

**Cyber Security Policy
VERSION 2.0
Dated: 25-October-2021**

Version	Date	Prepared by	Approved by
V1	25/10/2021		
V2			

CYBER SECURITY POLICY

1. Scope:

The scope of this Runaya Data Privacy policy document covers units and plants at the following entity locations:

1. Runaya Metsource Limited
2. Runaya Private Limited

2. Responsibilities

This policy shall be reviewed for updates by IT Head on an annual basis. Additionally, the data privacy policy shall be updated in-line with any major changes within the organization's operating environment or on recommendations provided by internal/external auditors.

3. Policy Compliance

Compliance to the cyber security policy shall be reviewed on an annual basis to ensure continuous compliance monitoring through the implementation of compliance measurements and periodic review processes. For proactive detection of data breaches, please refer breach management policy.

In cases where non-compliance is identified, IT Head shall review the reasons for such non-compliance along with a plan for remediation and report to Management. Depending on the conclusions of the review, need for a revision to the policy may be identified.

3. Cyber Security Principles

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, Runaya 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.

Information Security Planning

INFORMATION SECURITY MANAGEMENT FRAMEWORK

Under Enterprise Risk Management (ERM) framework, Runaya 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 Runaya Technology Landscape. Runaya 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. 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 Runaya 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

Runaya 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 Runaya Information Security Policy.

All the policies and procedure enforced in the Runaya 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 Runaya BUs are categorized under following areas:

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

INFORMATION SECURITY OPERATION

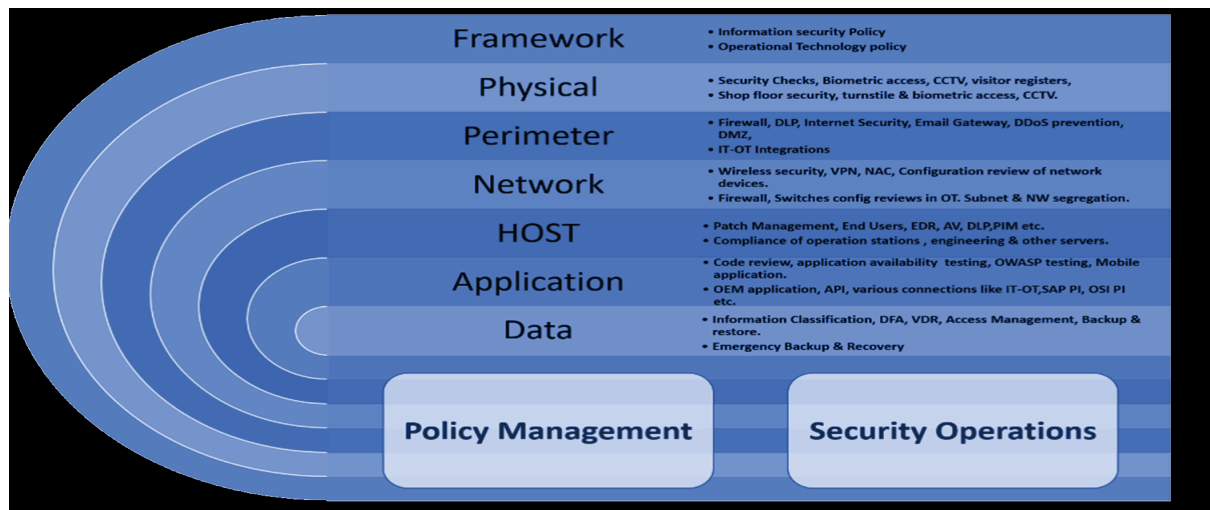
Information Security Operations at Runaya consists of following processes:

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

VULNERABILITY MANAGEMENT

Approach

Runaya has deployed a well-defined Vulnerability Management Program to identify and address risks and vulnerabilities across IT, OT and Digital Landscape of Runaya. This program is tailor-made to suit to Runaya 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 & unapproved 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. Runaya 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] Runaya Vulnerability Management Program is Data Centric, and objective is to identify risk in terms of Confidentiality, Integrity & Availability of Data. Privacy is also considered in Vulnerability Management Program.

