Cybersecurity

CYBERSECURITY GOVERNANCE

At Hindustan Zinc, we are committed to investing significantly in our cybersecurity, ensuring robust governance and a strong cybersecurity risk posture. Enhancing cyber resilience across our operations through improved technology and control systems is an ongoing process. We relentlessly focus on maintaining data integrity, safety, confidentiality, and business continuity against cyberattacks and disasters.

We have employed a robust enterprise risk management framework to achieve the highest standards of cybersecurity and consistent improvement in our cybersecurity posture.

Governance Committee

Board's Audit and Risk Management Committee

Composition

Chaired by our Independent Director, Mr. Kannan Ramamirtham, who is also a trained expert in "Enterprise Cyber Risk Management" with a special focus on Metals & Mining industry. He is experienced in:

- Embedding cyber risk management in strategic decisions
- Overseeing enterprise cyber resilience programmes including resiliency planning, incident management and recovery management
- Overseeing associated budget allocation and KPIs in cyber risk management programmes

Responsibilities and Accountability

- Reports to the Board
- Responsible for all business risks, including cyber risks
- Responsible for overseeing cybersecurity governance

IT and Cyber Security Steering Committee

Composition

- Chaired by the Chief Executive Officer (CEO)
- Comprises leaders from all the business functions, including IBU Heads, Chief Financial Officer (CFO), Chief Human Resource Officer (CHRO), Chief Information Officer (CIO) and Chief Commercial Officer (CCO)

Responsibilities and Accountability

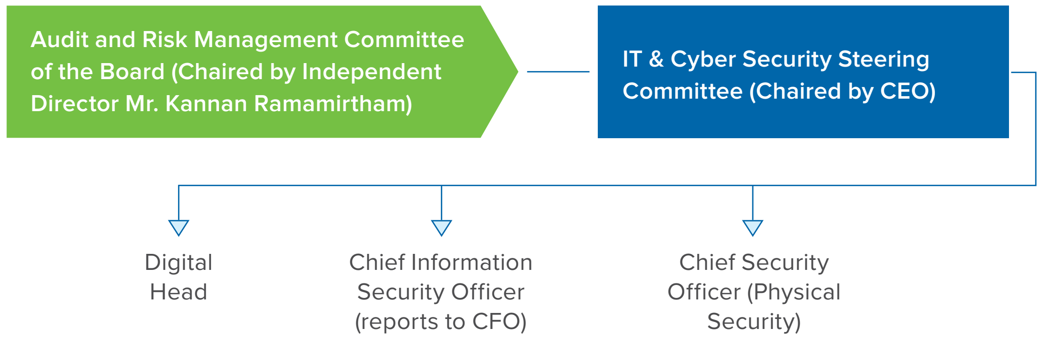
- Set up expectations, provide direction and support for the cybersecurity measures
- Review and monitor the progress and maturity of the organisation's cybersecurity posture

Chief Information Security Officer (CISO)

Responsibilities and Accountability

- Sets up the cybersecurity vision and strategy
- Defines cybersecurity governance framework
- Ensures the execution of the programmes for protecting confidentiality, integrity and availability of all information assets
- Holds accountability to the IT and Cyber Security Steering Committee as well as the Audit and Risk Management Committee of the Board on all cybersecurity matters

As outlined below, our leadership and governance structure guides our cybersecurity strategy, execution and monitoring.


Audit and Risk Management Committee of the Board (Chaired by Independent Director Mr. Kannan Ramamirtham)
IT & Cyber Security Steering Committee (Chaired by CEO)
Digital Head
Chief Information Security Officer (reports to CFO)
Chief Security Officer (Physical Security)

AGILITY IN CYBERSECURITY RISK MANAGEMENT

We fully acknowledge the need for a strong and agile cybersecurity risk management framework to protect the confidentiality, integrity and availability of our technology and data assets. We have employed a robust risk management framework, characterised by the following elements:

Risk-focused Cybersecurity Framework

Anchored in clearly defined principles/standards and an objective-based approach, the framework prioritises risk mitigation and implementation of critical controls around all our assets.

Cybersecurity Standards

Our Cybersecurity framework is supported by information security management and personal data privacy standards, disaster recovery and business continuity management, and risk management, ensuring strong governance for our information technology and cybersecurity practices.

