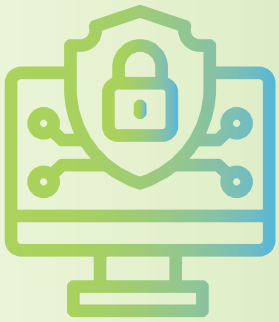


# CYBER SECURITY

# CYBER SECURITY APPROACH NOTE

HZL has established a well-entrenched and comprehensive Information Security Framework which includes Policies, Standard Operating Procedures (SOPs), and Technology Standards. HZL has also established an effective security assessment and audit process for preventing cyber-attacks, and implementation of security-by-design and privacy-by-design in HZL's business and technology landscape has further strengthened the framework.

The note covers the following aspects:

A. Context Setting (Importance of Cyber Security)

B. Leadership & Governance Structure

C. Information Security Planning

D. Information Security Operations

   a. Cyber resilience
   b. Social engineering and security awareness
   c. Operational Technology security
   d. Cloud security
   e. Data Governance & Privacy Management
   f. Third party risk management
   g. Governance, risk management and compliance management

E. Other core aspects

## A. IMPORTANCE OF CYBER SECURITY

Recent years have witnessed a spate of high-profile data breaches and cybersecurity events at global companies. This has triggered many corporate crises, transforming cybersecurity and cyber risks into a corporate governance issue for Boards. With regulators making it clear that cybersecurity is not merely an IT issue, companies worldwide have started embracing it as an integral component of their enterprise-wide risk management structure. Against this backdrop, cyber risk oversight has become explicitly material to the investor's ability to understand a company's strategy.

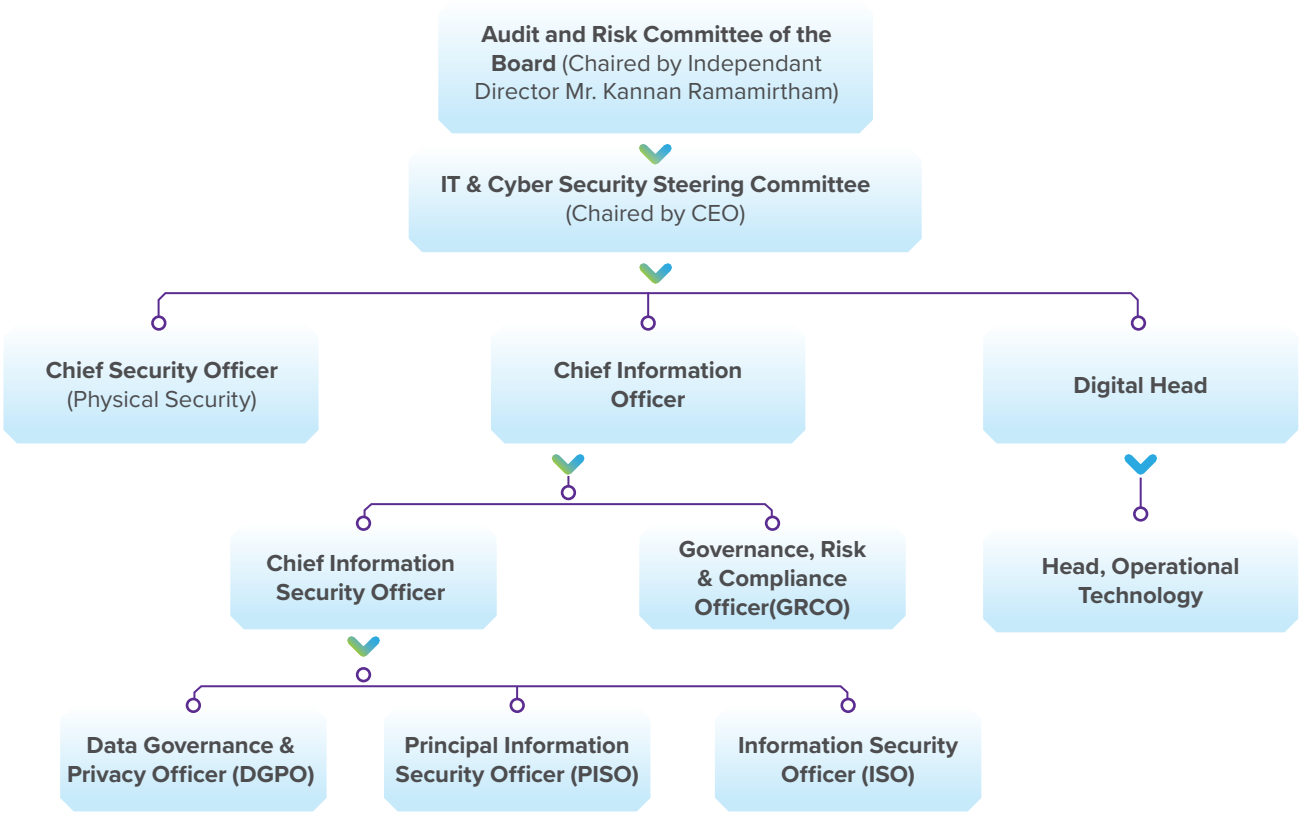
Amid this transforming business eco-system, we, at HZL, have forged aggressively and responsibly ahead towards enhancing our cybersecurity risk posture. Our efforts have yielded tangible outcomes, with the Company being ranked the highest in the metals and mining sector in the Corporate Sustainability Assessment 2023 by Standard & Poor Global. This award also endorses our success on the cybersecurity front.

