Doc: MSD 17 (26221)/WC
ISO/FDIS 22340

WIDE CIRCULATION DRAFT

BUREAU OF INDIAN STANDARDS
(DRAFT FOR COMMENTS ONLY)

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

ICS 13.310, 03.100.01

Risk Management, Security and Resilience, Sectional Committee, MSD 17	**Last Date for receipt of Comments is October 2024**

NATIONAL FOREWORD

(Formal clauses to be added later on)

The text of the International Standard has been approved as suitable for publication as an Indian Standard without deviations. Certain conventions are, however, not identical to those used in Indian Standards. Attention is particularly drawn to the following:

a) Wherever the words 'International Standard' appear referring to this standard, they should be read as `Indian Standard'.

In this adopted standard, reference appears to an International Standard for which Indian Standard also exist. The correspondence Indian standard, which is to be substituted in its place, is listed below along with degree of equivalent for the editions indicated:

International Standard	*Corresponding Indian Standard*	*Degree of Equivalence*
ISO 22300, Security and resilience — Vocabulary	IS/ISO 22300: 2021, Security and Resilience - Vocabulary	Identical

Note: The technical content of the document is not available on website. For details, please refer the corresponding ISO/FDIS 22340 or kindly contact:

Head
Management and Systems Department
Bureau of Indian Standards
Manak Bhawan, 9, B.S. Zafar Marg
New Delhi – 110 002
Email: msd@bis.org.in
Telephone/Fax: 011-23231106

Scope

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

a) security governance;
b) personnel security;
c) information security;
d) cyber security;
e) physical security.

This document is applicable for any organization.

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 policy framework within which the diverse community of security-related policy, processes and practices can be coordinated.

Clarity on what protective security is, what it means, and how it can be implemented and its benefits measured, will be helpful to managers, regardless of sector. This is particularly important for the many organizations that have expended substantial resources on various security measures (physical, cyber, and operational) 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 the management elements within them can implement and manage coherent protective security arrangements.
b) Demonstrates the critically important idea that effective security management is risk based, or based on risk management, and that the form and implementation of security risk controls (that protect an organization’s assets) are integral to the long-term success of the organization. Security is a business enabler, not purely an overhead cost to the organization.
c) Defines and details the elements of protective security, outlines an enterprise 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 policy frameworks appropriate to their security context. Organizations with such difficulties may 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 in accordance with better international and national practice.