Integrated ISO Certification

ISO 27001 (Information Security), ISO 22301 (Disaster Recovery & Business Continuity Plan), ISO 31000 (Risk Management), and ISO 27701 (Privacy Management) cover 100% of our assets in India.

Alignment with COBIT Framework

Our risk register and risk control matrix are aligned with the control objectives of the information and related technology (COBIT) framework

INFORMATION SECURITY FRAMEWORK

To manage information security in the Company, we maintain a well-established and comprehensive Information Security Management Framework, integral to our Enterprise Risk Management (ERM) framework. The framework covers various relevant policies, standard operating procedures (SOPs), technology standards, and an effective security assessment and audit process for preventing cyberattacks. Implementation of security-by-design in our business and technology landscape has further strengthened the framework.

Elements of the Information Security framework:

Cyber Resilience

Our Cyber Crisis Management Plan (CCMP) covers:

- 24x7 security incident detection and monitoring plan, and response and recovery playbooks
- Handshake with the organisation's crisis management plan, and associated decision/communication matrix for cross-functional stakeholders
- Cyber insurance and incident response retainer services to provide protection from low-probability, high-impact cyberattacks
- Annual executive cyber drills and purple teaming for continuous improvement of our cyber resilience

Social Engineering and Awareness

Our holistic and continuous cybersecurity awareness programmes enhance the team's capabilities to identify and report breaches. Some of these initiatives include:

- Mandatory cybersecurity training is integrated into the new joiners' onboarding process
- A self-service online awareness training capsule is available to all users
- Annual extensive security awareness covers all employees and business partners with access to our systems or premises
- Security awareness is communicated via posters, gamified videos, quizzes, end-to-end social engineering simulations (including scenarios such as phishing, vishing, smishing, deep-fake and digital arrest scenarios, etc.)
- Cyber Security Awareness Month (CSAM) is observed with various informative and engaging activities, featuring live demonstrations of prevalent digital frauds by external speakers

Data Privacy Readiness

Key measures taken by the Company to enhance Data Privacy Readiness include:

- Privacy information management system (PIMS), supported by privacy policies, procedures, consent management and data subject rights management
- Privacy awareness among our employees
- Privacy impact assessments for business processes involving large-scale personal information
- Data discovery to identify personally identifiable information (PII) collection, storage, processing, transfer, etc.

Operational Technology Security

Aimed at preventing cyber attackers from exploiting any vulnerabilities that may exist in legacy systems, we:

- Have invested significantly in the phased upgradation of our operational technology (OT) systems/plant technical systems to their latest versions
- Conduct vulnerability scanning of OT systems to identify and remediate known vulnerabilities declared by original equipment manufacturers (OEMs)
- Intend to implement a dedicated Security Operations Centre (SOC) for OT environment to ensure long-term resilience of plant technical systems

Cloud Security

- Perform risk-based remediation of security issues related to our assets, such as virtual machines, applications, services, etc., hosted in corporate IaaS (Infrastructure as a Service) cloud or SaaS (Software as a Service) applications
- Ensure that our assets are integrated with the Security Operations Centre (SOC) for 24x7 security monitoring
- Implemented a web application firewall and privileged access management, which ensures that our crown jewel applications and privileged users have an automated protection layer against cyberattacks

Data Leakage Prevention

- Thorough data flow analysis (DFA), along with our business/functional teams, is conducted to identify critical data and crown jewels
- A comprehensive data leakage prevention (DLP) capability, informed by DFA, has been implemented, covering various communication channels such as web, email, mobile devices, etc.
- Regular DLP rule-based review and fine-tuning ensure continuous alignment with DFA
- A dedicated 24x7 DLP monitoring desk monitors and manages all data leakage incidents

Third-Party Risk Management

- Systematically identified third parties posing cybersecurity risks to the organisation, with the required governance structure to address and mitigate them
- Annual risk assessment conducted for high-risk third parties (including new third-party vendors), ensuring risk measurement and mitigation
- Appropriate security clauses incorporated into third-party contracts

Governance, Risk and Compliance

As a risk-centric organisation, Hindustan Zinc has implemented a comprehensive risk management framework and conducts detailed risk assessments to identify and address a broad array of organisational risks. In line with the identified strategic areas, we regularly implement numerous cybersecurity initiatives to bolster our capabilities across businesses and minimise related risks. This risk framework guides our information security strategy and informs our long-term and short-term roadmaps.

