

SVENSK STANDARD

SS-ISO 22316:2017



Fastställt/Approved: 2017-10-18
Publicerad/Published: 2017-10-25
Utgåva/Edition: 1
Språk/Language: engelska/English
ICS: 03.100.01; 04.140

Säkerhet och resiliens – Organisatorisk resiliens – Principer (ISO 22316:2017, IDT)

Security and resilience – Organizational resilience – Principles and attributes (ISO 22316:2017, IDT)

This preview is downloaded from www.sis.se. Buy the entire standard via <https://www.sis.se/std-8029030>

Standarder får världen att fungera

SIS (Swedish Standards Institute) är en fristående ideell förening med medlemmar från både privat och offentlig sektor. Vi är en del av det europeiska och globala nätverk som utarbetar internationella standarder. Standarder är dokumenterad kunskap utvecklad av framstående aktörer inom industri, näringsliv och samhälle och befrämjar handel över gränser, bidrar till att processer och produkter blir säkrare samt effektiviserar din verksamhet.

Delta och påverka

Som medlem i SIS har du möjlighet att påverka framtida standarder inom ditt område på nationell, europeisk och global nivå. Du får samtidigt tillgång till tidig information om utvecklingen inom din bransch.

Ta del av det färdiga arbetet

Vi erbjuder våra kunder allt som rör standarder och deras tillämpning. Hos oss kan du köpa alla publikationer du behöver – allt från enskilda standarder, tekniska rapporter och standardpaket till handböcker och onlinetjänster. Genom vår webbtjänst e-nav får du tillgång till ett lättnavigerat bibliotek där alla standarder som är aktuella för ditt företag finns tillgängliga. Standarder och handböcker är källor till kunskap. Vi säljer dem.

Utveckla din kompetens och lyckas bättre i ditt arbete

Hos SIS kan du gå öppna eller företagsinterna utbildningar kring innehåll och tillämpning av standarder. Genom vår närhet till den internationella utvecklingen och ISO får du rätt kunskap i rätt tid, direkt från källan. Med vår kunskap om standarders möjligheter hjälper vi våra kunder att skapa verklig nytta och lönsamhet i sina verksamheter.

Vill du veta mer om SIS eller hur standarder kan effektivisera din verksamhet är du välkommen in på www.sis.se eller ta kontakt med oss på tel 08-555 523 00.



Standards make the world go round

SIS (Swedish Standards Institute) is an independent non-profit organisation with members from both the private and public sectors. We are part of the European and global network that draws up international standards. Standards consist of documented knowledge developed by prominent actors within the industry, business world and society. They promote cross-border trade, they help to make processes and products safer and they streamline your organisation.

Take part and have influence

As a member of SIS you will have the possibility to participate in standardization activities on national, European and global level. The membership in SIS will give you the opportunity to influence future standards and gain access to early stage information about developments within your field.

Get to know the finished work

We offer our customers everything in connection with standards and their application. You can purchase all the publications you need from us - everything from individual standards, technical reports and standard packages through to manuals and online services. Our web service e-nav gives you access to an easy-to-navigate library where all standards that are relevant to your company are available. Standards and manuals are sources of knowledge. We sell them.

Increase understanding and improve perception

With SIS you can undergo either shared or in-house training in the content and application of standards. Thanks to our proximity to international development and ISO you receive the right knowledge at the right time, direct from the source. With our knowledge about the potential of standards, we assist our customers in creating tangible benefit and profitability in their organisations.

If you want to know more about SIS, or how standards can streamline your organisation, please visit www.sis.se or contact us on phone +46 (0)8-555 523 00



Den internationella standarden ISO 22316:2017 gäller som svensk standard. Detta dokument innehåller den officiella engelska versionen av ISO 22316:2017.

The International Standard ISO 22316:2017 has the status of a Swedish Standard. This document contains the official version of ISO 22316:2017.

© Copyright/Upphovsrätten till denna produkt tillhör SIS, Swedish Standards Institute, Stockholm, Sverige. Användningen av denna produkt regleras av slutanvändarlicensen som återfinns i denna produkt, se standardens sista sidor.

