PD ISO/TS 22375:2018

BSI Standards Publication

Security and resilience — Guidelines for complexity assessment process

urrently in preview, click buy full versi

bsi.

National foreword

This Published Document is the UK implementation of ISO/TS 22375:2018.

The UK participation in its preparation was entrusted to Technical Committee GW/3, Private Security Management & Services.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2018
Published by BSI Standards Limited 2018

ISBN 978 0 580 96117 5

ICS 03.100.01

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 October 2018.

Amendments/corrigenda issued since publication

Date	Text affected

urrently in preview, click buy full versi

TECHNICAL SPECIFICATION

ISO/TS 22375

First edition
2018-10-16

Security and resilience — Guidelines for complexity assessment process

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

urrently in preview, click buy full versi

Reference number
ISO/TS 22375:2018(E)

© ISO 2018

COPYRIGHT PROTECTED DOCUMENT

© ISO 2018, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

Currently in preview, click buy full version

Contents

Page

Foreword ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Principles **1**
5 Preliminary assessment process **2**
5.1 General 2
5.2 Mandate and commitment 2
5.3 Needs and expectations of interested parties 2
5.4 Embedding competence and awareness 2
6 Planning the assessment process **3**
6.1 General 3
6.2 Defining the scope 3
6.3 Determining the objectives 3
6.4 Establishing the external context 4
6.5 Establishing the internal context 4
6.6 Establishing resource requirements 4
6.6.1 General 4
6.6.2 Personnel 4
6.6.3 Procedure 5
6.6.4 Method 5
6.6.5 Communication 5
6.6.6 Documentation 5
7 Implementing the assessment process **6**
7.1 General 6
7.2 Assessment process 6
8 Monitoring and review **6**
Annex A (informative) **List of potential parameters that drive complexity** **8**
Annex B (informative) **Examples of how to carry out the complexity assessment process** **12**
Bibliography **28**

urrently in preview, click buy full versi

© ISO 2018 – All rights reserved

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.

urrently in preview, click buy full versi

 © ISO 2018 – All rights reserved

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 they 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.

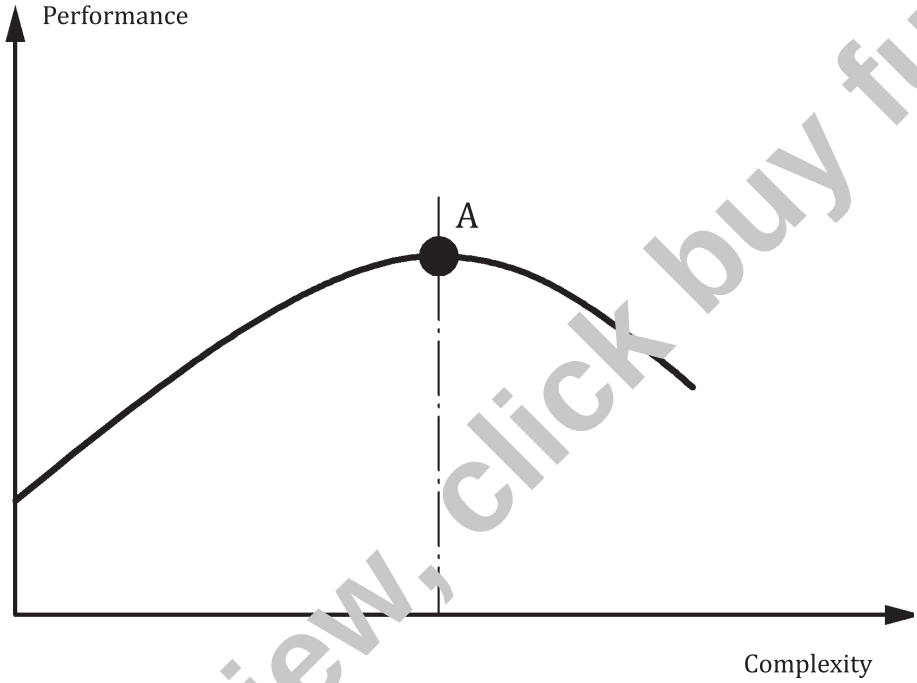

Figure 1 – The impact of complexity against performance

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.

Currently in preview, click buy full version

© ISO 2018 – All rights reserved

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.

urrently in preview, click buy full versi

© ISO 2018 – All rights reserved

TECHNICAL SPECIFICATION **ISO/TS 22375:2018**

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 and 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.

© ISO 2018 – All rights reserved

Currently in preview, click buy full version