Document Reference:	ISMS	Effective Date:	13/04/2024
Document Name:	External Attack Surface Management	Expiry Date:	13/4/2025

External Attack Surface Management

SIT374 Team Project A

Redback Operations

Document Owner:	Daniel McAulay	Last Modified By:	Daniel McAulay
Next Review Date:	13/4/2025	Last Modified on:	13/04/2024

Version	Modified By	Approver	Date	Changes made
V0.2	Daniel McAulay	Daniel McAulay	13/04/2024	Document Creation

Contents

Purpose

The purpose of this policy is to define the framework and strategies Redback Operations will employ to identify, assess, and manage the risks associated with its external attack surface.

This policy aims to minimize the risk of cyber-attacks that could compromise the confidentiality, integrity, or availability of the company's assets and sensitive information. By proactively managing its external attack surface, Redback Operations seeks to safeguard its reputation, ensure business continuity, and comply with relevant regulations and standards.

This policy aims to achieve the following:

Ensure Comprehensive Risk Management

Systematically address vulnerabilities and threats that could compromise the integrity, confidentiality, and availability of the organization's information assets accessible from external networks.

Align with Business Objectives

Support Redback Operations' business objectives by ensuring that cybersecurity measures do not impede business agility and innovation, while still protecting the organization from external threats.

Compliance and Regulatory Adherence

Meet legal, regulatory, and contractual obligations related to cybersecurity, thus protecting Redback Operations from legal and compliance risks.

Promote a Mature Security Culture

Encourage a culture of security awareness and responsibility among all employees and stakeholders, making security a foundational aspect of all business operations and decision-making processes.

Scope

This policy applies to all employees, contractors, and third-party service providers of Redback Operations who interact with any external-facing IT assets, systems, networks, and applications. It covers all digital assets owned, operated, or managed by Redback Operations that can be accessed directly or indirectly from an external network. This includes any cloud/SaaS services exposed to the internet.

This policy is a component of the broader cyber security Information Security Management System (ISMS) of Redback Operations and interfaces with other policies on information security, incident response, and business continuity.

Digital Assets and Services

All external-facing IT assets, including but not limited to websites, web applications, email servers, DNS servers, cloud services, and any other digital services accessible over the internet.

Data Protection

The management and protection of data processed, stored, or transmitted through external-facing systems, ensuring its confidentiality, integrity, and availability.

Third-party Interactions

The relationships and interactions with third-party vendors, partners, and service providers who may have access to or manage parts of the external attack surface.

Regulatory and Compliance Frameworks

Adherence to applicable legal, regulatory, and industry standards affecting the management of the external attack surface, including but not limited to GDPR, HIPAA, PCI-DSS, and ISO/IEC 27001.

Criteria & Metrics for Policy Adherence

To ensure comprehensive coverage and consistent enforcement of the policy, specific criteria are defined to determine when and how the policy should be applied.

Accessibility from the Internet

Any asset that is directly accessible from the Internet, whether through a public IP address, a DNS entry, or an exposed API, must be included under the scope of this policy. This encompasses all web-facing applications, servers, and cloud-based resources that can be accessed or interacted with from outside the internal network.

Ownership or Operation by Redback Operations

All digital assets that are owned, operated, or managed by Redback Operations fall under this policy, regardless of their physical location or whether they are hosted on-premises or in cloud environments. This includes leased or rented digital resources and services contracted through third parties but managed directly by our team.

Potential for Compromise & Risk Impact

Assets that, if compromised, could lead to significant adverse effects such as unauthorized access, data breach, disruption of operations, or other critical security incidents need to be prioritized. The policy applies especially to assets containing sensitive information, critical operational technology, or those integral to business continuity.

Metrics for Monitoring Policy Adherence

- Coverage Ratio
    - Measures the percentage of total identified assets that are covered by the policy's security measures.
- Compliance Rate
    - Tracks the adherence to security practices and controls as outlined in the policy across all applicable assets.
- Incident Response Effectiveness
    - Assesses the timeliness and effectiveness of the response to security incidents involving external-facing assets.

Application of the Policy

The application of these criteria ensures that the External Attack Surface Management Policy is consistently applied across all relevant assets, providing a clear framework for identifying which assets need to be secured and monitored. By adhering to these guidelines, Redback Operations aims to maintain a strong defensive posture against external threats and ensure the resilience and security of its operational and informational assets.