© Copyright SIS, Swedish Standards Institute, Stockholm, Sweden. All rights reserved. The use of this product is governed by the end-user licence for this product. You will find the licence in the end of this document.

Upplysningar om sakinnehållet i standarden lämnas av SIS, Swedish Standards Institute, telefon 08-555 520 00. Standarder kan beställas hos SIS Förlag AB som även lämnar allmänna upplysningar om svensk och utländsk standard.

Information about the content of the standard is available from the Swedish Standards Institute (SIS), telephone +46 8 555 520 00. Standards may be ordered from SIS Förlag AB, who can also provide general information about Swedish and foreign standards.

Denna standard är framtagen av kommittén för Samhällssäkerhet, SIS/TK 494.

Har du synpunkter på innehållet i den här standarden, vill du delta i ett kommande revideringsarbete eller vara med och ta fram andra standarder inom området? Gå in på www.sis.se - där hittar du mer information.

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Principles	2
4.1 General.....	2
4.2 Coordinated approach.....	2
5 Attributes for organizational resilience	2
5.1 General.....	2
5.2 Shared vision and clarity of purpose.....	2
5.3 Understanding and influencing context.....	3
5.4 Effective and empowered leadership.....	3
5.5 A culture supportive of organizational resilience.....	4
5.6 Shared information and knowledge.....	4
5.7 Availability of resources.....	4
5.8 Development and coordination of management disciplines.....	5
5.9 Supporting continual improvement.....	5
5.10 Ability to anticipate and managing change.....	5
6 Evaluating the factors that contribute to resilience	6
6.1 General.....	6
6.2 Organizational requirements.....	6
6.2.1 General.....	6
6.2.2 Determining gaps.....	7
6.3 Monitoring and assessment.....	7
6.3.1 Methods and processes.....	7
6.3.2 Review.....	7
6.4 Reporting.....	8
Annex A (informative) Relevant management disciplines	9
Bibliography	10

SS-ISO 22316:2017 (E)

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 292, *Security and resilience*.

Introduction

Organizational resilience is the ability of an organization to absorb and adapt in a changing environment to enable it to deliver its objectives and to survive and prosper. More resilient organizations can anticipate and respond to threats and opportunities, arising from sudden or gradual changes in their internal and external context. Enhancing resilience can be a strategic organizational goal, and is the outcome of good business practice and effectively managing risk.

An organization's resilience is influenced by a unique interaction and combination of strategic and operational factors. Organizations can only be more or less resilient; there is no absolute measure or definitive goal.

A commitment to enhanced organizational resilience contributes to:

- an improved ability to anticipate and address risks and vulnerabilities;
- increased coordination and integration of management disciplines to improve coherence and performance;
- a greater understanding of interested parties and dependencies that support strategic goals, and objectives.

There is no single approach to enhance an organization's resilience. There are established management disciplines that contribute towards resilience but, on their own, these disciplines are insufficient to safeguard an organization's resilience. Instead, organizational resilience is the result of the interaction of attributes and activities, and contributions made from other technical and scientific areas of expertise. These are influenced by the way in which uncertainty is addressed, decisions are made and enacted, and how people work together.

This document establishes the principles for organizational resilience. It identifies the attributes and activities that support an organization in enhancing its resilience.

This document includes:

- principles providing the foundation for enhancing an organization's resilience;
- attributes describing the characteristics of an organization that allow the principles to be adopted;
- activities guiding the utilization, evaluation and enhancement of attributes.

Security and resilience — Organizational resilience — Principles and attributes

1 Scope

This document provides guidance to enhance organizational resilience for any size or type of organization. It is not specific to any industry or sector. This document can be applied throughout the life of an organization.

This document does not promote uniformity in approach across all organizations, as specific objectives and initiatives are tailored to suit an individual organization's needs.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 22300, *Societal security — Terminology*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22300 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <http://www.iso.org/obp>
- IEC Electropedia: available at <http://www.electropedia.org/>

3.1 management

coordinated activities to direct and control an organization

3.2 interested party

person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity

Note 1 to entry: This can be an individual or group that has an interest in any decision or activity of an organization.