Maintaining tight cybersecurity across our operations is an ongoing process, and we remain committed to ensuring that our technology and control systems are protected from attacks. We shall continue to ensure that confidential information remains safe, data integrity is protected, and business continuity is maintained in the Company in case of any disastrous event.

## B. LEADERSHIP & GOVERNANCE STRUCTURE

To ensure the highest levels of cybersecurity and to drive continuous strengthening of the same, we have in place a robust enterprise risk management framework. Board Level- The Board's Audit and Risk Committee has the responsibility of overseeing cybersecurity governance. It reports to the Board every quarter, and is responsible for all business risks, including cyber risk. It is chaired by our Independent Director Mr. Kannan Ramamirtham during the year 23-24 .

Executive Level - The IT & Cyber Security Steering Committee is mandated with the task of setting up expectations, providing direction and support, and reviewing and monitoring the progress and maturity of the cybersecurity posture of the organisation. This is done in alignment with the Company's vision and strategy. The Committee is chaired by the Chief Executive Officer (CEO), and 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) among others.




Operational level- The Chief Information Security Officer (CISO) is responsible for setting up cybersecurity vision and strategy for HZL, defining cybersecurity governance framework, and executing programmes to ensure that confidentiality, integrity, and availability of all information assets are well protected. The CISO is accountable to the IT and Cyber Security Steering Committee as well as the Audit and Risk Management Committee of the Board on all cybersecurity-related issues

The PISO (Principal Information Security Officer), reporting to the CISO, is responsible for operationally driving cybersecurity programmes to ensure that business objectives are achieved.

The Data Governance & Privacy Officer (DGPO), reporting to the CISO, is responsible for establishing the data governance framework and drive data governance and privacy management throughout the data lifecycle.

The ISO (Information Security Officer), reporting to the CISO, is responsible for Vulnerability Management program and Audit Management.

The Governance, Risk & Compliance Officer (GRCO), reporting to the CISO, is responsible for driving IT Risk Management and overall compliance to adopted governance frameworks, including Sarbanes-Oxley Act (SOX) and Disaster Recovery (DR)/Business Continuity Plan (BCP).

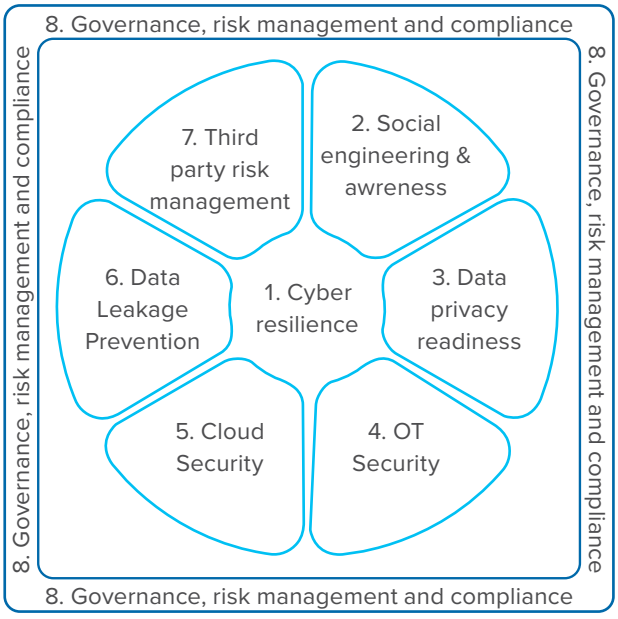
Head OT Cyber Security, reporting to Digital Head and working closely with CIO & CISO, is responsible for implementation of cybersecurity in OT system. OT cybersecurity consists of cybersecurity in SCADA/PLC, Industry 4.0 & Digitalization Initiatives and Laboratory Information Management Systems (LIMS).