Runaya 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. Runaya 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
2. Physical Security Review as part of Red Teaming Exercise
3. Vulnerability Assessment and Penetration Testing
 - Application Security (Including ERP)
 - OSDB
 - Networks
 - 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.

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 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. Runaya BUs has well-defined Incident Management & Data Breach Policy which is circulated among all employees. This applies to all employees and business partners. Runaya 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.

Runaya 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

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 noncompliance to the policy.

DISASTER RECOVERY AND BUSINESS CONTINUITY PLAN (DR/BCP)

Runaya recognizes that Disaster Recovery & Business Continuity is not only an IT subject, rather a business subject. Aligned to this thought, Runaya BUs has implemented ISO 22301 Disaster Recovery & Business Continuity Management Framework to prevent the interruption in operations of Runaya'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, Runaya 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.

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 Runaya’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 Runaya’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 CISO and are further reviewed by BU 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.

- 1. BU EXCO
- 2. Runaya Group EXCO
- 3. BU Audit & Risk Committee
- 4. Runaya Audit & Risk Committee

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

Responsible Use of Artificial Intelligence

Runaya recognises that Artificial Intelligence (“AI”), including Generative AI, Machine Learning models, automation tools, AI agents and analytics-based decision support systems, can create significant business value by improving productivity, operational efficiency, decision-making and innovation. At the same time, inappropriate or uncontrolled use of AI may create risks relating to data confidentiality, privacy, cyber

security, intellectual property, regulatory compliance, bias, accuracy, reputational impact and business continuity.

Accordingly, Runaya adopts a responsible, secure and risk-based approach to the use of AI across its businesses. The use of AI shall be aligned with the Company's Information Cyber Security Policy, Privacy Policy, Business Code of Conduct, applicable laws and other relevant internal policies.

Application of Policy

This section applies to all employees, directors, consultants, contractors, vendors, business partners and third parties who access, develop, deploy, integrate or use AI-enabled systems, tools or platforms on behalf of Runaya.

The policy shall apply to:

1. Use of publicly available or enterprise AI tools for business purposes.
2. Use of AI-enabled applications, software, platforms, chatbots, automation tools and analytics engines.
3. Development, procurement, testing or deployment of AI models or AI-based solutions.
4. Use of AI agents for performing tasks, generating content, processing data, supporting decision-making or automating workflows.
5. AI systems embedded within IT, OT, ERP, cyber security, finance, procurement, HR, manufacturing, sustainability or other business applications.

All AI usage for business purposes shall be undertaken only in accordance with approved procedures, access controls, data handling requirements and security protocols.

Understanding and Managing AI Use Risks

Runaya shall identify, assess and manage risks arising from the use of AI across its technology and business landscape. AI-related risks shall be considered as part of the broader Information Security, Data Governance and Enterprise Risk Management framework.

The following risk areas shall be considered while using, procuring or deploying AI systems:

1. **Data Confidentiality and Privacy Risk:** Sensitive, confidential, personal, proprietary or business-critical data shall not be entered into any AI tool unless such use is formally approved and appropriate safeguards are in place.
2. **Cyber Security Risk:** AI systems shall be assessed for vulnerabilities, unauthorised access, data leakage, prompt injection, malicious code generation, model manipulation and misuse.
3. **Accuracy and Reliability Risk:** Outputs generated by AI shall be reviewed and validated before being used for business decisions, external communication, reporting or operational execution.
4. **Bias and Ethical Risk:** AI systems shall be used in a fair, transparent and responsible manner, without discrimination or adverse impact on individuals, communities or stakeholders.
5. **Regulatory and Legal Risk:** AI usage shall comply with applicable data protection, cyber security, intellectual property, employment, sectoral and other regulatory requirements.

6. **Third-Party and Vendor Risk:** AI tools provided by external vendors shall be subject to due diligence, contractual safeguards, security assessments and ongoing monitoring, as applicable.
7. **Operational Risk:** AI shall not be used to automate critical business or operational decisions without appropriate human oversight, testing, approval and fallback mechanisms.

Where required, AI-related risks shall be recorded, tracked and mitigated through risk registers, control matrices, vulnerability assessments, incident management processes and management reviews.