Framework References

The External Attack Surface Management Policy references the following framework controls:

ISO 27001 Controls

A.5.23: Management of Information Security Incidents and Improvements

A.5.7: Management of Technical Vulnerabilities

A.8.15: Network Security

A.8.23: Configuration Management

CIS Controls

Control 1: Inventory and Control of Enterprise Assets

Control 2: Inventory and Control of Software Assets

Control 4: Secure Configuration of Enterprise Assets and Software

Control 9: Data Protection

Control 11: Network Infrastructure Management

Control 12: Endpoint Security

Control 18: Penetration Testing

Roles and Responsibilities

CISO (Chief Information Security Officer)

- Policy Oversight
    - Ensures the External Attack Surface Management Policy aligns with Redback Operations' overall security strategy and business objectives.
- Risk Management
    - Oversees the identification, assessment, and mitigation strategies for risks associated with the external attack surface.
- Compliance and Reporting
    - Ensures compliance with relevant laws, regulations, and standards.
    - Reports on security posture and risk management effectiveness to executive management.

IT Department

- Asset Management & Inventory
    - Maintains an up-to-date inventory of all external-facing assets, including hardware and software components.
- Network Security
    - Implements and manages firewalls, VPNs, and other network security measures to protect the external attack surface.
- Patch Management
    - Regularly updates and patches systems and applications to address security vulnerabilities.
- Systems Administration
    - Provides information technology support & operational technology support (I.T. & O.T.)

Security Team

- Vulnerability Assessment and Penetration Testing (VAPT)
    - Conducts regular vulnerability assessments and penetration testing on external-facing assets to identify and remediate security weaknesses.
- Incident Response
    - Leads the response to security incidents affecting the external attack surface, including investigation, containment, eradication, and recovery.
    - Monitors external-facing assets for suspicious activity or breaches using SIEM, IDS/IPS, and other security tools.

Developers

- Code Reviews, Security Collaboration and Security Testing
    - Participates in code reviews and incorporates security testing (e.g., static, and dynamic analysis) as part of the development lifecycle.
    - Works closely with the security team to address security issues identified in applications and implements security features and controls as advised.
    - Adheres to secure coding standards and practices to minimize vulnerabilities in web applications and services.

RACI Chart

A RACI chart is a management tool that outlines the roles and responsibilities of different team members for specific tasks or processes. The chart helps clarify expectations, improves communication, and ensures that all tasks have clear ownership, making it easier to manage projects and processes efficiently.

Legend:

R (Responsible):

Person or group who performs the activity.

A (Accountable):

Person who is ultimately accountable.

C (Consulted):

Person or group that provides information and/or expertise.

I (Informed):

Person or group that needs to be informed after the decision or action is taken.

Activity/Role	CISO	IT Department	Security Team	Developers
Asset Discovery & Inventory	I	RA	RC	I
Risk Identification	A	C	RA	I
Risk Analysis	A	C	RA	I
Risk Prioritization	A	C	RC	I
Risk Mitigation	A	R	RA	R
Risk Remediation	A	R	RA	R
Implementing Security Controls	AC	RA	RA	R
Policy Management	R	C	RA	C
Vulnerability Assessment (VAPT)	C	C	RA	I
Incident Response	A	R	RA	I
Secure Coding	A	I	A	RA
Security Strategy	RA	C	RC	I

External Attack Surface Components

To effectively manage and protect Redback Operations' external attack surface, a comprehensive identification of all external-facing components is mandatory. The external attack surface of Redback Operations encompasses all digital assets, systems, and services accessible from outside the organization's internal network.

These components can be broadly categorized into several key areas, each with technical examples.

Types of Digital Assets

The types of digital assets this policy refers to may include:

Web-facing Applications and Services

- Public Websites, Gateways and Portals
    - Main websites, customer portals, and blogs hosted on domains owned by Redback Operations.
- Web Applications
    - Online applications offering services or interactions to users, such as:
        - Web-based email systems
        - CRM platforms
        - Custom business applications
        - Application Programming Interface (API's)

Network Infrastructure

- DNS Servers
    - Servers responsible for resolving domain names into IP addresses for the organization.
- Firewalls and Edge Devices
    - Devices positioned at the boundary of the network to protect internal networks from external threats.
    - Example: Next-generation firewalls (NGFWs) that include intrusion prevention systems (IPS).
- VPN/Remote Access Gateways
    - Endpoints for VPN access that allow remote users to connect securely to the internal network.
        - Example: SSL VPN appliances for secure remote access.