The Chief Security Officer (CSO) is responsible for the physical security of the Company's assets, which include information assets. The CSO is a senior-level executive, who is accountable to the HZL IT & CYBER SECURITY STEERING COMMITTEE and works closely with the CIO and CISO

## C. INFORMATION SECURITY PLANNING

### Information Security Management Framework

Under HZL's Enterprise Risk Management (ERM) framework, HZL has established a robust Information Security Management Framework which is depicted below:



Based on this framework, information security strategy, long-term roadmap and annual information security plan is prepared.

Below is the list of industry standards, laws, acts and best practices which are referred to while preparing our Framework:

1. IMS (integrated Management Systems) with ISMS (ISO27001 :2022), BCMS (ISO22301 :2019), PIMS (ISO27701 :2019), Risk management ISO31000:2018,
2. NIST Security Framework
3. COBIT
4. Information Technology Act, 2000
5. IT General Controls under Sarbanes-Oxley (SOX) Compliance Framework
6. Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules, 2011
7. Section 43A & IT rules of Information Technology Act of India.
8. Digital Personal Data Protection Act, 2023
9. Supreme Court of India's verdict on Right to Privacy as a Fundamental Right, 28th August 2017.
10. European General Data Protection Regulation (GDPR).
11. OECD (Organization for Economic Co-Operation and Development) Privacy Guidelines
12. US Privacy Act 1974
13. Australian Privacy Act 1988
14. Aadhaar Act, 2016
15. SEBI (LODR) Regulations, 2015
16. Securities Contract (Regulation) Rules, 1957
17. Indian Companies Act, 2013
18. IEC 62443
19. Vedanta Information Security Standards
20. Cert-IN directions, Sub: Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response, and reporting of cyber incidents for Safe & Trusted Internet (No. 20(3)/2022-CERT-In)
21. Cert-IN directions, Sub: Key Roles and Responsibilities of Chief Information Security Officers (CISOs) in Ministries/Departments and Organisations managing ICT operations (No. 6(12)/2017-PDP-CERT-In)

The Information Security Framework is reviewed annually by HZL Information Security team in consultation with external expert agencies to incorporate applicable regulatory requirements, prevailing industry knowledge and emerging threats and risks.

## Standards and Certifications:

HZL is an ISO Certified Organization and has established, implemented, maintains, and continually improves the integrated management system (IMS) in accordance with the requirements of the International Standards ISO 27001:2022, ISO/IEC 27701:2019, ISO 22301:2019, ISO 31000:2018 across all the sites .

### Information Security Policies

HZL has a robust information security policy, disaster recovery policy & data governance policy and all policies are defined incorporating various applicable frameworks and domains pertaining to Information Security, Risk Management, Disaster Recovery & Business Continuity Management, and Data Privacy.

All policies and procedures are reviewed annually by competent personnel in Information Security Function. All the approved and enforced policies are made available to employees and business partners over Intranet Portal. Communication is also sent to all stakeholders when any change is carried out in any of these policies or procedures.

Policies defined by HZL are categorized under the following areas:

1. Information Security Management Policies
2. Data Governance & Privacy Management
3. Risk Management Policies.
4. Business Continuity Management Policies
5. Incident Response & Emergency Preparedness Plan

Standard Operating Procedures, Standards and Guidelines are further prepared in line with these policies.

## D. INFORMATION SECURITY OPERATION

Information Security Operations at HZL consists of following domains:

a. Cyber resilience

b. Social engineering and security awareness

c. Data Governance & Privacy Management

d. Operational Technology security

e. Cloud security

f. Third party risk management

g. Governance, Risk & Compliance Management

### Cyber resilience

Our end-to-end cyber resilience programme covers 24X7 security incident monitoring plan, incident detection, response and recovery playbooks, hand-shake with Organization Crisis management plan, and associated decision/communication matrix for cross-functional stakeholders, such as human resources, corporate communications, legal, business and information security. We have put in place cyber insurance and incident response retainer services to protect from any low-probability high-impact cyber-attacks. We conduct annual executive cyber drills and purple teaming for continuous improvement of the cyber resilience programme.

### Social Engineering and Security Awareness

To build the team's capability to identify and report breaches, HZL has prepared a holistic cybersecurity awareness plan, which is executed continually throughout the year. All new joiners are mandated to attend cybersecurity training during on-boarding process. An online awareness training capsule on self-service mode is available to all users. Our business ethics and Code of Conduct (CoC) also has a cybersecurity element with which employees must comply as it is linked with their annual performance evaluation. Information Security function tracks and monitors the status of training conducted by user and accordingly carries out periodic follow-up to propagate it further.