SETTING DATA PROTECTION STANDARDS WITH DPDPA ALIGNMENT

Hindustan Zinc has defined and rolled out an ambitious privacy compliance and readiness programme to align with the Digital Personal Data Protection Act, 2023 (DPDPA). The initiative involves identifying privacy risks/footprint across processes and/or applications through detailed ROPA (Record of Processing Activities) and DFD (Data Flow Diagrams), performing gap assessment, and preparing privacy policies, procedures and templates incorporating DPDPA requirements and global privacy best practices. Alongside technical implementations, such as privacy notices/cookie banners, data masking, encryption, consent management, etc., we have also formalised an organisation of trained Privacy Champions and Business Heads, responsible for stewardship of any personal data processing as a part of their business processes, going forward.

Hindustan Zinc is certified in the ISO 31000:2018 risk management framework.

Review of Policies and Procedures

Review by the IT and Cyber Security Steering Committee

Annual review of the risk framework by the IT and Cyber Security Steering Committee, in consultation with external expert agencies, facilitates the integration of applicable regulatory requirements, prevailing industry insights, and evolving threats and risks.

Review by CIO, CISO and Information Security Function

The CIO, CISO and other competent personnel in our information security function review the information security and data governance policies and procedures every year, to keep pace with the evolving security landscape.

The approved and enforced policies are made available to all employees and business partners (BPs) through impactful communication across media.

INCIDENT MANAGEMENT AND RESPONSE

At Hindustan Zinc

- Our Security Operations Centre (SOC), data loss prevention (DLP) desk operations, and reports from both the information security function and end users detect all information security and data incidents
- There is a well-established system to track and monitor all security incidents to logical closure
- Root cause analysis is performed and mitigation plans are developed, in line with our incident management and data breach policy, to avoid future recurrence of such incidents
- A well-defined and comprehensive escalation process is also in place
- Disaster recovery drills (DR drills) are conducted twice a year as part of our business continuity plan (BCP)

Vulnerability Management

We maintain a robust vulnerability management policy that enables us to effectively identify and mitigate risks and vulnerabilities across information technology (IT), operational technology (OT) and digital environment. The in-depth structure of the Company's vulnerability management programme extends across all tiers of defence, ensuring adequate coverage to policy & framework, physical perimeter, network, application, and data security.

Vulnerability Assessment and Analysis

Multiple assessments were conducted during the year to enable vulnerability identification, threat monitoring, shortcomings and associated risk/impact analysis, tracking of mitigation actions and continuous compliance. These assessments include governance & framework review, red teaming exercise as part of physical security assessment, data governance and compliance assessment. We also engage globally reputed and recognised third-party agencies for internal and external vulnerability assessment and penetration testing (VAPT) programme, surveillance audit under various ISO frameworks and assessment of IT general controls (ITGC) by a statutory auditor under applicable financial compliance frameworks.

We employ VAPT, including simulated hacker attacks, which are conducted at least twice a year. This exercise helps us define, identify, classify, and prioritise vulnerabilities in computer systems, applications, and network infrastructures. The exercise is conducted jointly by Hindustan Zinc's information security function and group management assurance services (MAS) function. Our consistently strong performance is reflected in the fact that we are among the highest-rated entities as part of the MAS audit group.

Evaluation, Escalation And Reporting

Escalation Mechanism

As a part of our security paradigm, we facilitate our employees to report suspicious activities or threats against the organisational assets, intellectual property, other business documentation, our personnel, or finances, to Myitsupport@vedanta.co.in and hzl.isms@vedanta.co.in. Phishing emails are reported via the "Report Phishing" option provided in the mail menu. Subsequently, these incidents undergo due review and analysis, followed by an escalation process post triage.

Integrating Cybersecurity with Employee Performance Evaluation

At Hindustan Zinc, we leverage a multi-faceted framework for employee performance evaluation, synergising the goals and performance of IT/OT personnel with the Company's information security goals. The effectiveness of the processes and technologies is measured through multiple internal and external vulnerability assessments, management reviews, and reported incidents. Further, as part of the social engineering simulation exercises, offenders are issued advisory letters from the CHRO's office, cautioning them about the risks and potential punitive actions that any repeated instance of offence may incur.

Our Report Card

	FY2025	FY2024
Total number of information security breaches	0	0
Total number of clients, customers and employees affected by the breaches	0	0