AS ISO 22340:2024
ISO 22340:2024

Australian STANDARD®

STANDARDS Australia

Security and resilience — Protective security — Guidelines for an enterprise protective security architecture and framework

currently in preview, click buy full versi

AS ISO 22340:2024

This Australian Standard® was prepared by MB-025, Security and Resilience. It was approved on behalf of Standards Australia's Standards Development and Accreditation Committee on 06 December 2024.

This Standard was published on 20 December 2024.

The following are represented on Committee MB-025:

Australasian Fire and Emergency Service Authorities Council
Australian Emergency Management Institute
Australian Institute of Human Resources
Australian Risk Policy Institute
Australian Security Industry Association
Australian Strategic Policy Institute
Business Continuity Institute Australasia
Department of Defence (Australian Government)
Energy Networks Australia
Engineers Australia
International Association of Privacy Professionals, Australia and New Zealand
Office of the Victorian Information Commissioner
Risk and Insurance Management Society of Australasia
Risk Management Institute of Australasia
Security Professionals Australasia
Victorian Managed Insurance Authority

This Standard was issued in draft form for comment as DR AS ISO 22340:2024.

currently in preview, click buy full version

Keeping Standards up-to-date

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals, and new projects by visiting:
www.standards.org.au

ISBN 978 1 76139 976 3

Security and resilience — Protective security — Guidelines for an enterprise protective security architecture and framework

First published as AS ISO 22340:2024.

COPYRIGHT

© ISO 2024 — All rights reserved
© Standards Australia Limited 2024

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968 (Cth).

currently in preview, click buy full version

Preface

This Standard was prepared by the Standards Australia Committee MB-025, Security and Resilience.

The objective of this document is to provide guidance on the enterprise protective security architecture and the framework of protective security policies, processes and types of controls necessary to mitigate and manage security risks across the protective security domains, including —

(a) security governance;

(b) personnel security;

(c) information security;

(d) cybersecurity; and

(e) physical security.

This document is applicable for any organization.

This document is identical with, and has been reproduced from, ISO 22340:2024, *Security and resilience — Protective security — Guidelines for an enterprise protective security architecture and framework.*

As this document has been reproduced from an international document, a full point substitutes for a comma when referring to a decimal marker.

Australian or Australian/New Zealand Standards that are identical adoptions of international normative references may be used interchangeably. Refer to the online catalogue for information on specific Standards.

The terms “normative” and “informative” are used in Standards to define the application of the appendices or annexes to which they apply. A “normative” appendix or annex is an integral part of a Standard, whereas an “informative” appendix or annex is only for information and guidance.

urrently in preview, click buy full versi

© Standards Australia Limited 2024

Contents

currently in preview, click buy full version

currently in preview, click buy full versi

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 document 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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.

currently in preview, click buy full version

© Standards Australia Limited 2024

Introduction

This document aims to meet a global need for organizations to formulate and integrate their protective security controls in a way that is based on risk management principles and strategically aligned with the interests of the organization. It details an enterprise architecture and integrated framework within which a diverse suite of security-related policy, processes and practices can be coordinated.

Clarity on what protective security is, what it means, how it can be implemented, and how its benefits can be measured, will be helpful to managers, regardless of the sector. This is particularly important for the many organizations that have expended substantial resources on various security measures that have not necessarily been coordinated or informed by the full range of security risk. In an increasingly complex security environment, this document aims to provide clarity in this regard and to provide a basis for better enterprise security outcomes as a result.

This document:

a) Provides guidance on how organizations and their managers can implement and manage coherent protective security arrangements.

b) Demonstrates the critically important idea that effective security management is based on an understanding of risk and the application of risk management principles and that the form and implementation of security controls (that protect an organization's assets) are integral to the long-term success of the organization. Security is a business enabler, not an overhead cost to the organization.

c) Defines and details the elements of protective security, outlines an enterprise protective security governance model and defines the roles and responsibilities necessary in delivering protective security outcomes.

d) Demonstrates the critical importance of establishing and sustaining an organizational culture supporting positive security behaviours: where all personnel and interested parties have a sense of shared ownership of security outcomes; and where all are authorized and competent to act in the security interests of the organization and invested in the security of the organization.

e) Outlines the importance of continuous improvement in relation to an organization's protective security.

This document is applicable for any organization and will be particularly useful for those that have had difficulty implementing risk-based frameworks appropriate to their security context. Organizations with such difficulties can be guided by this document in identifying and procuring appropriately competent services to assist.

The guidelines contained in this document do not provide detailed procedures at the technical or operational level. Where standards are not available at this level, organizations should formulate and implement procedures based on the high-level guidance contained in this document and according to best practices at international and national levels.

urrently in preview, click buy full versi

© Standards Australia Limited 2024

Australian Standard®

Security and resilience — Protective security — Guidelines for an enterprise protective security architecture and framework

1 Scope

This document provides guidance on the enterprise protective security architecture and the framework of protective security policies, processes and types of controls necessary to mitigate and manage security risks across the protective security domains, including:

a) security governance;

b) personnel security;

c) information security;

d) cybersecurity;

e) physical security.

This document is applicable for any organization.

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 terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

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

3.1
asset owner
person within an organization who is responsible for a given asset

3.2
business impact
impact on an organization's or sector's ability to operate resulting from the compromise of confidentiality, integrity or availability of assets

3.3
culture
shared values and attitudes that are applied within an organization by its personnel and interested parties

Note 1 to entry: This recognizes that an organization has a culture that, to varying degrees, supports and accepts security as part of business as usual; and that fostering this element of the organization's culture should be the aim of top management in delivering protective security outcomes.

© Standards Australia Limited 2024

currently in preview, click buy full version