We conduct extensive security awareness for all employees and business partner employees who have access to HZL's systems or are working on the Company's premises. We engage with them through periodic security awareness communications as well as end-to-end social engineering simulations, including various scenarios such as phishing, smishing, vishing, deepfakes, video learnings, scare-ware/fraud-ware, etc. As part of social engineering simulation exercises, offenders are issued advisory letters from CHRO's office sensitizing them about the risks and warning about further punitive action in case of repeat offense. Exclusive webinars are also conducted for these repeat offenders. Our efforts are geared towards making these security awareness communications informative and engaging via physical posters at prominent places across the organization. We also conduct monthly stand-up sessions and executive briefings on cybersecurity at various locations.

### Data Governance & Privacy Management

At HZL Ltd, we recognize data as a vital enterprise asset that drives informed decision-making, innovation, and operational efficiency. Our Data Governance Program is strategically designed to manage data effectively, securely, and in full compliance with both national and international regulations, including the Digital Personal Data Protection Act (DPDPA) 2023 and the ISO 27701 Privacy Information Management System (PIMS).

We are committed to protecting all types of data—personal, sensitive, and business-critical—across all formats, whether digital or physical. Our governance framework integrates robust policies, technical safeguards, and continuous monitoring to ensure the confidentiality, integrity, and availability (CIA) of data throughout its lifecycle.

The implementation of ISO 27701 (PIMS) & Digital Personal Data Protection Act (DPDPA) 2023 in our organization strengthens stakeholder confidence by embedding privacy management into our operational and technological processes.

**Key Pillars of the HZL Data Governance & Privacy Program:**

* Establishment of robust data governance, privacy, and consent policies.
* Comprehensive data flow analysis to identify critical business information across HZL.
* Data classification and protection using enterprise-grade tools and automation.
* Development of privacy-specific documentation such as Records of Processing Activities (ROPA) and Data Flow Diagrams (DFD) to map the data landscape.
* Execution of Privacy Impact Assessments (PIAs) and Privacy Risk Assessments (PRAs) for processes involving personal or sensitive data.
* Clearly defined organizational structure with Data Governance & Privacy Champions, and a role Data Governance & Privacy Officer (DGPO) to lead the program.

HZL Data Governance & Privacy Management approach underscores a long-term commitment to responsible data stewardship, regulatory compliance, and building trust with stakeholders in an increasingly digital and data-driven environment.

## Operational Technology Security

We have made large investments in phased upgradation of our operational technology systems/ plant technical systems to the latest versions. This is aimed at preventing cyber attackers from exploiting any vulnerabilities that may exist in legacy systems. We further intend to conduct vulnerability scanning of operational technology systems to ensure that known vulnerabilities declared by original equipment manufacturers (OEMs) are identified and remediated.

## Cloud Security

At HZL, we leverage cloud technologies to enhance various aspects of our operations, from ERP to customer engagement and workplace safety. Our cloud security strategy is integrated into our broader cybersecurity framework, emphasizing a proactive, comprehensive, and continuously evolving approach to protect our digital assets in the cloud.

We are actively embracing digital transformation, including cloud adoption, and has a strong focus on cybersecurity to protect our operations and data.

Our approach to cloud security: Cloud Adoption and Platforms:

* **SAP RISE with SAP:** HZL has made a significant move to the cloud by upgrading to SAP S/4HANA and migrating it to the SAP RISE cloud platform. This is a key step in our journey towards becoming an intelligent and sustainable enterprise, enhancing competitive advantage, and enabling a future-ready technology landscape.
* **SAP Commerce Cloud (Hybris):** We utilize SAP Commerce Cloud for our online buying platform, "Evolve," for non-ferrous metals. This platform emphasizes convenience, security, and ease of access for customers, particularly MSMEs.
* **Cloud-based AI Inference Engine:** HZL recently deployed "Detect AI" system for workplace safety utilizes a cloud-based AI inference engine to process real-time image and video analytics, trigger automated alerts, and generate data-driven insights.

We have implemented a Web Application Firewall, which ensures that our crown jewel applications have an automated protection layer against web-based attacks.

## Third Party Risk Management

At HZL Ltd. (HZL), we recognize that third parties can pose significant cybersecurity risks to our information ecosystem. To address this, we have established a comprehensive Third-Party Risk Management (TPRM) framework that ensures proactive identification, assessment, and mitigation of these risks. Our framework tailored with the help of best-in-class TPRM standards and frameworks.

We have identified third parties that may impact our cybersecurity posture and implemented a robust governance mechanism to monitor and manage them. As part of our due diligence and ongoing oversight:

* Profiling of vendor as high medium low risk vendors based on nature of work.
* Annual third-party risk assessments are conducted for high-risk & medium risk partners,
* There is TPRM program for new onboarded partners to evaluate their security posture.
* Risks identified during assessments are documented, tracked, and mitigated through action plans and controls.
* All relevant contracts with third parties incorporate mandatory security and data protection clauses aligned with regulatory and internal policy requirements.

## Governance, Risk Management and Compliance

As a risk-driven organisation, we carry out detailed risk assessment across the organisation. We have successfully implemented a robust risk management framework, which helps the organisation to consider the full range of risks it faces. HZL is certified in the ISO 31000:2018 risk management framework.

## E. OTHER CORE ASPECTS

1. Incident management and Response
2. Business Continuity & Disaster Recovery (BCP/DR)
3. Vulnerability Management
4. Escalation, Performance Evaluation and Reporting
5. Continual Improvement

### 1. Incident management and response

**Incident Management**

Information Security and Data Incidents are generated mainly through following channels:

1. 24 x 7 Monitoring of critical IT Assets through SIEM (Security Incident and Event Management) Services.
2. Daily Monitoring of Data Movement using End Point, Email and Web Channels through DLP (Data Leakage Prevention) tools.
3. Incident reported by end user to a designated email id.
4. Incidents picked up by Internal Security Organization including breach of business code of conduct or IT acceptable usage policy.

HZL has well defined processes for detecting and reporting incidents relating to exceptional situations in day-to-day administration of IT and information security related areas. All the security incidents are tracked & monitored till logical closure including root cause analysis and action plan to mitigate them in future. HZL has well-defined Incident Management & Data Breach Policy which is circulated among all employees. This applies to all employees and business partners. HZL has set up a common e-mail id hzl.isms@vedanta.co.in to which any user can report any suspicious activities pertaining to Information Security. Every reported incident is investigated by information security personnel and action is taken to address the incident.

HZL has also implemented multiple best-in-class tools and technologies to continuously monitor critical IT assets and data movement. Such tools automatically generate incidents based on the rules. These incidents are tracked and resolved by the IT Operations Team under guidance from Information Security Organization.

**Data Incident Management**

HZL has also implemented a robust data governance structure in line with various global standards and framework. Data Governance Program consists of:

1. Defining Data Governance Framework, Policies, Procedures
2. Implementation of Best-in-Class Tools & Technologies
3. Data Incident Management
4. Data Governance Awareness and Capability Building

As part of this program, HZL has implemented a DLP tool across all channels of data communication, to detect and prevent any potential data leakages. Robust rules sets have been configured on DLP tools which has been arrived at based on Data Flow Analysis (DFA) in discussion with respective business functions. DLP tool is implemented in blocking mode.

A dedicated DLP Desk is also established to continuously detect, evaluate, and action data incidents as reported by DLP tool. Potential leakage incidents are shared to line manager for evaluation and accordingly incident is confirmed as leakage. Action is taken in line with policy in case of any data leakage.

Effectiveness of overall program is assessed under Data Governance assessments. Such assessments includes physical security aspects and compliance to Clear Desk Policy.

#### Incident Response & Emergency Preparedness Plan

HZL has a well-defined Incident & Crisis Management Response Plan to meet any emergency arising due to Cyber Incident. Under this plan various teams and roles are created and roles & responsibilities are defined for all the teams and their members. Plan also covers aspect of incident arising during office hours and non-office hours.

Crisis communication strategy is available to communicate about incident with internal & external interested parties.

Below are the teams.

- Incident Response Team
- Crisis Management Team
- Business Continuity manager
- Communication management team

