



Information Security

Zayo maintains a comprehensive Security Policy that establishes the foundation for protecting its information assets, technology infrastructure, business operations, and customer information. The policy defines enterprise-wide security expectations designed to preserve the confidentiality, integrity, and availability of information and services while addressing applicable business, contractual, legal, and regulatory requirements.

Zayo's security program incorporates risk management, governance and accountability, access control, data protection, network security, physical security, supplier oversight, incident management, and operational resilience. These areas are supported by documented standards establishing specific control requirements and responsibilities across the organization.

The program incorporates ongoing oversight, risk assessment, compliance monitoring, security awareness, and continuous improvement. