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
    a. Risk Management
    b. Vulnerability Management
    c. Information Security Administration
    d. Incident Management & Response (Cyber & Data Incidents)
    e. Business Continuity & Disaster Recovery Plan (BCP/DR)
E. Performance Evaluation & Reporting
F. Awareness and Capability Building
G. Incidence Response & Emergency Preparedness Plan
H. 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 globally. 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.

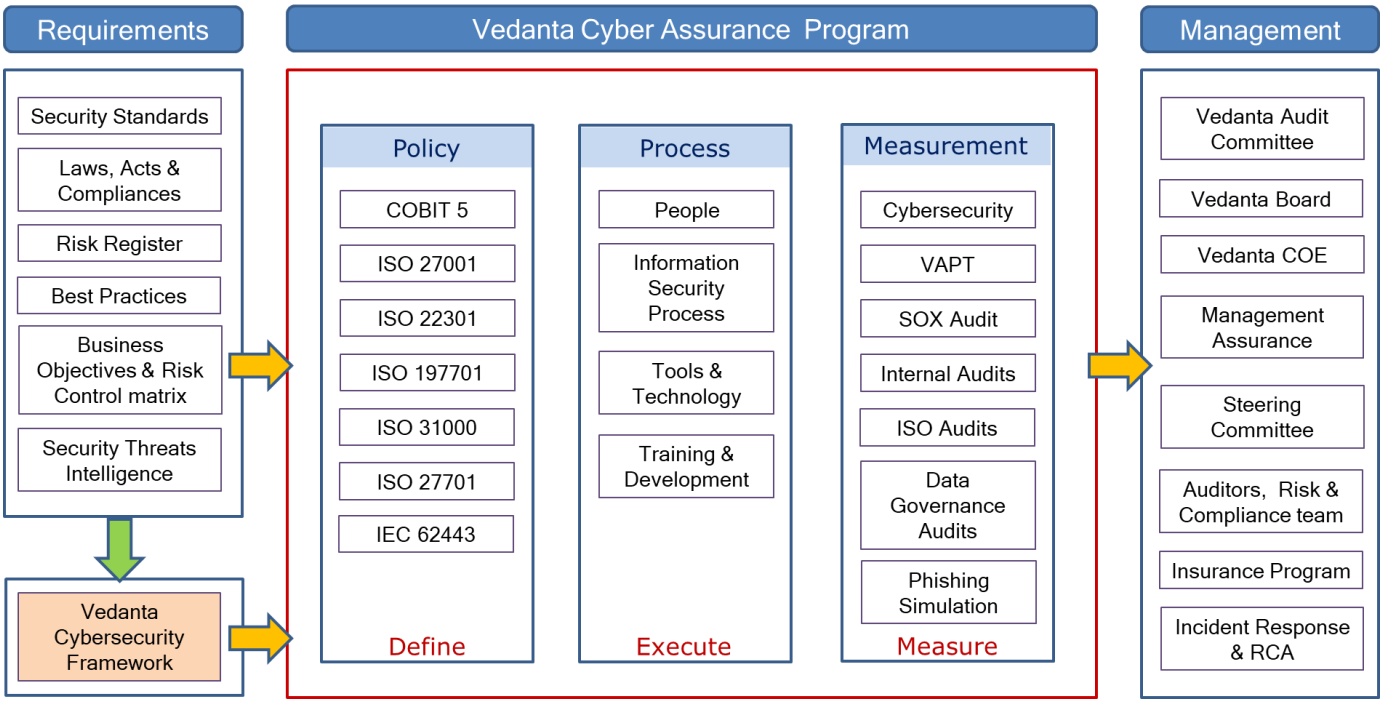
The Group Chief Information Officer (CIO) is responsible for setting up cybersecurity vision and strategy, defining cybersecurity governance framework, and executing programmes to ensure that confidentiality, integrity, and availability of all information assets are well protected. The CIO is accountable to Vedanta EXCO and Audit and Risk Committee of the Board for cybersecurity related matters.

The Group Chief Information Security Officer (CISO), reporting to Group CIO, with below mentioned responsibilities.