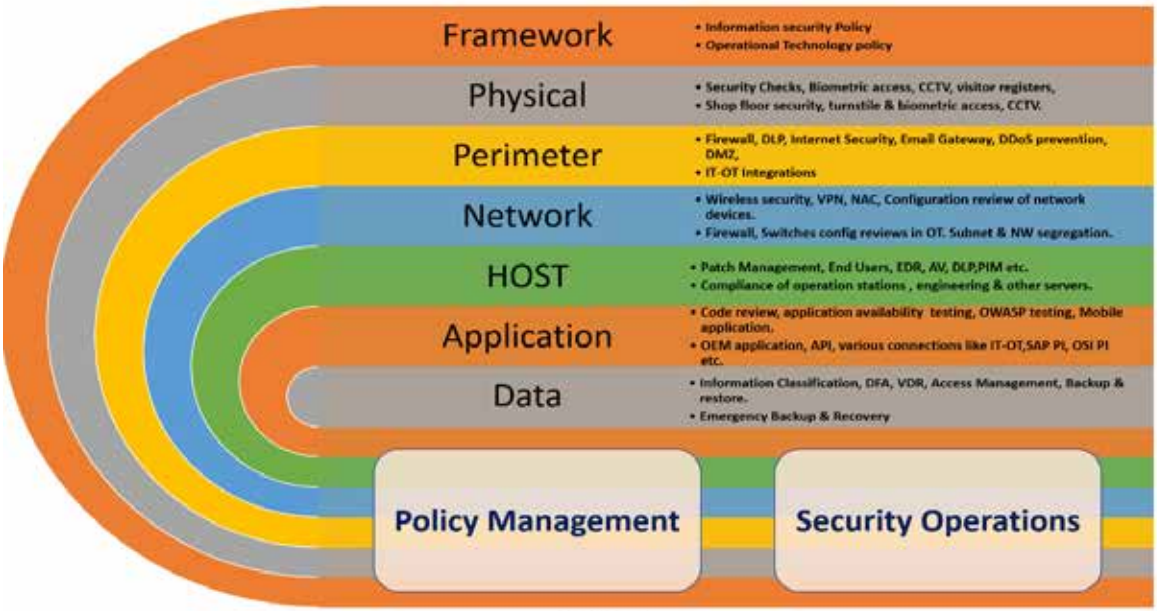
In case of any disruption, Crisis Management Team would be the key SPOC for handling all incidents at HZL and would coordinate with staff members to handle crises/incidents including ransomware.

### 2. Vulnerability Management

Risks and vulnerabilities are identified and addressed across the information technology (IT), operational technology (OT) and digital landscape, in line with the Company's vulnerability management policy. Internal and external vulnerability assessment and penetrating testing (VAPT) programme, surveillance audit, as well as assessment of IT general controls (ITGC) are carried out by globally reputed and recognised third-party agencies on an annual basis. Our vulnerability management programme is structured across all the layers of defence-in-depth covering policy & framework, physical, perimeter, network, application, and data security. Vulnerability identification, monitoring and

tracking of mitigation actions and continuous compliance are achieved through various assessments. We conduct various assessments during the year to identify vulnerabilities, threats, shortcomings, and associated risk/impact. It includes governance & framework review, red teaming exercise as part of physical security assessment, VAPT testing, data governance and compliance assessment, surveillance audit under various ISO frameworks and assessment of ITGC by statutory auditor under applicable financial compliance frameworks. VAPT including simulated hacker attacks is conducted at least twice a year and is put together by HZL's information security function and group Management Assurance Services (MAS) function. It is conducted for defining, identifying, classifying, and prioritising vulnerabilities in computer systems, applications, and network infrastructures. This helps us in conducting the assessment by providing necessary knowledge, awareness, and risk background to understand the threats to our environment and react appropriately. At the conclusion of each assessment, observation tracker is prepared for all identified vulnerabilities with clear-cut mitigation timelines and ownership, based on criticality of observation. This is rigorously monitored, reviewed and reported to various forums.

Following is the defence-in-depth layers considered as part of the program to identify risks and vulnerabilities.




**Framework** [Level-0] Vulnerability Management Program checks the relevance and effectiveness of frameworks, policies and procedures. and risks in control designing.

**Physical Security** [Level-1] Dedicated Red-Teaming is part of Vulnerability Management Program where a third-party person tries to intrude physical security of office & plant premises. Exercise is not limited to information system but also covers impact on other areas of business.

**Perimeter Security** [Level-2] External penetration testing is carried out for perimeter devices. Various attack frameworks are used to assess vulnerabilities. Possibility of lateral movement is also envisaged. Configuration reviews are also carried out for all devices.

**Network Security** [Level-3] Various scans are carried out to identify vulnerability in Wireless Security, VPN, Network Access Controls, VLAN etc. Configuration reviews are done for all network devices with reference to various benchmarks like CIS.

**Host** [Level-4] We have Host / Computing Devices Assessment Program where we identify vulnerabilities in operating systems and configuration of baselining & security policy. End computing devices are also scanned to identify vulnerabilities. Identification of Rogue & un-approved Software and tracking of Compliance Level are part of this program. Under this program, host system of VIP user is also scanned to identify vulnerability.