Cloud Services and Infrastructure

- Cloud-based Web Hosting
    - Services used for hosting websites and web applications on cloud platforms.
- Cloud Storage
    - Publicly accessible cloud storage buckets or containers. Example: Microsoft Azure Storage accounts
- IaaS, PaaS & SaaS Services
    - Cloud-based applications accessed by users over the Internet.
        - Example: Salesforce CRM, Google Workspace.

Email and Communication Servers

- Email Servers
    - Servers handling incoming and outgoing email communications.
    - Example: SMTP, IMAP, and POP3 servers accessible from the internet for email exchange.
- Unified Communications Systems
    - Systems that provide communications services such as VoIP, video conferencing, and instant messaging.
    - Example: Microsoft Teams or Zoom servers configured for external access.

Remote Access Services

- Remote Desktop Services
    - Services allowing remote control of desktops or servers within the organization's network. Example: Remote Desktop Protocol (RDP) endpoints.
- Network Management Systems
    - Tools and systems used for managing and monitoring the network infrastructure, which might be accessible from the internet for remote management purposes.
    - Example: SNMP (Simple Network Management Protocol) interfaces on network devices.
- Privileged Access Management Platform
    - Platform/solution utilized for managing service and application identities and facilitating privileged access for sensitive/protected systems.

Identifying these components involves a detailed inventory and regular audits to ensure that all external-facing assets are known, managed, and secured. This includes not only the direct exposure of services to the internet but also indirect exposures through third-party services and integrations that might provide pathways into the organization’s network.

Methodology

Asset discovery is a critical first step in managing Redback Operations' external attack surface effectively. It involves identifying all assets that are part of or can interact with the external digital environment. These assets include, but are not limited to, web servers, domain names, DNS servers, external IP addresses, cloud services, and third-party services.

A comprehensive asset discovery process ensures that all components exposed to potential external threats are accounted for, monitored, and protected.

Asset Discovery

This Asset Discovery methodology is integral to our External Attack Surface Management Policy, enabling Redback Operations to systematically identify, monitor, and secure our digital assets against external threats. Through this comprehensive approach, we bolster our defence mechanisms, enhancing our cybersecurity posture and protecting company assets.

Automated Scanning and Enumeration

Automated scanning techniques form the backbone of our Asset Discovery process. While there is no mandatory requirement to use specific tooling, provided in this section of the report is a typical penetration testing methodology used for enumeration & discovery of attack surface and vulnerabilities.

This involves deploying systematic approaches to uncover and catalogue all internet-facing assets:

Port & Service Scanning

Nmap (Network Mapper) is a powerful tool often used for network discovery and security auditing. In port scanning, Nmap is utilized to scan target IP addresses to identify open ports and associated services, providing insights into potential entry points for security threats.

Network Mapping

Zenmap is the official graphical user interface (GUI) for Nmap, which facilitates easier visualization of network mapping. It helps in plotting the network structure, showing all the connected devices and the relationships between them, crucial for spotting potential vulnerabilities.

Vulnerability Scanning

Nessus vulnerability scanning is known for its comprehensive detection capabilities. It automatically scans systems, networks, and applications to identify vulnerabilities, including misconfigurations and outdated software prone to exploits.

Banner Grabbing

Netcat is a versatile networking tool used for reading from and writing to network connections using TCP or UDP. It is particularly effective for banner grabbing, where it can retrieve details about software running on an open port, aiding in the identification of out-of-date systems or applications.

Web Application Scanning

The OWASP Zed Attack Proxy (ZAP) is an open-source web application security scanner. It automatically finds security vulnerabilities in web applications while they are running, making it a valuable tool for organizations to secure their web-based services and platforms.

DNS Enumeration

DNSEnum is a script that combines the power of multiple DNS enumeration techniques. It uses DNS diagnostics and records to extract valuable information about domain-related entries, providing insights into potentially misconfigured domains and subdomains.

API Endpoint Discovery

Postman is extremely useful for API endpoint discovery and testing. By analysing API traffic and responses, security teams can identify undocumented or loosely secured API endpoints that might be vulnerable to attacks.

Cloud Asset Identification

Given the extensive use of cloud services, identifying assets deployed in cloud environments is critical. This step ensures a comprehensive view of our external attack surface.

Cloud-native Discovery Tools

Leveraging tools provided by cloud service providers to enumerate and manage resources. This includes inventorying all assets deployed, from virtual machines to storage accounts, across our cloud environments.

Example of native tools utilized include:

- Microsoft Defender for Cloud
- Azure Security Centre
- Azure Resource Manager.
- Google Cloud Resource Manager
- Google Cloud Asset Inventory
- Google Cloud Security Command Centre

Manual Verification, Auditing & Continuous Discovery

To complement automated discovery processes, manual verification by security teams ensures the accuracy and completeness of our asset inventory.

As part of Redback Operations' comprehensive External Attack Surface Management Policy, manual verification and auditing are crucial for ensuring the accuracy and effectiveness of our security measures. Here are the key manual techniques included in the policy:

Audit and Verification

Engage in manual checks and reviews to validate the findings from automated scans and enumerations, ensuring no asset is overlooked and all information is up to date.

Physical Network Inspections

To validate the accuracy of automated scanning results, physical inspections of network hardware and configurations are conducted. This includes verifying the settings on routers, switches, and servers to ensure compliance with our security standards.

Firewall and Network Configuration Reviews

Administrators are required to manually review firewall and network device configurations regularly. This involves accessing devices through secure interfaces like PuTTY or SecureCRT to check for proper rule enforcement and to ensure that only necessary ports and services are exposed.

Penetration Testing

Our policy mandates regular manual penetration testing to simulate potential security breaches. This testing is performed by qualified personnel using specialized tools such as Metasploit and Burp Suite from the Kali Linux distribution, providing a real-world assessment of our defences.

Code Review and Security Audits

Developers must conduct thorough manual reviews of code, particularly for web applications and services that are part of our external attack surface. This process helps identify and rectify security vulnerabilities that automated tools may miss.

Policy Compliance Reviews

Regular reviews of security policies and practices are required to ensure ongoing compliance with legal and regulatory standards. This manual review ensures that all operational practices are up-to-date and effective in mitigating security risks.

Integration with Centralized Asset Management

In the context of Redback Operations' External Attack Surface Management Policy, the integration of asset discovery and monitoring data into a centralized asset management system is critical for ongoing monitoring and discovery of company assets.

This process ensures that all information regarding external-facing assets is accurately maintained and readily accessible, enhancing our security posture. Here are the key aspects of this integration process included in our policy:

Note: This section refers to a theoretical high-level design that is not yet implemented due to missing tooling and infrastructure. No centralized asset management system exists currently.

Centralized Inventory Updates

Automated and manually verified asset discovery results are systematically fed into a centralized asset management system. This ensures that our asset inventory is comprehensive and up to date, providing a single source of truth for all asset-related information.

Continuous Synchronization

Our policy requires continuous synchronization between asset discovery tools and the centralized asset management system. Any changes detected in the external attack surface, such as the addition of new assets or modification of existing ones, are automatically updated to maintain current asset records.

Security Data Integration

Security configurations, vulnerability data, and compliance statuses are integrated into the centralized system. This provides a holistic view of each asset's security posture, facilitating more effective risk assessment and management.

Access Control and Accountability

Strict access controls are enforced to ensure that only authorized personnel can view or modify asset information. Audit logs are maintained to track changes, providing accountability, and aiding in forensic investigations if needed.

Automated Reporting

The centralized asset management system generates automated reports that provide insights into the status, vulnerabilities, and compliance of all external-facing assets. These reports are crucial for ongoing security assessments and decision-making processes.

Continuous Discovery:

Asset discovery is not a one-time activity but an ongoing process. As Redback Operations evolves, new assets will be created, and existing assets may change or be decommissioned. Continuous discovery ensures that the organization's external attack surface is accurately represented in real-time, allowing for proactive security management.

To address gaps and unregistered/rogue assets, the techniques listed in this policy's *Methodology* section are to be used during annual reviews to ensure maximum policy coverage and adherence across Redback Operations' systems & infrastructure.

By adhering to this methodology, Redback Operations can ensure a thorough and effective asset discovery process, laying the groundwork for comprehensive external attack surface management. This proactive approach enables the organization to identify, assess, and manage risks associated with each external asset, enhancing the overall security posture and resilience against cyber threats.

Risk Management

Risk Management in the context of the External Attack Surface Management Policy involves a systematic process to identify, analyse, prioritize, mitigate, and remediate risks associated with external digital assets. This ensures continuous protection against vulnerabilities and external threats, while reducing the overall external attack surface and maximizing coverage of IT Systems & Infrastructure.

