Vedanta has established a robust Information Security Framework which includes Policies, Standard Operating Procedures (SOP), Technology Standards and setting up an effective Security Assessments & Audit process for prevention of Cyber Attacks and strengthening the overall Information Security Posture of Vedanta Digital Landscape.

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
E. Performance Evaluation & Reporting
F. Awareness and Capability Building
G. Continual Improvement

A. Importance of Cyber Security

Cyber security has become very important in current digital age because of the increasingly connected world we live in. The rise of the internet and smart devices have made businesses more vulnerable to cyberattacks. It's no longer a question of if, but when, your business will be hacked. Cyber security is paramount for businesses to keep their information systems and data secure.

Over the last few years, number of information security incidents and breached have increased exponentially. Such incidents adversely impact the businesses significantly, including financial losses and reputation damages. It is very important how well companies are prepared to prevent such incidents and how well it can react swiftly and appropriately in case of attack. Recognizing such importance, Vedanta has identified cyber security as a principal risk as part of overall enterprise risk management framework, with potential to impact people, environment, community, and operational performance.

B. Leadership & Governance Structure

As part of Vedanta's Enterprise Risk Management Framework, responsibility of oversight of cybersecurity governance is delegated to the Audit and Risk Committee of the Board. The Audit & Risk Committee reports to the board and is responsible for oversight of all business risks including cyber risk.

Vedanta Executive Committee has overall responsibility and accountability to set up expectations, provide direction and support, review and monitor the progress & maturity of cybersecurity posture of the organization in line with Vision and Strategy.

The Group Chief Information Officer (CIO) is responsible setting up cybersecurity vision, establishing cybersecurity strategy, define cybersecurity governance framework, and executing programs to ensure that confidentiality, integrity, and availability of all information assets are well protected. Group CIO is accountable to Dy CEO Centre of Excellence and Audit & Risk Committee of the Board for cybersecurity related matters.

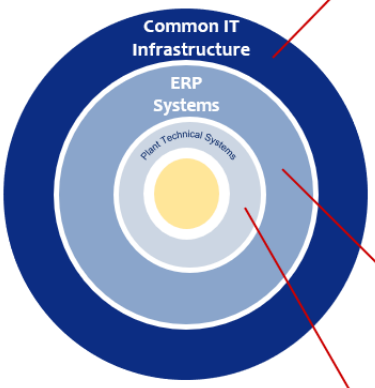
The Group Chief Information Security Officer (CISO), reporting to Group CIO, is responsible to operationally drive cybersecurity programs and ensure that business objectives are achieved. Group CISO is supported by BU CISOs and partner eco-system.

Sensitivity: Confidential (C2)

Group CISO is responsible to establish Data Governance Framework and drive Data Governance & Privacy Management and support BU Data Governance officer. Also, responsible to drive IT Risk Management and overall compliance to adopted governance frameworks including SOX and DR/BCP.

The Chief Security Officer (CSO) is responsible for physical security of company's assets which includes information assets. CSO is a senior-level executing reporting to leadership, is accountable to Vedanta EXCO and works closely with Group CIO/CISO.

Overall Information Security Framework & Governance layer adopted by Vedanta is as depicted below:



Layer	Risks	Sub – Components			
Peripheral layer of the circle / last layer – Common IT Infrastructure	• Cyber Attacks • Unauthorized access • Mis-configured Security components. • Data leakage risks • Unauthorized Software • Mobility risks	IT Risk Assessment and Management Process	Cyber Security Governance Structure	Cyber Security Policies and Procedures – Comprehensiveness	Active Directory security configuration review
		IT Security Architecture	Network Component Configuration (Firewall, Switches, Routers, etc.)	Component level security configuration check on OS and DB.	Patch Management Review
		Cyber Security Incident Management	Mobile Device Management	Logging and Monitoring	Backup and recovery review & High Availability
		Logical and Physical Access	Incident Management Review/	Cloud Security	IT Asset Management
		Antivirus Management review	Wireless Security	Remote access review	Personnel Security Review
		DLP security	Web Application testing	VA/PT	Software license management
		Email phishing campaign	Change Management Review	Cybersecurity Organisation	System and service acquisition (SDLC)
2nd Layer of the circle – ERP Systems / Business Systems	• SOD Conflicts. Unauthorized access to critical data on ERP • Non availability of business information	Logical and Physical Access	BASIS Controls	Program Change - SDLC	Computer Operations
		Interfaces between ERP and other systems		Policies and Procedures	Automated controls
3rd Layer of circle – Plant Technical Systems	• Lack of adequate IT Security governance on Core layer automation. • Remote management / Network Architecture risks • Capacity and Perf. management risks of interfacing systems • Vulnerabilities through IP networks. • Unavailability of regular patches or updates	Information Security Policies and Procedures (incl Administrative controls)	PTS / ICS / OT security and governance architecture.	Vulnerability Assessment and Penetration Testing.	Firewall configuration review
		Incident Management Review	Antivirus Management review	Patch Management Review	Backup and Recovery review
		Remote access review	Network components review	Personnel Security Review	Logical and Physical Access