**Application Security** [Level-5] Method is put in place to identify vulnerabilities in all application including web-based applications and mobile applications.

Dedicated approach is created to assess security of Commercially-Off-The-Shelves (COTS) applications and SaaS (Software as a Service) applications.

**Data Security** [Level-6] HZL Vulnerability Management Program is Data Centric, and objective is to identify risk in terms of Confidentially, Integrity & Availability of Data. Privacy and data risks (such as inappropriate data upload risks, data exfiltration risks etc.) is also considered in Vulnerability Management Program.

HZL has adopted various kinds of assessments under this Vulnerability Management Program, as listed below:

## Vulnerability Assessment

Vulnerability Identification, monitoring and tracking of mitigation actions & continuous compliance level are being done through various assessments. HZL carries out / undergoes following assessments during the year to identify vulnerabilities, threats, short-comings, and associated risk/impact.

1. Internal Vulnerability Assessment and Penetrating Testing (VAPT) Program undertaken by Information Security Function (Through Third-Party Expert Agency)
2. External Vulnerability Assessment and Penetrating Testing (VAPT) Assessment through Group Management Assurance System (Through Third-Party Expert Agency).
3. Red Teaming Exercise as part of point # 2 above
4. Bug Bunty program is carried out to cross check our environment
5. Surveillance Audit under ISO 27001, ISO 22301, ISO 31000, and ISO 27701 Framework Requirements (Through Surveillance Audit Partner).
6. Assessment of IT General Controls (ITGC) by Statutory Auditor under Sarbanes-Oxley (SOX) Compliance Framework (Through Statutory Auditor).

All assessments are carried out by globally reputed and recognized third-party agencies on an annual basis. This is carried out by a team of certified and qualified personnel in various domains of cyber security and data governance.

Assessment covers the following for both IT and OT environment:

1. Overall IT Governance & Framework Review
2. Physical Security Review as part of Red Teaming Exercise
3. Vulnerability Assessment and Penetration Testing

a. Application Security (Including ERP)

b. OSDB

c. Networks

d. Active Directory

4. Compliance Assessments
5. Data Governance

Assets for assessments are arrived at through a sampling methodology considering population and criticality of assets.

Vulnerability Assessment (VA) and Penetration Testing (PT) are carried out with combination of various automated tools and manual testing as appropriate and risk ratings are arrived at using globally recognized standards and rating systems like OWASP (Open Web Application Security Project) and CVSS (Common Vulnerability Scoring System). Penetration Testing is carried out using simulated hacking techniques such as Blackbox Testing, Whitebox Testing, Greybox Testing, Red Teaming Exercise . As part of third-party vulnerability analysis, HZL conducts simulated hacker attacks.

At the conclusion of each assessment, an observation tracker is prepared for all the identified vulnerabilities with clear-cut mitigation timelines and ownership. This observation tracker consists of details like discovered vulnerabilities, severity, affected information system and kind of impact to the affected system. Severity of observation is categorized under High, Medium, Low and Information categories.

Observations are reported to various forums and progress is updated periodically to various forums as mentioned in the Information Security Governance Structure.

## Journey & Coverage of Vulnerability Assessment

HZL started its structured and focused journey of Cyber Security way back in year 2010 and since then has evolved and matured in line with current threat landscape

## Vulnerability Treatment

Treatment of vulnerabilities consists of identification and implementation of controls and measures as part of the agreed-upon observation tracker during assessment phase.

Each observation is assigned with owner and timelines for closure. Remediation timelines for such observations are aligned to Vulnerability Management Policy. Progress on remediation is tracked and monitored by Information security team.

Remediated observations are re-tested or verified based on system evidence, by the third-party agencies, as applicable. This is done by the same agency who carries out assessment.

Status of remediation progress and compliance are updated periodically to various forums and committees as mentioned in the Information Security Governance Structure.

### Information Security Administration

From Information Security Administrative perspective, observations and points emanating from the below activities would form the part of regular operations.

1. Risk Controls Matrix and Review Controls defined as part of Information Security Management Framework
2. Open observations reported through various assessments
3. Actions emerging from Annual IT Risk Assessment and DR/BCP Reviews

Each control/action point is assigned to an owner for execution purpose. This may be a one-time or recurring activity.

Execution is tracked as part of CIO's review and reviews under various other internal/external forums.

