TECHNICAL SPECIFICATION

ISO/TS 22375

First edition
2018-10

Security and resilience — Guidelines for complexity assessment process

Sécurité et résilience — Lignes directrices relatives au processus d'évaluation de la complexité

Reference number
ISO/TS 22375:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

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 of 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 www.iso.org/iso/foreword.html.

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

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Complexity is a fundamental property of many systems. An appropriate level of complexity is required for systems operation, but a high degree of complexity can weaken the system, particularly during turbulent times. High system complexity could be an obstacle to the security, resilience, effectiveness and efficiency of all organizations. As organizational systems, products, processes, technologies, organizational structures and contracts become more complex, organizations may fail to pay sufficient attention to the introduction and proliferation of more complex and less secure systems that then become unsustainable and lose their integrity. Figure 1 explains where the introduction of complexity can improve performance, but where, after it reaches certain point, it will degrade performance. Point A is the best ratio between performance and complexity.

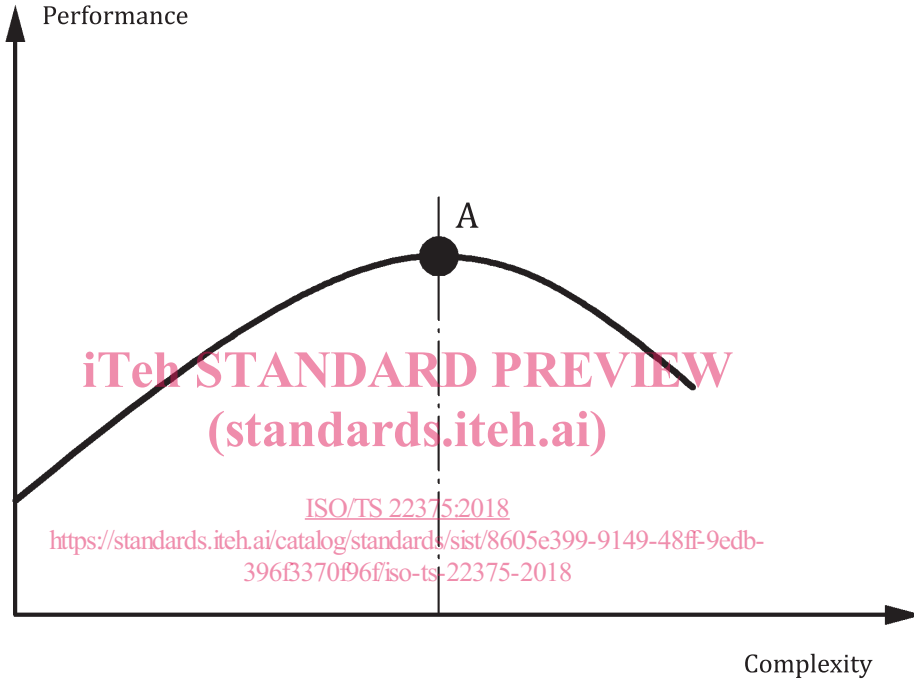

Figure 1 — The impact of complexity against performance

Organizational complexity cannot be increased indefinitely, however. If complexity exceeds a manageable level, e.g. interdependencies expand to the degree that all elements are connected with one another, the system behaviour turns chaotic. Hence, the relationship between organizational complexity and performance is hypothesized to be inversely u-shaped, as shown in Figure 1[16].

The complexity of an organization's system is influenced by external and internal factors, often linked to direct or indirect actions carried out by different parties.

Day-to-day managerial decisions about the organization's activities tend to generate complexity.

For large companies with decentralized decision-making, decisions tend to be made without the assessment of complexity cost and benefit trade-offs.

These decisions could add complexity without creating customer or competitive benefits and could increase the organization's vulnerability.

Moreover, the decisions taken by customers, competitors and suppliers, as well as the enactment of new regulations, induce the organizations to adapt themselves to new scenarios. Increasing the complexity of the external environment may induce the organization to increase the number of functional units and this could increase functional and structural complexity of the organization.

Functional complexity is characterized by its management system and its business processes set out in directives, procedures and reports.

Structural complexity deals with the variety of elements and relationships among the people, products and services, and assets of the organization.

To assess the complexity of an organization's system, it is necessary to take into account a large number of parameters where the interactions change and develop dynamically and in a non-linear laws.

This is particularly true in the context of a turbulent and interdependent global economy, punctuated by shocks and instabilities of increasing intensity and frequency, which can undermine the performance and survival of any system.

High complexity is an important source of a new form of risk called "complexity-related risk" that organizations have to address and manage if the security and resilience of its system are to be sustained.