C. Information Security Planning

Information Security Management Framework

Under Enterprise Risk Management (ERM) framework, Vedanta has established a robust Information Security Management Framework which includes Policies, Standard Operating Procedures (SOP), Technology Standards of all Bus and has set up an effective Security Assessments & Audit process for prevention of cyber-attacks and strengthening the overall Information Security Posture of Vedanta Technology Landscape.

Vedanta Information Security Framework is cohesive and comprehensive, and takes following aspects as an input:

1. Globally recognized Information Security Management Frameworks and Standards
2. Applicable Regulatory Requirements
3. Risk Assessment and Risk Control Matrix defined under Risk Management Process

Sensitivity: Confidential (C2)

4. Information Security Objectives aligned to Business Objectives
5. Prevailing Best Practices
6. Security Threat Intelligence

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

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

1. IMS (integrated Management Systems) with ISMS (ISO27001 :2013), 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. The Personal Data Protection Bill of India (Draft), 2018 (Justice Srikrishna Committee Report on Data Protection).
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

This Information Security Framework is reviewed annually by Vedanta Information Security Organization in consultation with external expert agencies to incorporate applicable regulatory requirements, prevailing industry knowledge and considering newer threats and risks.

Information Security Policies

Vedanta has robust information security policy & data governance policy further all BUs has adopted various Management Framework and therefore all policies are defined incorporating various applicable frameworks and domains pertaining to Information Security, Risk Management, Disaster Recovery & Business Continuity Management and Data Privacy in line with Vedanta Information Security Policy.

All the policies and procedure enforced in the Vedanta environment are all inclusive to manage the Information Security and Data Governance aspects. All these policies are reviewed annually by competent personnel in Information Security Function. All the approved and enforced policies are made available to all 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 Vedanta BUs are categorized under following areas:

Sensitivity: Confidential (C2)

1. Information Security Management Policies
2. Data Privacy Policies
3. Risk Management Policies.
4. Business Continuity Management Policies

D. Information Security Operation

Information Security Operations at Vedanta consists of following processes:

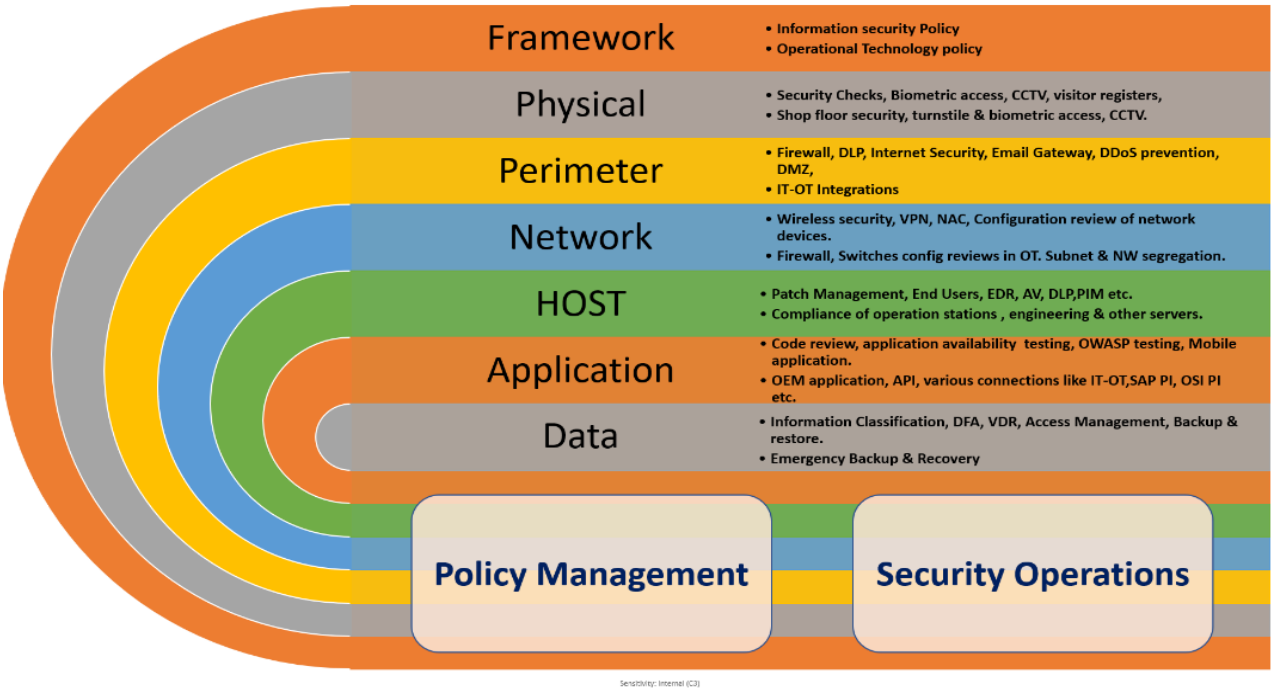
1. Vulnerability Management
2. Information Security Administration
3. Incident Management & Response (Cyber & Data Incidents)
4. Disaster Recovery & Business Continuity

Vulnerability Management

Approach

Vedanta has deployed a well-defined Vulnerability Management Program to identify and address risks and vulnerabilities across IT, OT and Digital Landscape of Vedanta. This program is tailor-made to suit to Vedanta landscape and requirements, is derived from various established and best-in-class frameworks, standards, and practices; and is structured across all the layers of defence-in-depth.

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. Based to identify risk in control designing.

Sensitivity: Confidential (C2)

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 being 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. Vedanta also conducted WASA/MASA before going live of any application.
Dedicated approach is created to assess security of Commercially-Off-The-Shelves (**COTS)** applications.

Data Security [Level-6] Vedanta Vulnerability Management Program is Data Centric, and objective is to identify risk in terms of Confidentially, Integrity & Availability of Data. Privacy is also considered in Vulnerability Management Program.

Vedanta has adopted various kind 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. Vedanta carries out / undergoes following different 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 BU 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. Surveillance Audit under ISO 27001, ISO 22301, ISO 31000, and ISO 27701 Framework Requirements (Through Surveillance Audit Partner).
5. 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

Sensitivity: Confidential (C2)