AI Oversight and Governance

Runaya shall maintain appropriate oversight over the adoption and use of AI-enabled systems. The Information Security Function, in coordination with IT, Legal, Data Privacy, Risk Management and relevant Business Functions, shall be responsible for defining governance requirements for AI usage.

AI oversight shall include:

1. Approval of AI tools, AI agents and AI-enabled business applications before use.
2. Classification of AI use cases based on risk, sensitivity and business criticality.
3. Review of data types proposed to be used in AI systems.
4. Monitoring of access controls, user permissions and usage logs, wherever applicable.
5. Periodic review of AI-related risks, incidents and control effectiveness.
6. Employee awareness on responsible, secure and ethical use of AI.
7. Escalation of material AI-related risks or incidents to relevant governance forums.

Human accountability shall remain central to AI usage. AI-generated outputs shall not replace professional judgement, management responsibility, statutory accountability or approved business decision-making processes.

Prohibited Use of AI

Runaya prohibits the use of AI in any manner that may compromise information security, data privacy, legal compliance, ethical conduct or business integrity.

The following uses of AI are strictly prohibited:

1. Uploading or entering confidential, personal, sensitive, proprietary, financial, customer, employee, vendor, technical, plant, operational or cyber security-related information into unauthorised AI tools.
2. Using personal or publicly available AI accounts for official work where enterprise-approved alternatives are required.
3. Using AI to generate, test, modify or deploy malicious code, phishing content, credential theft techniques or cyberattack methods.
4. Using AI to bypass access controls, security systems, monitoring tools or internal approval processes.
5. Using AI-generated content for external disclosures, regulatory submissions, financial reporting, legal communication or public statements without appropriate review and approval.
6. Using AI to make employment, disciplinary, performance, compensation, safety, security or other high-impact decisions without authorised human review.
7. Using AI to impersonate employees, customers, vendors, regulators, management personnel or any other stakeholder.

8. Using AI in a manner that infringes intellectual property rights, confidentiality obligations, contractual commitments or applicable laws.
9. Using AI tools that have not been approved by Runaya for processing business data.
10. Using AI outputs without validation where such outputs may impact operations, safety, compliance, financial decisions or stakeholder interests.

Any suspected misuse of AI, unauthorised AI tool usage, data leakage, inaccurate AI output causing business impact or AI-related cyber incident shall be reported immediately through the defined incident reporting channels.

Use of Approved AI Agents

Runaya may permit the use of approved AI agents for specific business purposes, subject to defined security, privacy, access and governance controls. AI agents shall be deployed only after evaluation by the relevant IT, Information Security and Business teams. Approved AI agents may be used for activities such as workflow automation, knowledge assistance, document summarisation, data analysis, reporting support, process monitoring, cyber security support, helpdesk automation or other authorised business use cases.

The use of approved AI agents shall be governed by the following principles:

1. AI agents shall be used only for approved business purposes and within the scope for which they are authorised.
2. Access to AI agents shall be role-based and limited to authorised users.
3. AI agents shall process only approved categories of data, based on data classification and business need.
4. AI agent activity, where applicable, shall be logged, monitored and reviewed.
5. AI agents shall not independently execute critical actions without appropriate approval or human-in-the-loop controls.
6. AI agents integrated with enterprise systems shall follow secure configuration, identity management, authentication and access control requirements.
7. AI agents shall be periodically reviewed for performance, security, accuracy, relevance and continued business need.
8. Any change in the scope, functionality, integration or data access of an approved AI agent shall require reassessment and approval.

Runaya shall maintain an inventory of approved AI tools and AI agents, including their purpose, owner, risk classification, data access, approval status and review frequency. Use of AI tools or AI agents outside the approved inventory shall not be permitted for business purposes.

INFORMATION SECURITY AWARENESS AND CAPABILITY BUILDING

Runaya understands the fact that Human is the weakest link in establishing a cyber-resilient environment. As a result, Runaya 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. Runaya 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. Runaya intends to strengthen responsible AI awareness through targeted training on secure, ethical and approved use of AI tools.
- 9.. Surprise checks on compliance of Clear- Desk are carried out for end-user desks and observations are being shared to users.
10. 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.

CONTINUAL IMPROVEMENT

Runaya has adopted a process of continuously measuring effectiveness of security operations - technology, people and processes. Runaya 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 Runaya.