This document aims to stimulate organizations to take into account the threat created by an excess of complexity and to consider complexity assessment as an integral part of their plan for security management.

Security and resilience — Guidelines for complexity assessment process

1 Scope

This document gives guidelines for the application of principles and a process for a complexity assessment of an organization's systems to improve security and resilience. A complexity assessment process allows an organization to identify potential hidden vulnerabilities of its system and to provide an early indication of risk resulting from complexity.

This document is generic and applicable to all sizes and types of organization systems, such as critical assets, strategic networks, supply chains, industrial plants, community infrastructures, banks and business companies.

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, *Security and resilience — Vocabulary*

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 https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
complexity
condition of an organizational system with many diverse and autonomous but interrelated and interdependent components or parts where those parts interact with each other and with external elements in multiple end non-linear ways

Note 1 to entry: Complexity is the characteristic of a system where behaviour cannot be determined only as the sum of individual variables behaviours.

3.2
parameter
specific value describing the measurable or theoretical features of the elements of a system

4 Principles

To carry out complexity assessment process effectively, an organization should adopt and apply the principles below.

a) Complexity is a fundamental property of many organization's systems. An appropriate level of complexity is required for systems operations.

b) High complexity could be a source of a new form of risk called “complexity-related risk”. Complexity is often an important cause of vulnerability and should be managed.

c) The complexity assessment process should inform the security management process and the risks management process. It helps the organization to enhance the security and resilience of its system.

d) A complex system has numerous components and interconnections, interactions or interdependences that may be difficult to describe, understand, predict, manage, design and change. The complexity assessment process aims to identify the most important process/parameters that contribute to making the system vulnerable.

e) A complexity assessment process enhances an organization’s resilience and creates strategic and tactical advantages. It assists the organization to decide how to reduce the variability/volatility of the parameters to achieve these benefits.

5 Preliminary assessment process

5.1 General

The preliminary assessment process for the complexity assessment process provides the foundations, structures and capabilities that enable the process to be applied and to ensure its consistent application.

5.2 Mandate and commitment

Top management should provide evidence of its commitment to the development and implementation of the complexity assessment process and to continually improving its effectiveness by:

a) defining and endorsing the organization’s policy for managing the complexity assessment process;

b) determining the objectives consistent with the organization’s policy;

c) ensuring the availability of sufficient resources and reliable data sources;

d) assigning roles, accountabilities and responsibilities at appropriate levels within the organization;

e) establishing an awareness programme to communicate the benefits of the complexity assessment process to relevant interested parties;

f) ensuring legal and regulatory compliance.

5.3 Needs and expectations of interested parties

The organization should identify all interested parties relevant to managing the complexity assessment process and should determine their requirements based on their needs and expectations.

The organization should ensure that the requirements of interested parties are considered.

5.4 Embedding competence and awareness

The organization should make the complexity assessment process a core value of the organization and should ensure the required competence is maintained.

The organization should ensure that any person(s) is (are) competent on the basis of appropriate education, training or experience, and should retain associated records to provide evidence of the training.

The organization should identify training needs associated with its security management plan. It should provide training or take other action to meet these needs, and should retain associated records.

6 Planning the assessment process

6.1 General

The complexity assessment process should be an integral part of the security management process and should be tailored to the objectives of the organization.

6.2 Defining the scope

6.2.1 The organization should define the scope of the complexity assessment process that is appropriate to:

a) its size and nature;

b) its requirements, considering its mission, goals, legal responsibilities, and internal and external obligations;

c) its operational objectives, products and services, activities and resources.

6.2.2 The scope should include:

a) the goals and objectives of the process;

b) the frequency, depth and breadth of measurement;

c) specific inclusions and exclusions;

d) the complexity assessment structure and methodologies.

6.3 Determining the objectives

6.3.1 The organization should define the objectives of the complexity assessment process in accordance with the security management process.

6.3.2 The process could be addressed to identify, at least:

a) the structural complexity of the organization;

b) the functional complexity of the organization;

c) the interdependencies between organizational process and functional units;

d) the main parameters connected with the complexity of the system.

6.3.3 These objectives should:

a) be consistent with the scope and policy;

b) be retained as documented information;

c) be clearly stated;

d) have time frames for their achievement;

e) enable opportunities to maintain or improve performance;

f) be monitored and updated as appropriate.

6.4 Establishing the external context

The organization should identify those areas of the external environment in which it seeks to achieve its objectives. The external context can include, but is not limited to:

a) the social, cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;

b) the external infrastructure on which the organization depends, including the market, utilities, suppliers, logistics and related processes;

c) key external drivers and trends that impact on the objectives of the organization.