## 4. Escalation, Performance Evaluation and Reporting

**Escalation**

As part of our IT security framework we have developed an escalation process that enables employees to report anything suspicious or which is a threat to the organization, our intellectual property, our business documentation, our people, or our finances. As part of the escalation process all Information Security Incidents are reported at Myitsupport@vedanta.co.in and hzl.isms@vedanta.co.in mail ID. These incidents are then reviewed and analyzed by the IT & Cyber Security Steering committee. The escalation process is also regularly monitored by the same committee. Besides this, provision for reporting phishing mails has been given via a "Report Phishing" option in the mail menu itself.

**Performance Evaluation and Reporting**

Performance evaluation of Information Security is carried out based on following aspects:

a. People

b. Process

c. Technology

For the workforce working in IT function, each employee has well-defined KRA/KPI as part of their Annual Goals and Performance Management process and requirements in line with HZL's Information Security Goals. Performance of employee is measured against these goals. Similarly, employees working on OT environment and managing OT systems also have KPI aligned to HZL's Information Security Goals in their Annual KRA/KPI Plan.

Effectiveness of processes and technologies is measured through various internal and external vulnerability assessments, management reviews and incidents are reported as mentioned earlier.

Observations reported under internal / external vulnerability assessments are first discussed and agreed upon with respective IT asset owner along with Information security team. These observations are subsequently deliberated with CISO and final observation tracker is prepared.

Observations reported as part of Information Security Administration are reviewed by CISO along with respective IT asset owner. This is further validated during surveillance audit of ISO certifications as well as during ITGC reviews conducted by Internal & Statutory Auditors as part of SOX compliance assessments.

Cyber incidents reported through SIEM and by End Users are evaluated by PISO and are further reviewed by CISO.

Data incidents reported through DLP and by End Users are evaluated by DGPO and are further reviewed by CISO.

Based on the criticality and impact, these observations and incidents are reported and discussed in following forums for direction and support to address them.

I. HZL IT & CYBER SECURITY STEERING COMMITTEE

II. Vedanta Group EXCO

III. HZL Audit & Risk Committee

IV. Vedanta Audit & Risk Committee

Compliance to observations as per agreed due dates is reported on a quarterly basis.

**Business Continuity & Disaster Recovery Plan (BCP/DR)**

HZL recognizes that Business Continuity & Disaster Recovery is not only an IT subject, rather a business subject. Aligned to this thought, HZL has implemented ISO 22301 Disaster Recovery & Business Continuity Management Framework to prevent the interruption in operations of HZL's critical IT systems and to ensure that IT systems are continuously available to all the authorized users, all statutory & legal requirements are complied with, and organization's finance and reputational interests are protected.

Under ISO 22301 framework, HZL has defined and rolled out an effective BCP/DR. As part of this process, HZL has carried out a Business Impact Analysis (BIA) for all critical IT systems and has defined RPO & RTO for these systems in collaboration and approval by respective system owners and functional business heads. Business Continuity Plan (BCP) has considered various risks including Technical Risk, Natural Disasters Risk, Human Risk, Risk related to External Partners.

Business Continuity Testing & Disaster Recovery Drills are carried out on a half yearly basis to test the readiness of recovery sites.

A Table-Top exercise is also carried out on half-yearly basis with a role play, which provides understanding and clarity to every member of BCP/DR teams about "Do's & Don'ts" to be considered during an incident.

Since threat landscape is extremely dynamic and business undergoes frequent changes, managing information security is a major challenge. In view of this, HZL has recognized that improving information security requires more than just fixing what is broke.

HZL has adopted a process of continuously measuring effectiveness of security operations - technology, people, and processes. HZL continually assesses the security controls defined under management framework and measures the results over time through bench-marking and maturity assessments HZL also takes into account strategic, tactical and operational threat intelligence from multiple sources to strengthen its cyber security posture, and nominates its employees to attend various events/forums from where knowledge can be gained around latest trends and techniques in this area. "Project Raksha" is the flagship program adopted by HZL.

## INFORMATION SECURITY REQUIREMENTS FOR THIRD PARTIES (E.G. SUPPLIERS)

Hindustan Zinc Limited (HZL) has implemented a structured Third-Party Risk Management (TPRM) Program to ensure robust oversight and governance of third-party engagements from a security and privacy standpoint. As part of this program, HZL has defined comprehensive information security requirements for all third parties who access, process, or manage HZL data or systems.

A systematic process is in place to evaluate, monitor, and enforce third-party compliance with HZL's information security policies.

The TPRM program ensures that all third-party risks are proactively identified, assessed, and mitigated in alignment with HZL's risk appetite, regulatory obligations (such as the Digital Personal Data Protection Act), and industry best practices (e.g., ISO 27001, ISO 27701, BCMS, RMS).