

HAYS GLOBAL

CYBER & INFORMATION SECURITY

STRATEGY

THE ROADMAP FOR HAYS GLOBAL
CYBER AND INFORMATION SECURITY
TO 2030



ACCOUNTANCY &
MA/CONSTRUCTI
CONTACT CENTR
ATIONS/EDUCATI
HNOLOGY/LEGAL
SAFETY/POLICY&
OURCES & MINING
NGINEERING/HU
LOGISTICS/FACILITIES MANAGEMENT/FINANCIAL
CIAL SERVICES/SOCIAL CARE/SALES & MARKETI
ING/ENERGY/OFFICE SUPPORT/RESPONSE MANA
HEALTHCARE/OIL & GAS/ARCHITECTURE/ASSESS
& DEVELOPMENT/PUBLIC SERVICES/ACCOUNTAN
NCY & FINANCE/EDUCATION/PHARMA/CONSTRU
NSTRUCTION & PROPERTY/RESOURCE MANAGEM
MENT/MANUFACTURING & OPERATIONS/RETAIL/I
INFORMATION TECHNOLOGY/SALES & MARKETING
RATEGY/BANKIN
MARKETING/ENE
INING/TELECOMS
HUMAN RESOURC
TRES/FINANCIAL
PHARMA/MANUF
HEALTHCARE/AR
PROCUREMENT/H

UCATION/PHARM
TY/CONTACT CEN
URING & OPERATI
ON TECHNOLOGY
NT/HEALTH & SAF
NKKING/RESOURC
INSURANCE/ENG
RESOURCES/LOG
PUBLIC SERVICES
RESOURCES&MIN
ENGINEERING/H
CONTACT CENTR
ES/SOCIAL CARE
NG/ENERGY/HEA
OFFICE SUPPORT
LEGAL/OIL & GAS

Purpose of Hays Cyber and Information Security Strategy

This Strategy establishes the roadmap for Hays Global Cyber and Information Security at all levels.

The strategy aligns all regions to a unified approach to tackling cyber security threats and ensuring that a set of minimum-security policies, standards, and controls are established and maintained on an ongoing basis.

Goals and Scope of the Hays Cyber Strategy

- The Global Cyber and InfoSec Strategy sets out the high-level approach to Cyber Security up until 2030.
 - The strategy will be reviewed on a regular basis by the global cyber security committee.
- It sets out the approach to improve and strengthen Cyber and Information Security across the Group on a continuous improvement basis.
- The strategy is split into two separate parts: **Part 1** - Cyber and Infosec vision, and **Part 2** - Implementation and approach.
- This Strategy is designed to provide a consistent approach to Cyber Security for all regions of Hays and to drive a standard methodology and minimum sets of controls and defenses.

Challenges of the Digital Age and Hays response

Technology is evolving and the adoption of digital technologies rapidly increasing; with this so are the cyber and Information security risks.

This Strategy sets out, at a high level, the Hays approach to the response and mitigation of Cyber and Information risks, as far as possible, facing the business.

This provides a guide to the business and IT to assist them to make well-informed risk-based decisions.

This Strategy is designed to support efforts to **Detect, React** to and **Defend** against Cyber and Information threats and risks;

Highlighting the organisational, process, and technological responses needed to support the strategy at both a global and regional level.

The primary audience of this document is the IT organisation and Cyber Security / Risk Management roles or functions.



Strategy Document Contents

Part 1: Strategy

Hays Strategic Context

Overall Strategy, Strategic Context, Cyber and InfoSec Landscape, Cyber and Information Security Change Management.

Hays Vision

Cyber Vision, Goals, and Principles, Role, Responsibilities, and Authorities, Enforcement

Part 2: Implementation

Hays Global Cyber and Information Security and the 6 Pillars

Pillar 1: Business First Approach

Pillar 2: Establish Trust

Pillar 3: Communicate and Collaborate

Pillar 4: Adoption of Cyber Tools, Techniques, and Tracking

Pillar 5: Security Built-In

Pillar 6: Smart Detect, React, and Defence

Delivering Hays Cyber and IT Ambition

Understand Cyber Risk, Cyber Resilience, Scope for Implementation, Control and Monitoring, Frameworks, Cyber Security Implementation Procedure, Incident Response Management (IRM) Process.



For further
details contact
your local IT
Security team

Serious about
Security