- Group CISO is responsible for operationally driving cybersecurity programmes to ensure that business objectives are achieved. The CISO is supported by the information technology (IT) team and our partner eco-system.
- Group CISO is responsible for establishing the data governance framework and drive data governance and privacy management throughout the data lifecycle.
- Group 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).
- Group CISO responsible for implementation of cybersecurity in OT system. OT cybersecurity consist of cybersecurity in SCADA/PLC, Industry 4.0 & Digitalization Initiatives and Laboratory Information Management Systems (LIMS).

The Group 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 Vedanta EXCO and works closely with group CIO/CISO.

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



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 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
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. Draft Digital Personal Data Protection Bill, 2022
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, 2017
16. Securities Contract (Regulation) Rules, 1957
17. Indian Companies Act, 2013
18. IEC 62443
19. Vedanta Information Security Standards
20. Data Governance Policy Framework
21. Social Media Policy
22. 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)
23. 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)

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

Standards and Certifications:

Business units of Vedanta are an ISO Certified Organizations and has established, implemented, maintains and continually improve the integrated management system (IMS) in accordance with the requirements of the International Standards ISO 27001, ISO 27701, ISO 22301, ISO 31000.

Below is the unit wise framework implementation & certification status.

S.No	BU / Group	ISO 27001 framework implement status	ISO 27001		ISO 22301 framework implement status	ISO 22301		ISO 31000 framework implement status	ISO 31000		ISO 27701 framework implement status	ISO 27701
			IT	OT		IT	OT		IT	OT		IT
1	Cairn	Yes	Yes	NO	Yes	NO	NO	Yes	NO	NO	Yes	NO
2	HZL	Yes	Yes	Yes	Yes	Yes	NO	Yes	Yes	NO	Yes	Yes
3	VZI	Yes	NO	NO	Yes	No	NO	Yes	NO	NO	NO	NO
4	BALCO	Yes	Yes	Yes	Yes	Yes	Yes	Yes	NO	NO	NO	NO
5	JSG	Yes	Yes	Yes	Yes	Yes	Yes	Yes	NO	NO	NO	NO
6	LAN	Yes	Yes	Yes	Yes	Yes	Yes	Yes	NO	NO	NO	NO
7	TSPL	Yes	Yes	NO	Yes	Yes	NO	Yes	NO	NO	NO	NO
8	ESL	Yes	Yes	NO	Yes	No	NO	Yes	NO	NO	NO	NO
9	IOB	Yes	Yes	NO	Yes	Yes	NO	Yes	Yes	NO	Yes	Yes
10	FACOR	Yes	Yes	NO	Yes	Yes	NO	Yes	Yes	NO	Yes	Yes

11	VGCB	Yes	Yes	NO	Yes	Yes	NO	Yes	Yes	NO	Yes	Yes
12	Nicomet	Yes	NO	NO	Yes	NO	NO	Yes	NO	NO	NO	NO
13	Sesa Coke	Yes	NO	NO	Yes	NO	NO	Yes	NO	NO	NO	NO
14	Gujrat NRE	Yes	NO	NO	Yes	NO	NO	Yes	NO	NO	NO	NO
15	Desai Cement	Yes	NO	NO	Yes	NO	NO	Yes	NO	NO	NO	NO
17	Sterlite Copper	Yes	Yes	Yes	Yes	NO	NO	Yes	NO	NO	Yes	NO
18	Fujairah Gold	Yes	No	No	Yes	NO	NO	Yes	NO	NO	NO	NO

Information Security Policies

Vedanta has robust information security policy & data governance policy and 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 framework.

All the policies and procedure enforced in the Vedanta environment is 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 are categorized under following areas:

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

Following is the applicable list of policies:

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

D. Information Security Operation

Information Security Operations at Vedanta consists of following processes:

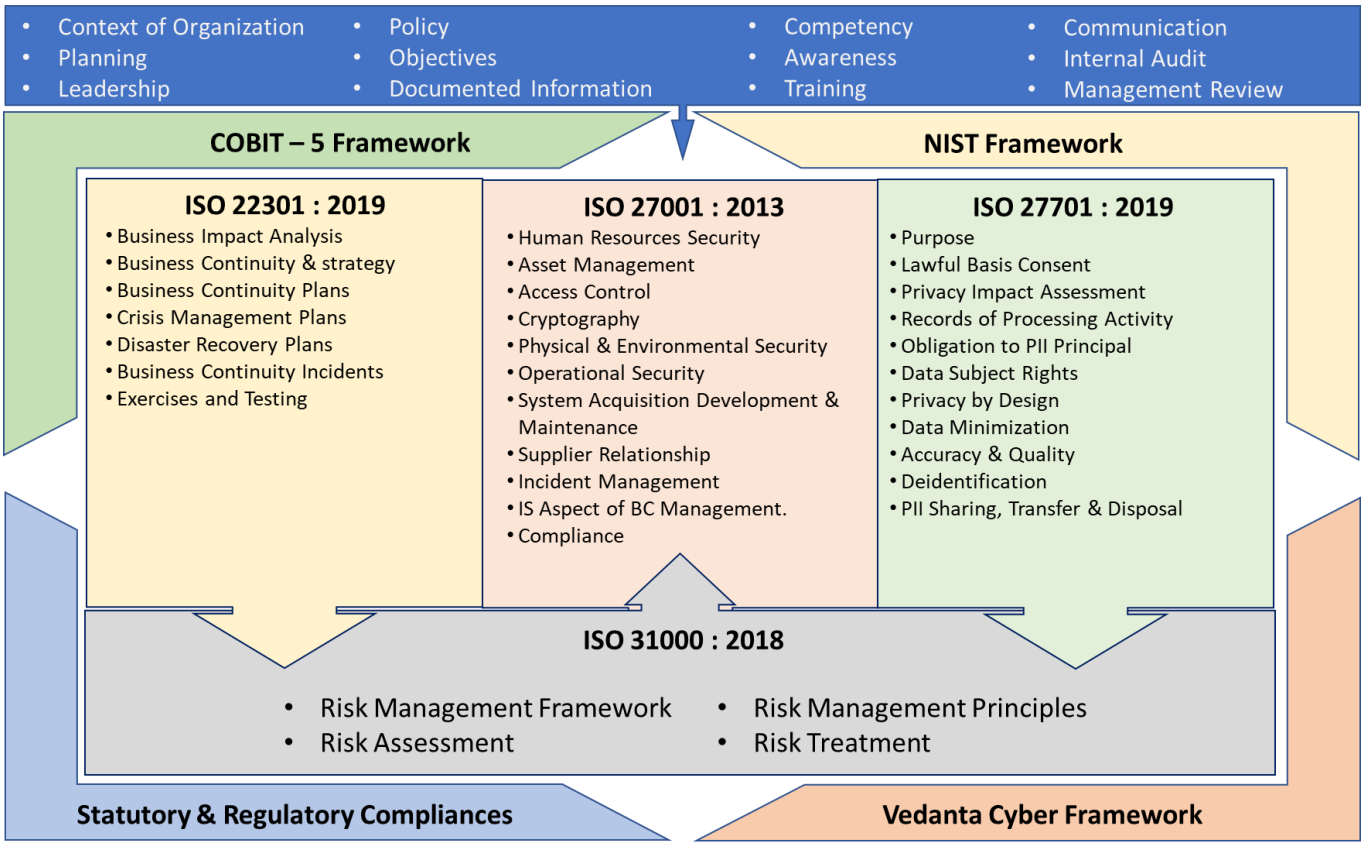
1. Risk Management
2. Vulnerability Management
3. Information Security Administration
4. Incident Management & Response (Cyber & Data Incidents)
5. Business Continuity & Disaster Recovery Plan (BCP/DR)

Risk Management

Risk management is a process of identification, evaluation, controlling and prioritization of risks and threats to an organization. These risks stem from a variety of sources, including financial uncertainties, legal liabilities, technology issues, strategic management errors, accidents, natural disasters etc.,

Vedanta has successfully implemented a robust risk management framework which helps our organization considering the full range of risks it faces. Business units of Vedanta are certified in ISO 31000:2018 Risk management which helps in improving decision making in the enterprise, align risk management potential impact on the enterprise and ensure that value is created by maintaining risk within acceptable tolerances and appetites. This also examines the relationship between risks and the cascading impact they could have on an organization's strategic goals.

Vedanta is a risk driven organization and detailed risk assessment is carried out across the organization, risks with required controls are mapped in risk control matrix. The below diagram depicts the overall alignment of Risk Management processes cutting across various domains of information technology.

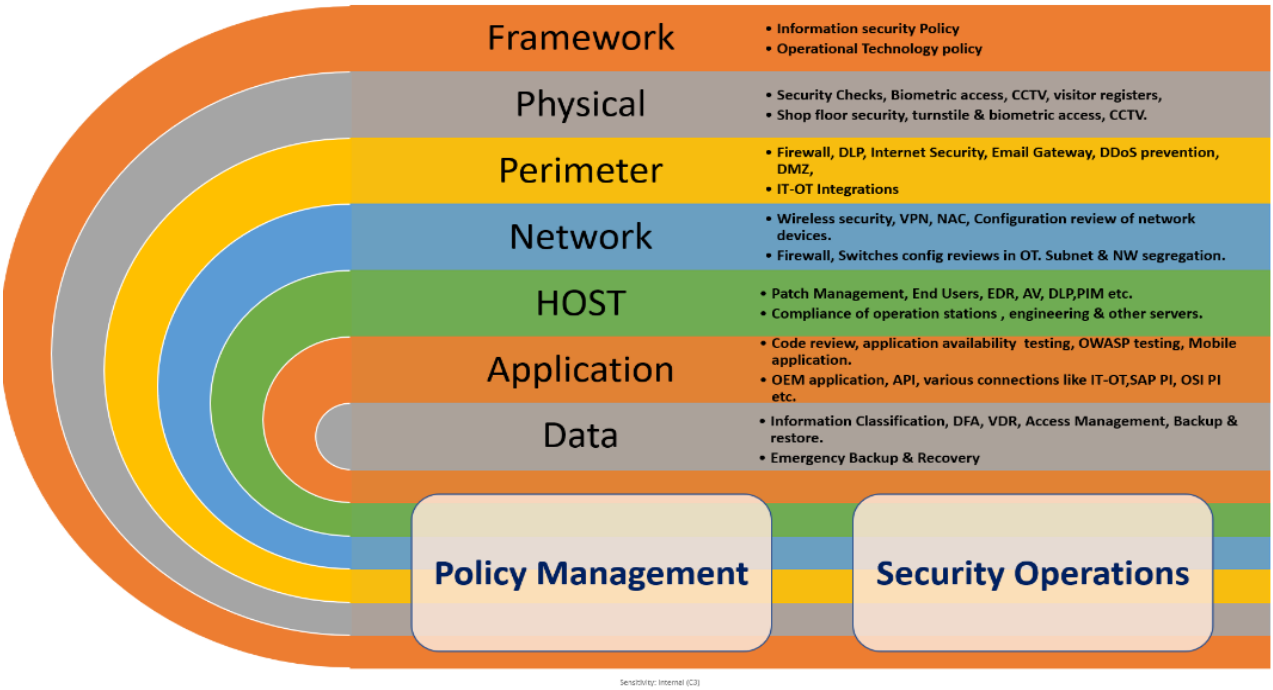


Vulnerability Management

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.

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 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 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
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.

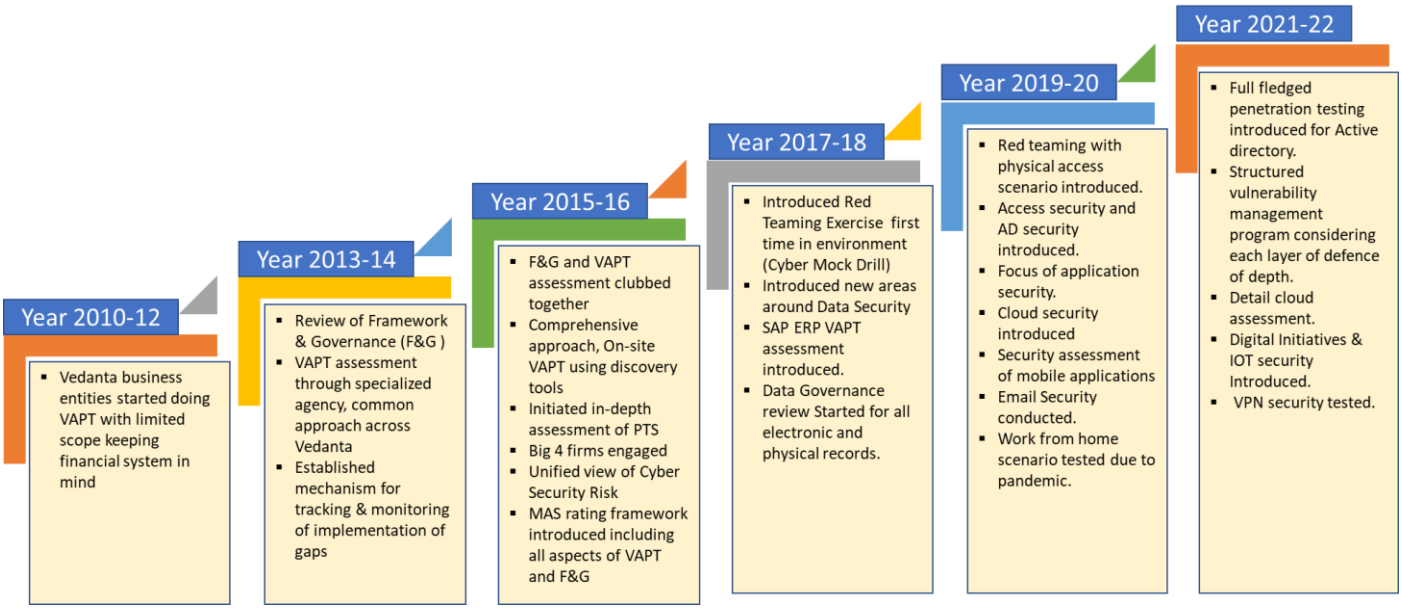
Vulnerability Assessment (VA) and Penetration Testing (PT) are carried out with combination of various automated tools and manual testing as appropriated. and risk ratings are arrived at using globally recognized standards and rating systems like OWASP (Open Web Application Security Project) and CVSS (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

Vedanta 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. Journey and coverage over the years are depicted below.



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 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 (Cyber & Data Incidents)

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.

Vedanta 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. Vedanta has well-defined Incident Management & Data Breach Policy which is circulated among all employees. This applies to all employees and business partners. Vedanta has set up a common e-mail id Vedanta.isms@vedanta.co.in 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.

Data Incident Management

Vedanta 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, Business Units of Vedanta 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. This DLP tools is implemented in a blocking mode.

A dedicated DLP Desk is also established to continuously detect, evaluate, and action data incidents as reported by DLP tool. Potential leakage is being 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.

Robust DLP rule sets have been created with help of business team based on Data Flow Analysis (DFA), Dedicated DLP desk exist for each BU, this DLP desk services are taken from expert agencies. Potential leakage incident being shared with line manager & after confirmation incident marked as confirmed leakage incident.

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

Consequence Management

Organization has a 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 a Zero Tolerance approach on breach of code of conduct.

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

Business Continuity & Disaster Recovery Plan (BCP/DR)

Vedanta recognizes that Business Continuity & Disaster Recovery is not only an IT subject, rather a business subject. Aligned to this thought, Business Units of Vedanta 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 BCP/DR. As part of this process, Vedanta 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.

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 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 CISO. These observations are subsequently deliberated with CIO and final observation tracker is prepared.

Observations reported as part of Information Security Administration are reviewed by CIO 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 CISO and are further reviewed by CIO.

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

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. Vedanta Group EXCO
II. Vedanta Audit & Risk Committee
III. Business Unit EXCO
IV. Business Unit 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 prepares 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.

Importance of Information Security Awareness Program:

Every organization needs protection against cyberattacks and security threats. Cybercrime and malware are constant threats to anyone with an Internet presence, and data breaches are time-consuming and expensive. An effective information security awareness program will help organization to mitigate digital information risks and keep systems running without disruption.

Security awareness training helps to minimize risk thus preventing the loss of PII, IP, money, or brand reputation. An effective awareness training program addresses the cybersecurity mistakes that employees may make when using email, the web and in the physical world such as tailgating or improper document disposal.

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. Vedanta 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. Vedanta conducts a Mandatory awareness training to all employees on annual basis.

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.

Phishing Simulations

Phishing is one of the common ways of social engineering and hence Vedanta has brought special focus on carrying out phishing simulations amongst its employees. This enables to teach employees how to detect and avoid phishing attacks in a safe environment.

Phishing simulations are carried for all 100% users to test the vigilance and awareness of the users. Vedanta carryout variety of simulations like General Phishing, Spear Phishing, Whaling, Smishing, Vishing. This is a quarterly activity with multiple templates. Learning from phishing simulation is shared to users. User falling prey to the simulation is also asked to undergo Phishing specific learning video as a training.

