåtgärder i informationssystem för statliga myndigheter**.

Number	Description	Help text	Reference to standard or guidance	Link to statutes
IC8	The organisation chooses the security measures that need to be taken to protect the information based on the results of the information classification and risk assessment. The implementation of the measures includes the development of an action plan describing: • Who will implement the security measure. • When it should be implemented. • How the organisation checks that the measure is implemented and provides the necessary protection.	The security measures can be of various kinds, e.g. organisational, staffrelated, technical, or physical.	**ISO 27000:2020** Section 4.5.4–4.5.5. **ISO 27001:2022** Section 6.1.3 and 8.3. **ISO 27003:2018** Section 6.1.3. **ISO 27005:2022** Section 8.3–6. **MSB 30128** Section 2.3.7.	8 § punkt 3 i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:8) om informationssäkerhet för leverantörer av samhällsviktiga tjänster**. 6 § punkt 3 i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter**.
IC9	The organisation has introduced sufficient security measures to protect the information by placing requirements on resources that process information during information management.	For example, by imposing requirements on staff management, physical protection, and technical measures.	**ISO 27001:2022** Section 8.3. **ISO 27002:2022** Section 5, 5.18–5.20, 5.30, 6.1, 7–7.9, and 8–8.28. **ISO 27003:2018** Section 8.1. **ISO 27005:2022** Section 9.2. **SS-EN IEC 62443-3-3** Section 5–11. **MSB 30128** Section 2.1–2.1.7, 4.1–4.6, 4.9–4.10,4.11, 4.13–4.14, and 5.1.	3–5 kap. i **Säkerhetsskydds-förordning (2021:955)**. 8 § punk 3 i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:8) om informationssäkerhet för leverantörer av samhällsviktiga tjänster**. 6 § punkt 3 och 4 i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter**. 4 kap. 1 § och 22 § i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:7) om säkerhetsåtgärder i informationssystem för statliga myndigheter**.

Number	Description	Help text	Reference to standard or guidance	Link to statutes
IC10	The organisation works with precautionary security measures to ensure continuity of its information and information systems, see business continuity management checklist.	See in particular K.5–K.9.	**ISO 27002:2022** Section 5.29–5.30 and 8.13–8.14. **SS-EN IEC 62443-3-3** Section 11. **MSB 30128** Section 4.14.	12 § i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:8) om informationssäkerhet för leverantörer av samhällsviktiga tjänster**. 13 § **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter**. 4 kap. 22 § i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:7) om säkerhetsåtgärder i informationssystem för statliga myndigheter**.

Number	Description	Help text	Reference to standard or guidance	Link to statutes
IC11	The organisation has governing documents for how information and cybersecurity incidents should be reported and work practices for incident management. This includes communicating established work practices, roles and areas of responsibility for information security incident management.		**ISO 27002:2022** Section 5.24–5.27 and 6.8.	14 § i **Förordning (2022:524) om statliga myndigheters beredskap**. 11 § i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:8) om informationssäkerhet för leverantörer av samhällsviktiga tjänster**. 1–12 §§ i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter**. 2–7 §§ i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:8) om rapportering av it-incidenter för statliga myndigheter**. 2 kap. 1–5 §§ i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:5) om rapportering av it-incidenter** för leverantörer av samhällsviktiga tjänster.

Number	Description	Help text	Reference to standard or guidance	Link to statutes
IC12	The organisation follows up and evaluates implemented measures to ensure that they have had the intended effect.		**ISO 27001:2022** Sections 9 and 10.	6 § punkt 3, 8 § punkt 4 och 9 § punkt 3 i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:8) om informationssäkerhet för leverantörer av samhällsviktiga tjänster**. 5 § punkt 5, 6 § punkt 4 och 14–15 §§ i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter**.