Note: This section of the External ASM Policy adheres to Redback Operations' ISMS Risk Management Framework & Security Compliance Frameworks. Refer to the relevant policy for further details regarding Risk Management.

Risk Identification

Overview
The initial phase in the risk management process where potential security risks associated with external-facing assets are detected and documented.

Purpose
To uncover all possible sources of security threats so that they can be thoroughly analysed and addressed in subsequent steps.

Risk Identification involves:

- Automated Vulnerability Scanning & Discovery
    - Deploy continuous scanning mechanisms to identify vulnerabilities in real-time across all external-facing assets.
    - This includes detecting outdated software, misconfigurations, and known security flaws.
- Threat Intelligence Integration
    - Utilize advanced threat intelligence platforms to gather and analyse data on new and emerging threats that could potentially affect our external systems.
- Targeted Penetration Testing
    - Schedule and execute regular and targeted penetration tests to simulate attacks on external-facing assets and identify exploitable vulnerabilities.

Risk Analysis

Overview
This stage involves a deeper examination of the identified risks to understand their nature, potential impacts, and the likelihood of occurrence.

Purpose
To quantify and qualify risks, enabling focused and prioritized risk management efforts based on potential impacts to the organization.

Risk Analysis Involves:

Impact Analysis
Conduct a detailed analysis of the potential impacts of identified risks, considering factors such as the sensitivity of data exposed, potential operational disruptions, financial implications, and reputational damage.

Likelihood Assessment
Evaluate the probability of each risk occurring based on existing security controls, historical data, and current threat landscape insights.

Risk Prioritization

Overview
Following analysis, risks are prioritized based on their potential impact and probability, ensuring that resources are allocated efficiently to address the most significant threats.

Purpose
To strategically manage response efforts by prioritizing risks that pose the greatest threat to the organization's security and operational stability.

Risk Prioritization Involves:

Risk Scoring and Matrix
Implement a quantitative & qualitative scoring system to prioritize risks based on their severity and likelihood. Use a risk matrix to visually categorize and prioritize risks, aiding in effective resource allocation.

Regulatory Impact Consideration
Regularly review and align risk prioritization with compliance and regulatory requirements, ensuring that risks with legal implications are promptly and adequately addressed.

Risk Mitigation

Overview
Actions and strategies are implemented to reduce the severity or likelihood of prioritized risks, or to shield the organization from their impact.

Purpose
To deploy effective control measures that prevent, reduce, or transfer risks, thereby enhancing the security of external-facing assets.

Risk Mitigation Involves:

Implementation of Security Controls
Based on the risk assessment outcomes, appropriate security controls are selected and implemented. These may include technical controls (such as firewalls, intrusion detection systems, and encryption), administrative controls (such as security policies and training), and physical controls (such as access control systems and surveillance).

Regular Updates and Patch Management
Ensuring that all software and systems are kept up to date with the latest security patches is crucial. A structured patch management process is maintained to quickly apply patches to vulnerable systems, reducing the window of opportunity for attackers.

Enhancing Security Architectures
Continuous improvement of security architectures is essential for defending against sophisticated threats. This may involve segregating networks, strengthening endpoints, and implementing advanced threat detection technologies.

Configuration Management
Proper configuration of IT systems and applications is vital to eliminating unnecessary vulnerabilities. Standardized configurations that adhere to industry best practices are developed and implemented, and continuous configuration monitoring is conducted to ensure compliance.

Training and Awareness Programs
Employees are regularly trained on security best practices and the specific tactics, techniques, and procedures used by threat actors. This training includes how to recognize phishing attempts, the importance of using strong passwords, and the safe handling of data.

Redundancy and Failover Processes
To ensure availability and continuity of operations, redundancy is built into critical systems and networks. Failover processes are established to switch to backup systems automatically in the event of a system failure or breach.

Risk Remediation

Overview
The process of applying specific solutions or changes to fully resolve vulnerabilities or eliminate risks.

Purpose
To ensure that once risks are identified and assessed, they are effectively neutralized or managed to acceptable levels.

Risk Remediation Involves:

Immediate Containment
When a critical vulnerability is identified, immediate steps are taken to contain its potential impact. This may involve temporary fixes or workarounds that prevent the exploitation of the vulnerability while a permanent solution is being developed.

Developing Remediation Plans
For each identified risk, a tailored remediation plan is developed. This plan outlines the steps required to address the vulnerability, assigns responsibilities to specific teams or individuals, and sets deadlines for resolving the issues.