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

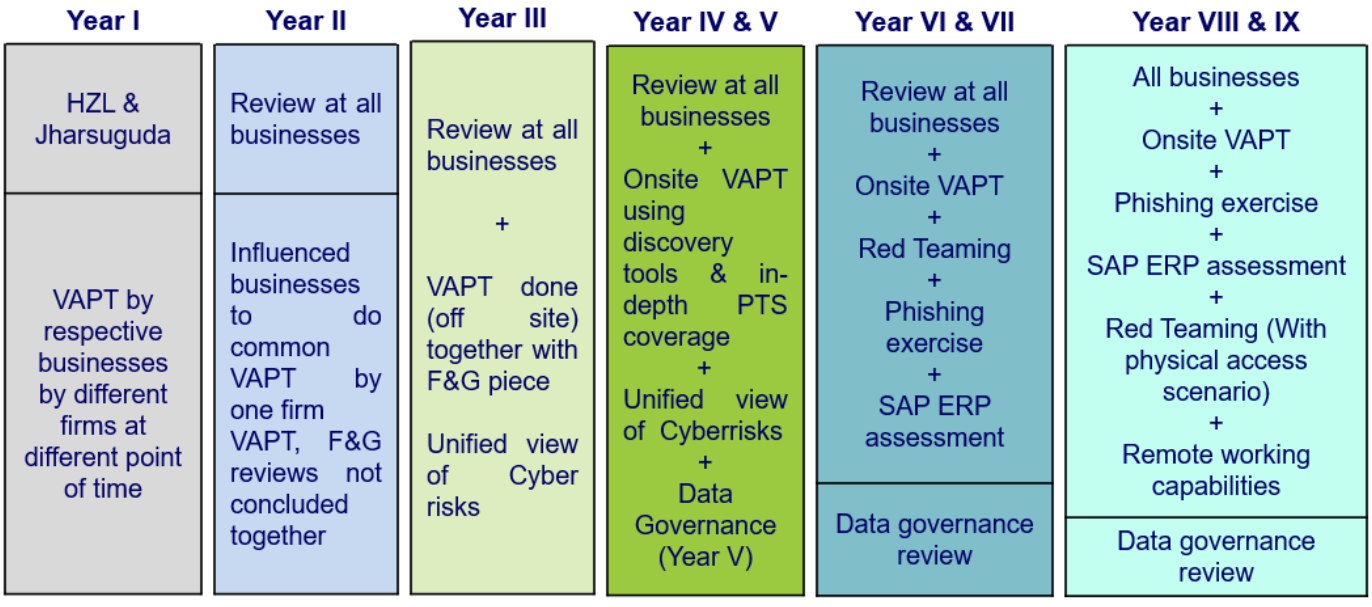
Assets for assessments are arrived at through a sampling methodology considering population and criticality of assets.

Vulnerability Assessment (VA) and Penetration Testing (PT) are carried out with combination of various automated tools and manual testing as appropriated. 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.

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 Critical, 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



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.

Sensitivity: Confidential (C2)

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 BU CISO.

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.

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. Incident picked up by Internal Security Organization including breach of business code of conduct or IT acceptable usage policy.

All the security incidents are tracked & monitored till logical closure including root cause analysis and action plan to mitigate them in future. Vedanta BUs has well-defined Incident Management & Data Breach Policy which is circulated among all employees. This applies to all employees and business partners. Vedanta BUs has set up a common e-mail id to which any user can report any suspicious activities pertaining to Information Security. Every reported incident is investigated by CISO and action is taken to address the incident.

Vedanta 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 in guidance from Information Security Organization.

Consequence Management

Sensitivity: Confidential (C2)

Organization has detailed Business Code of Conduct which is mandatory program for all employees. Business Code of Conduct is aligned with Information Security & Privacy Standards & Regulations. There is zero tolerance approach on breach of code of conduct.

Apart from this, BUs has enforced Usage Policy to all the users of IT systems. Policy also incorporates clear consequence management in case of non-compliance to the policy.

Disaster Recovery and Business Continuity Plan (DR/BCP)

Vedanta recognizes that Disaster Recovery & Business Continuity is not only an IT subject, rather a business subject. Aligned to this thought, Vedanta BUs has implemented ISO 22301 Disaster Recovery & Business Continuity Management Framework to prevent the interruption in operations of Vedanta'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, Vedanta has defined and rolled out an effective DR/BCP. As part of this process, BUs 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 to test readiness of recovery sites.

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

E. 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 in line with Vedanta's Information Security Goals as part of their Annual Goals and Performance Management process and requirements. Performance of the employee is measured against these goals. Similarly, employees working on OT environment and managing such systems also have KPI aligned to Vedanta's Information Security Goals in their Annual KRA/KPA Plan.

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

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

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

Data incidents reported through DLP and by End Users are evaluated by BU DGPO/ BU CISOand are further reviewed by BU CIO.

Sensitivity: Confidential (C2)

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. BU EXCO
II. Vedanta Group EXCO
III. BU Audit & Risk Committee
IV. Vedanta Audit & Risk Committee

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

F. Information Security Awareness and Capability Building

Vedanta understands the fact that Human is the weakest link in establishing a cyber-resilient environment. As a result, Vedanta has brought a dedicated focus on this area. At the start of the year, Information Security function prepared a holistic Cyber Security Awareness Plan and Calendar which is executed through the year. Awareness area includes all the important domains of IT and OT Security and Data Governance. This program is framed in a manner which gives clear message to all the users that Cyber Security is very crucial subject for an organization and everyone in the organization has a role to play. Content of the awareness program is prepared with an objective to make them sensitized about prevailing threats & risk, learn on mitigation aspects and ultimately change their behaviour.

