
Security and resilience — Guidelines for complexity assessment process

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

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[ISO/TS 22375:2018](https://standards.iteh.ai/catalog/standards/iso/8605e399-9149-48ff-9edb-396f3370f96f/iso-ts-22375-2018)

<https://standards.iteh.ai/catalog/standards/iso/8605e399-9149-48ff-9edb-396f3370f96f/iso-ts-22375-2018>



iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[ISO/TS 22375:2018](https://standards.iteh.ai/catalog/standards/iso/8605e399-9149-48ff-9edb-396f3370f96f/iso-ts-22375-2018)

<https://standards.iteh.ai/catalog/standards/iso/8605e399-9149-48ff-9edb-396f3370f96f/iso-ts-22375-2018>



COPYRIGHT PROTECTED DOCUMENT

© ISO 2018

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
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	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

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.

ISO/TS 22375:2018

<https://standards.iteh.ai/catalog/standards/iso/8605e399-9149-48ff-9edb-396f3370f96f/iso-ts-22375-2018>

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.

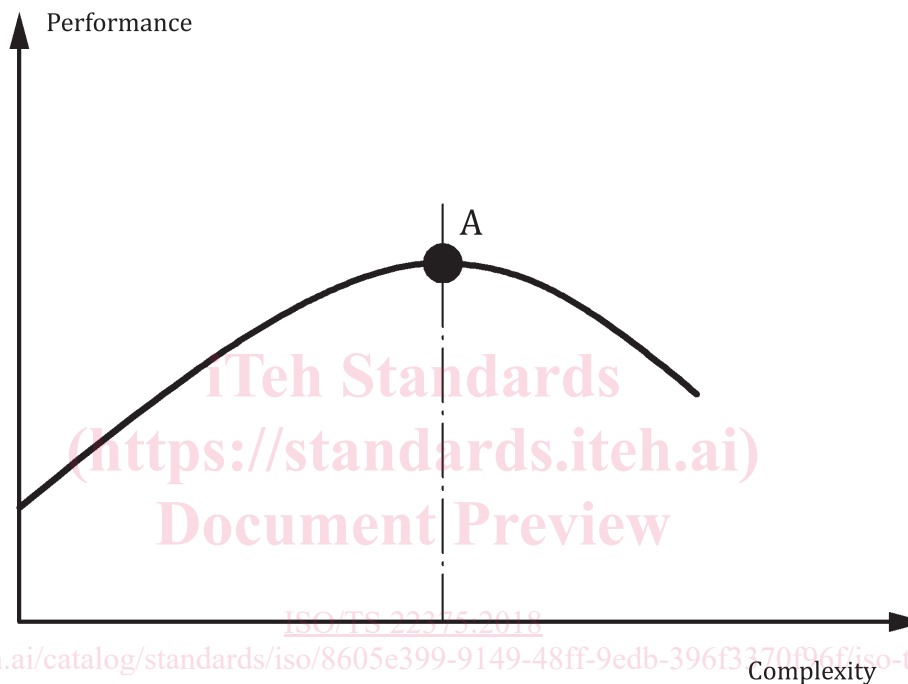


Figure 1 — The impact of complexity against performance

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.