Managing unwanted events

Table 11. Checklist – Managing unwanted events

Number	Description	Help text	Reference to standard or guidance	Link to statutes
H1	A policy regarding incident and crisis management is established and known in the organisation.		**ISO 22320:2019** Section 4.	
H2	Objectives have been developed for the organisation's work with managing unwanted events.		**ISO 22320:2019** Section 5.2.1 and 5.3.1.	
H3	The organisation has sufficient resources to meet the objectives/requirements regarding the organisation's work with managing unwanted events.		**ISO 22316:2020** Section 4.2, 5.2, 5.5 and 5.7–5.8. **ISO 22320:2019** Section 5.2.1f, 5.2.4b, 5.3.3.4, 5.3.4 and Appendix B6.	15 § i **Förordning (2022:524) om statliga myndigheters beredskap**.
H4	The organisation has established and documented work practices for how to handle an unwanted event, including clear roles and responsibilities: • Internally within the own organisation. • In cooperation with other actors.		**ISO 22301:2019** Section 8.4–8.4.3. **SS 22304:2023** Section 8.4–8.4.3. **ISO 22313:2020** Section 8.4–8.4.3. **ISO 22320:2019** Section 5.3.1. **FSPOS Crisis Management Guidance** Section 3.1. **Common grounds** – framework for cooperation and management work practices/ common direction and coordination.	6 § i **Lag (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap**.
H5	The organisation has established contacts,networks, or forums with relevant actors.		**ISO 22301:2019** Section 8.4–8.4.3. **SS 22304:2023** Section 8.4–8.4.3. **ISO 22313:2020** Section 8.4–8.4.3. **ISO 22320:2019** Section 6.2.3–6.2.4 and Appendix A3. **Common grounds** – framework for cooperation and management.	9 § i **Förordning (2022:524) om statliga myndigheters beredskap**. 6 § i **Förordning (2017:870) om länsstyrelsernas krisberedskap och uppgifter inför och vid höjd beredskap**.

Number	Description	Help text	Reference to standard or guidance	Link to statutes
H6	The organisation has a contact point for: • Alerts and coordination internally within the organisation. • To cooperate with other actors.	For example TiB, official on standby, responsible manager, direction and coordination contact (ISK) or equivalent.	**ISO 22320:2019** Section C3. **Common grounds** – framework for cooperation and management.	2 § i **Förordning (2017:870) om länsstyrelsernas krisberedskap och uppgifter inför och vid höjd beredskap**. 15 § i **Förordning (2022:524) om statliga myndigheters beredskap**.
H7	The organisation conducts external monitoring for the purpose of strengthening its management capabilities.	External monitoring is conducted to actively collect, analyse, evaluate and convey information that helps organisations create a knowledge of the surrounding world to support better decision-making in an event/ emergency.	**ISO 22316:2020** Section 5.3. **Common grounds** – framework for cooperation and management.	15 § i Förordning (2022:524) om statliga myndigheters beredskap.
H8	The organisation has methods for drawing up and communicating situational pictures internally and externally.	A situational picture is a selection of information compiled in the form of descriptions or assessments of the situation. The purpose is to provide an overview, understanding or basis for decisions and measures.	**ISO 22320:2019** Section 5.2.1h and 5.3.3.1h. **FSPOS Crisis Management Guidance** Section 3.1.2 and 3.2.2. **Common grounds** – framework for cooperation and management/work practices/ situational picture.	12 § i **Förordning (2022:524) om statliga myndigheters beredskap**. 4 § 1 punkten i **Förordning (2017:870) om länsstyrelsernas krisberedskap och uppgifter inför och vid höjd beredskap**.
H9	The organisation has appropriate technical systems and equipment in place to deal with an unwanted event that may affect critical infrastructure.		**ISO 22320:2019** Section 6.3.3.	
H10	The organisation has procedures in place to document the handling, analysis and decision before, during and after an unwanted event occurs.		**SS 22304:2023** Section 8.4.2. **ISO 22320:2019** Section 6.2.5.	

Number	Description	Help text	Reference to standard or guidance	Link to statutes
H11	The organisation has drawn up one or more plans for managing unwanted events. These plans may include: • Objective and purpose. • Procedure for alerts and activation of plan. • Contact details, both internally and to other actors. • Methods and forms for how unwanted events should be managed internally and in cooperation with other actors. • Procedures for sharing information and creating situational pictures. • Internal and external communication procedures. • Crisis communication procedures. • External monitoring procedures. • Premises and technical equipment. • Procedures for lessons learned. • Procedures for training and exercise of plan. • Recovery plan.	Plans may consist of one or more procedures, checklists, etc. They are used in the event where there is a need to establish a crisis management organisation to deal with the event. These plans may be called contingency plans, crisis management plans, etc.	**ISO 22301:2019** Section 8.4.2. **ISO 22320:2019** Section 5.3.1–5.3.3. **FSPOS Crisis Management Guidance** Section 3.1.3 and 3.2.1.	2 kap. 1 § och 8 § **islag (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap genom**.
H12	The organisation has made plans to be able to provide psychological and social care of its own staff.		**ISO 22320** Section 4.3.	

Swedish Civil
Contingencies
Agency

651 81 Karlstad Telephone 0771-240 240 **www.msb.se/en/**
Publication no. MSB2536 – December 2024 ISBN 978-91-7927-589-1