Some of the activities being carried out by the organization is stipulated below.

1. All new joiners are mandatory to attend Cyber Security Training while they are onboarded to the organization.
2. Online Awareness Training Capsule on self-service mode is launched to all users. Information Security function tracks and monitors the status of training conducted by user and accordingly carries out periodic follow-up to propagate it further. Periodically trainings are also arranged through Virtual Classrooms on a voluntary / self-nomination basis.
3. BUs also conducts Dip-Stick Assessment to check the level of users' awareness, in the form of periodic tests and quizzes. Based on the effectiveness, targeted trainings & communications are made in the organization.
4. Phishing simulation is carried for all users to test the vigilance and awareness of the users. Learning from phishing simulation being shared to users. User falling prey to the simulation is also asked to undergo Phishing specific learning video as a training.
5. Awareness mailers sent to all the users on a periodic basis as cyber advisories on latest threats, tips & tricks, things need to know etc.
6. Vedanta also celebrates Cybersecurity Awareness month in October where focused Cyber Security Awareness Campaign which runs across the organization with multiple activities.
7. Data Privacy Day is celebrated in organization every year in January wherein multiple awareness activities is being carried out related to the subject matter.
8. Surprise checks on compliance of Clear-Desk are carried out for end-user desks and observations are being shared to users.
9. Guidance is circulated periodically to all users on how to classify information as per Information Classification policy.

To build the capability within Information Security Organization, members are periodically trained on various cyber security & data governance domains and are encouraged to formally get certified on applicable certificates and credentials.

G. Continual Improvement

Vedanta has adopted a process of continuously measuring effectiveness of security operations - technology, people and processes. Vedanta continually assesses the security controls defined under management framework and measures the

Sensitivity: Confidential (C2)

result over time. Learnings are further incorporated in the Information Security Management Framework. "Better Security through Better Management" is the principle adopted by Vedanta.

Annexure-1: BU wise ISO Certification

Framework is deployed in all BUs, however some entities are certified and some are under process of certifications.

S.No	BU / Group	ISO 27001		ISO 22301		ISO 31000		ISO 27701
		IT	OT	IT	OT	IT	OT	IT
1	Cairn	Yes	NO	NO	NO	NO	NO	NO
2	HZL	Yes	Yes	Yes	NO	Yes	NO	Yes
3	VZI	NO	NO	No	NO	NO	NO	NO
4	BALCO	Yes	NO	Yes	NO	NO	NO	NO
5	JSG	Yes	NO	Yes	NO	NO	NO	NO
6	LAN	Yes	NO	Yes	NO	NO	NO	NO
7	TSPL	Yes	NO	Yes	NO	NO	NO	NO
8	ESL	Yes	NO	No	NO	NO	NO	NO
9	IOB	Yes	NO	NO	NO	NO	NO	NO
10	FACOR	NO	NO	NO	NO	NO	NO	NO
11	VGCB	Yes	NO	NO	NO	NO	NO	NO
12	Nicomet	NO	NO	NO	NO	NO	NO	NO
13	Sesa Coke	NO	NO	NO	NO	NO	NO	NO
14	Gujrat NRE	NO	NO	NO	NO	NO	NO	NO
15	Desai Cement	NO	NO	NO	NO	NO	NO	NO
17	Sterlite Copper	Yes	Yes	NO	NO	NO	NO	NO
18	Fujairah Gold	No	No	NO	NO	NO	NO	NO

Annexure-2: Link of Vedanta Policies

Below are the link of Vedanta Information Security Policy & Data Governance Framework.

https://hzlone.hzlmetals.com/OneFiles/Vedanta_Data_Governance_Framework_V1_3.pdf

https://hzlone.hzlmetals.com/OneFiles/Vedanta_Information_security_Policy_V3_3.pdf

End of Document

Sensitivity: Confidential (C2)