Information Security Awareness Calendar

Vedanta has created information security awareness calendar. As per published calendar Vedanta creates cyber & digital awareness among persons. Vedanta believes information should be behavioural subject and it should be practiced in day-to-day life. Information security awareness plan is created, and this plan further converted to calendar activities.

Information security awareness plan which includes Data Governance, Data Privacy & OT is given below:

S.No.	Item	Details		Frequency	Target Audience	Approach
1	Phishing Simulation	For All Employees	Phishing, E-mail	Half-Yearly	All Employees	To be launched twice a year to all employees, each time with different template.
		For Senior Management	Whaling, E-mail	Quarterly	Sr. Management	To be launched quarterly once to Senior Management with different templates and techniques.
		For Group of people or Function	Spear/Targeted Phishing, E-mail	Monthly	Specific Functions	To be launched monthly once to one of the targeted functions and their set of employees. Each time template will be different.
2	Video Learning	Theme Based Short Videos	12 Different Themes	Monthly	All Employees	Short Video of 2 to 3 minutes covering one of the 12 themes followed by 2 to 5 assessment questions.
3	Quizzes	Assessment Quiz	Based on Themes	Quarterly	All Employees	Quiz for assessment purpose in line with themes covered under Video Learning.

4	Training	Master e-Learning	Mandatory, Self-Service Video/Audio	Annually	All Employees	One Comprehensive Training Course to all Employees, proposed to be Mandatory.
		Virtual Class	Nomination, Virtual Meeting	Monthly	All Employees	To be arranged through HR. Employees can nominate/participate based on Interest.
		New Joiners	Onboarding, Virtual Meeting	Monthly	New Joiners Batch	Being done on monthly basis or as scheduled by HR function based on employee on-boarding schedule.
5	Recurring Communications	Tips & Tricks/Do's & Don'ts	E-mail	Monthly	All Employees	To be published through mail.
		Screen Saver	Based on Posters	Monthly	All Machines	Screen Saver created based on Posters. One each for 12 months.
		Physical Banners/Posters	Physical Posters	One Time	All Sites	4 different banners/poster for 12 different themes. To be published at all important location across sites.
		Management Communications	E-mail	Monthly	All Employees	Communication from 12 CXO/SBU Directors/Functional Heads
		Advisory & Knowledge Sharing	E-mail	Monthly	All Employees	Knowledge Propagation, Advisory circulated through mail.
6	Cyber Security Awareness Month	Celebration of Cyber Security Awareness Month in October 2022		One Time	All Employees	Special Campaign to be carried out
7	Privacy Day Celebrations	Celebration of Privacy Day 28th JAN.		One Time	All Employees	Special Campaign to be carried out

Capability Building

While Vedanta works with a philosophy of outsourcing majority of its Cyber Security services to reputed agencies, organization also invests in building internal capability for the employees who anchors Cyber Security program in conjunction with outsourced partners. To build such capabilities, members are periodically trained on various cyber security & data governance domains and are encouraged to formally get certified on applicable certificates and credentials.

G. Incidence Response & Emergency Preparedness Plan

Vedanta 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 each 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.

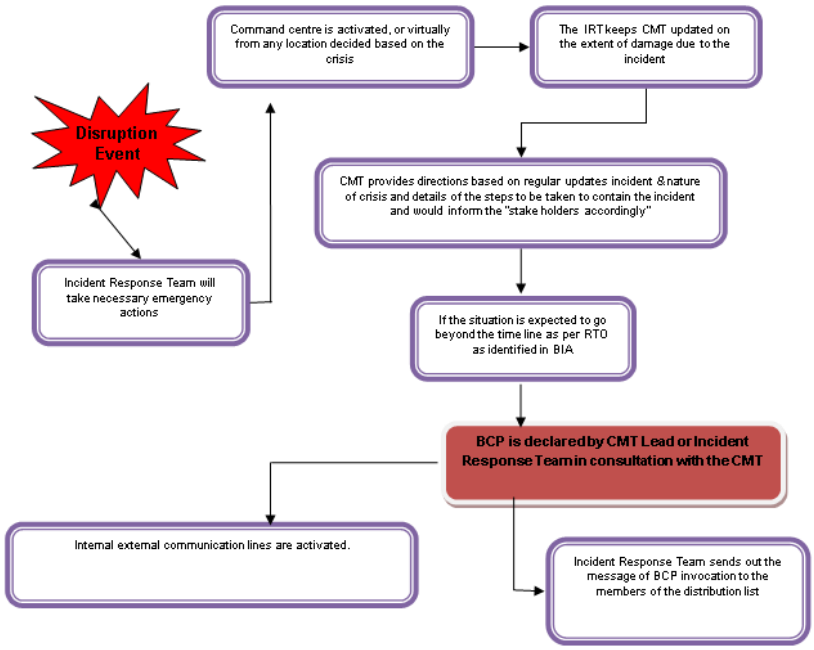
Below are the teams.