3.3 organizational culture

collective beliefs, values, attitudes and behaviour of an organization that contribute to the unique social and psychological environment in which it operates

3.4 organizational resilience

ability of an organization to absorb and adapt in a changing environment

3.5 values

beliefs an organization adheres to and the standards that it seeks to observe

SS-ISO 22316:2017 (E)

4 Principles

4.1 General

The principles provide the foundation upon which a framework and strategy to achieve an enhanced state of organizational resilience can be developed, implemented and evaluated.

An organization's resilience:

- a) is enhanced when behaviour is aligned with a shared vision and purpose;
- b) relies upon an up-to-date understanding of an organization's context;
- c) relies upon an ability to absorb, adapt and effectively respond to change;
- d) relies upon good governance and management;
- e) is supported by a diversity of skills, leadership, knowledge and experience;
- f) is enhanced by coordination across management disciplines and contributions from technical and scientific areas of expertise;
- g) relies upon effectively managing risk.

4.2 Coordinated approach

The organization should develop a coordinated approach that provides:

- a mandate to ensure its leaders and top management are committed to enhance organizational resilience;
- adequate resources needed to enhance the organization's resilience;
- appropriate governance structures to achieve the effective coordination of organizational resilience activities;
- mechanisms to ensure investments in resilience activities are appropriate to the organization's internal and external context;
- systems that support the effective implementation of organizational resilience activities;
- arrangements to evaluate and enhance resilience in support of organizational requirements;
- effective communications to improve understanding and decision making.

5 Attributes for organizational resilience

5.1 General

An organization that has adopted the resilience principles will demonstrate common attributes supported by activities, which guide their utilization, evaluation and enhancement. Such attributes include those described in [5.2](#) to [5.10](#).

5.2 Shared vision and clarity of purpose

Organizational resilience is enhanced by a clearly articulated and understood purpose, vision and values to provide clarity to decision making at all levels of the organization.

The organization should prioritize and resource the following activities:

- a) articulate its vision, purpose and core values to all interested parties to provide strategic direction, coherence and clarity in all decision-making;
- b) ensure individual goals and objectives are aligned with and committed to the organization's purpose, vision and values;
- c) monitor and review regularly the suitability of the organization's strategies and their alignment with purpose, vision, core values and objectives;
- d) recognize the need to reflect on and, if necessary, revise the organization's purpose, vision and core values in response to external and internal changes;
- e) seek out and promote new and innovative ideas to achieve and develop its strategic objectives.

5.3 Understanding and influencing context

A comprehensive understanding of the organization's internal and external environments will help the organization make more effective strategic decisions about the priorities for resilience.

The organization should demonstrate and enhance the following:

- the ability to think beyond current activities, strategy, and organizational boundaries;
- understanding, collaborating and strengthening of relationships with relevant interested parties to support the delivery of the organization's purpose and vision.

The organization should prioritize and resource the following activities:

- a) monitor and evaluate the organization's context, including interdependencies, political, regulatory environment and competitor activities under changing circumstances;
- b) maintain strong relationships with interested parties and foster co-operation at all levels;
- c) collaborate with interested parties that share the organization's purpose and vision.

5.4 Effective and empowered leadership

Organizational resilience is enhanced by leadership that develops and encourages others to lead under a range of conditions and circumstances, including during periods of uncertainty and disruptions.

The organization should demonstrate and enhance the following:

- effective leadership throughout the organization that encourages a culture supportive of resilience;
- leadership that can adapt to changing circumstances;
- leadership that utilizes a diverse set of skills, knowledge and behaviour within the organization to achieve organizational objectives.

The organization should prioritize and resource the following activities:

- a) develop trusted and respected leaders who act with integrity and are committed to a sustained focus on organizational resilience;
- b) assign roles and responsibilities for enhancing organizational resilience;
- c) encourage the creation and sharing of lessons learned about success and failure and promote the adoption of better practice;
- d) empower all levels of the organization to make decisions that protect and enhance the resilience of the organization.