Implementing Changes
Depending on the nature of the risk, remediation may involve software updates, changes to system configurations, enhancements to security policies, or physical security improvements. Each action is carefully implemented to ensure that it effectively resolves the identified risks without introducing new vulnerabilities.

Testing and Validation
After remedial actions are implemented, they are thoroughly tested to confirm that the risk has been effectively mitigated. This testing may involve repeat scans, penetration tests, or other assessment methods to ensure that the vulnerability no longer poses a threat.

Documentation
Comprehensive documentation of the remediation process is maintained, including details of the vulnerability, the analysis performed, the remediation steps taken, and the results of post-remediation testing.

Feedback and Improvement
The effectiveness of the remediation process is reviewed, and feedback is gathered to improve future risk remediation efforts. Lessons learned are integrated into the organization's risk management practices to enhance overall security posture.

Documentation and Reporting

Overview
Essential for maintaining records of risk management activities, decisions, and outcomes, and for communicating the ongoing status of risk to relevant stakeholders.

Purpose
To provide transparency, support compliance, and facilitate informed decision-making by keeping comprehensive records and reporting on risk management performance.

Risk Remediation Involves:

Dynamic Risk Register
Maintain an up-to-date risk register that records all identified risks, their severity, mitigation actions, and resolution status. This register serves as a central repository for tracking and managing risks across the organization.

Regular Risk Reporting
Generate and disseminate regular risk reports to senior management and relevant stakeholders. These reports should highlight current risk levels, mitigation efforts, and any changes in the risk landscape.

With a structured approach to risk assessment and management, Redback Operations can effectively minimize vulnerabilities and threats to its external attack surface. The next step in developing the policy involves outlining the roles and responsibilities of individuals and departments within the organization.

Established Security Controls

To safeguard its external attack surface, Redback Operations will implement a comprehensive set of security measures and controls. These controls are designed to protect against unauthorized access, data breaches, and other cyber threats.

Note: This section refers to adherence to the ISMS in reference to established security frameworks, such as Essential 8, CIS Security Controls or ISO27001. Refer to the relevant ISMS policy for further details.

Technical Controls

Firewalls and Intrusion Prevention Systems (IPS)
Advanced firewall technologies are utilized, such as IPS to monitor, control, and block malicious traffic based on dynamic rule sets.

Ports & Services are restricted on Gateway devices to allow external access from public sources unless required for functionality purposes.

Vulnerability Management
Regularly scheduled vulnerability scans and automated discovery tooling is used for continuous threat detection and response.

Encryption
End-to-end encryption protocols are implemented for all data in transit and at rest, using industry-standard algorithms to ensure data confidentiality and integrity.

Access Control
Access control systems are implemented, incorporating multi-factor authentication (MFA) and role-based access controls (RBAC) to regulate access to sensitive information and systems.

Web Application Firewalls (WAF)
WAF's are deployed to protect against web-based attacks by filtering and monitoring web traffic.

Secure Software Development Life Cycle (SDLC)
Secure coding principles are implemented at every phase of the software development process to identify and mitigate vulnerabilities early during development.

Network Segmentation
Networks are divided into subnetworks to limit an attacker's ability to move laterally within the network and to contain potential breaches.

Security Information and Event Management (SIEM)
SIEM systems provide real-time analysis of security alerts generated by network hardware and applications.

Administrative Controls

Security Policies and Procedures
Comprehensive security policies and procedures addressing all aspects of organizational security are regularly updated and enforced.

Risk Management
A formalized risk management framework is established to systematically identify, assess, mitigate, and monitor organizational risks.

Security Training and Awareness
Regular training sessions and continuous awareness programs educate employees on security best practices and threat awareness.

Incident Response Plan
A detailed incident response plan is maintained, outlining roles, responsibilities, and procedures for managing and recovering from security incidents.

Data Protection Policies
Policies focused on data protection, including data retention, data destruction, and data leakage prevention, are implemented, and adhered to.

Third-Party Risk Management
Security risks associated with third-party vendors and service providers are assessed and managed through regular audits and compliance checks.

Physical Controls

Secure Data Centres
Advanced physical security measures such as biometric access controls, CCTV surveillance, and security patrols protect physical data centres and server rooms.

Visitor Access Controls
Strict access protocols for visitors are enforced, including escorted access, visitor logs, and time-limited access badges.

Physical Device Security
Cable locks, secure enclosures, and other physical restraints are used to prevent unauthorized removal of devices.