- Incident Repose Team
- Crises Management Team
- Business Continuity manager

- Communication management team

In case of any disruption, Incident Management Team would be the key person handling all incidents at the Vedanta and would coordinate with the staff members to handle crisis/incidents. Incident Response Team (IRT) will use the below specified workflow for resumption operations.

Crisis Incident Communication Workflow



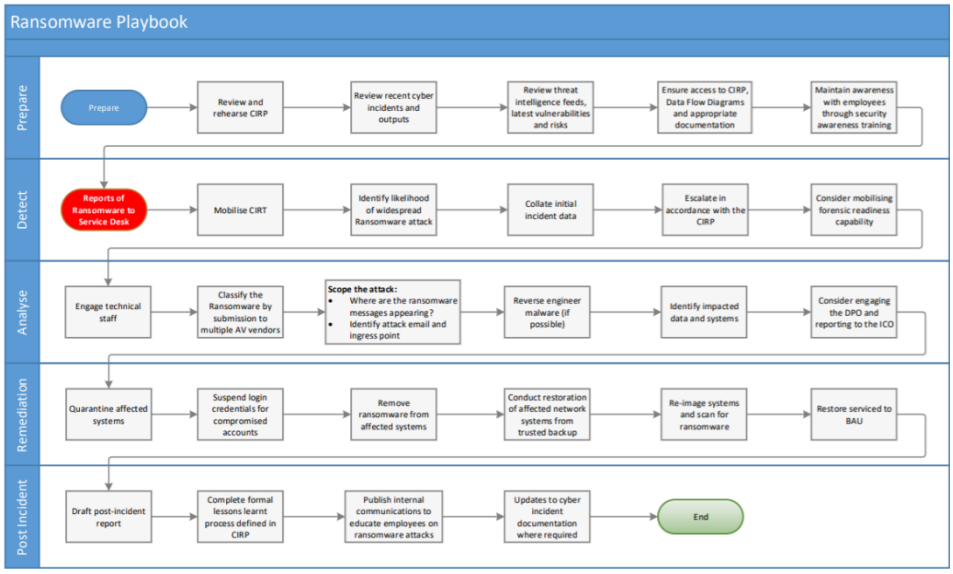
Ransomware Handling

Ransomware is a type of malware that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system so that it is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called crypto viral extortion. It encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them. A ransomware attack can result in a catastrophic data breach and disrupt business continuity.

Recognizing the criticality and impact such ransomware may create to the organization, Vedanta has defined a Ransomware Attack Handling Procedure in Vedanta Incident Crisis Management Plan.

Vedanta Data Protection Strategies are in place and follows complete Ransomware Protection 3-2-1-1-0 backup rule. We keep three copies of our critical business data—one primary and two backups—with two copies stored locally on two formats (network-attached storage, tape, or local drive) and one copy stored offsite in the cloud or secure storage and the entire backup should have 0 errors. Overall, this extended 3-2-1-1-0 rule offers two important things. It helps to protect our organisation from all potential attack vectors. And it ensures a fast and effective recovery process if an attack occurs.

Below is our Ransomware Playbook based on NIST framework:



H. Continual Improvement

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

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

Version Control	Issue & Effective Date	Description
1.0	22nd Feb 2022	Approach note document.
2.0	24th March 2023	Added awareness and calendar, Added Incident response.

Prepared by:-

Rahul Rathore

Mr. Rahul Rathore

Approved by:-

Chetan Trivedi

Mr Chetan Trivedi