6.5 Establishing the internal context

The organization should identify the factors of the internal environment in which it seeks to achieve its objectives. The internal context can include, but is not limited to:

a) governance arrangements, including policies, structures, roles and accountabilities, and the decision-making processes (both formal and informal);

b) personnel and related capabilities;

c) physical assets, technologies and internal infrastructure;

d) capital, financial arrangements and income streams;

e) information systems, reporting and other information flows.

6.6 Establishing resource requirements

6.6.1 General

The organization should allocate sufficient resources to managing each step of the complexity assessment process. The allocation should consider:

a) funding;

b) trained and competent personnel with the appropriate knowledge, skills and experience;

c) procedures, methods and supporting infrastructure;

d) communication and documentation.

6.6.2 Personnel

6.6.2.1 The organization should:

a) appoint one or more management representatives who, irrespective of other responsibilities, should have defined roles, responsibilities and authority for ensuring the effectiveness of the complexity assessment process;

b) identify the skills and knowledge required by those involved in the complexity assessment process;

6.6.2.2 Knowledge requirements include:

a) analytic systems, business intelligence, etc.;

b) organizational processes and functional units of the organization;

c) corporate enterprise resource planning (ERP) or business warehouse systems, and protocols, etc.

6.6.3 Procedure

The organization should define a specific, flexible and focused procedure to manage the implementation of the complexity assessment process.

This procedure should define:

a) how the assessment is to be clearly targeted to the organization's system;

b) the frequency within which assessments are conducted and the intervals between assessments that are considered to be appropriate by the organization;

c) how the changes since the last assessment are to be determined.

The complexity assessment process may be performed by self-review or on-site review by an external organization or a combination of both.

6.6.4 Method

The organization should:

a) identify suitable assessment methodologies and/or techniques to identify, analyse and evaluate the complexity;

b) choose the appropriate qualitative and/or quantitative analytic approach based on the type, size, or nature of the organization and resource and skill constraints.

NOTE A qualitative approach uses the answers to questionnaires to identify the main causes of increases in the complexity of the organization's system.

A quantitative approach uses algorithms to measure the parameters within the ERP to highlight the critical points of the system or the organization.

6.6.5 Communication

The organization should have effective communication and consultation procedures for the exchange of information of the complexity assessment process with interested parties.

These should include:

a) internal communication among interested parties, including employees within the organization;

b) external communication with customers, partners and other interested parties, including the media;

c) receiving, documenting and responding to communication from all interested parties.

6.6.6 Documentation

The complexity assessment process documentation should include:

a) policy, scope and objectives;

b) complexity assessment process options;

c) awareness programme;

d) training programme;

e) procedures for implementing the complexity assessment process.

7 Implementing the assessment process

7.1 General

The main source of complexity in an organizational system is the unpredictable variability of its most important and interdependent parameters.

These parameters could be identified inside these main fields:

a) size and diversity of products and services;

b) management hierarchy and behaviours;

c) amount of directives, procedures and reports;

d) relationships among the people of functional units;

e) interactions among the operative, support and control processes.

A list of potential parameters that drive complexity is provided in Annex A.

7.2 Assessment process

The complexity assessment process should be managed at three different levels.

a) LEVEL 1: Define complexity environment.

At this level, the organization can identify only the framework of the organizational system in terms of external and internal complexity fields.

b) LEVEL 2: Qualitative complexity assessment.

If the organization recognizes that the complexity of its organizational system could generate a risk, it should use methodologies and/or techniques for a qualitative complexity assessment.

The assessment is performed with questionnaires, which should be filled in during suitable surveys and workshop. Through a set of internal and external parameters, it is possible to compare the interrelationships among the organizational elements (process, product, organization, performance, resources, mission etc.) and identify the related complexity fields.

c) LEVEL 3: Quantitative complexity assessment.

If the organization wishes to thoroughly investigate its complexity, it should pass to a quantitative methodology. It should use algorithms that highlight the critical issues of the organizational system through the measurement of parameters inside the ERP.

The output is the ranking of each parameter based on its contribution to overall system complexity.

Annex B provides some examples of how to carry out the complexity assessment process.

8 Monitoring and review

8.1 The organization should develop procedures for the systematic monitoring and review of the performance of the complexity assessment process on a regular basis and at planned intervals.

8.2 Monitoring procedures should:

a) determine the extent to which the organization's complexity assessment process, objectives and targets are met and how they impact system performance over the expected range of operating situations;

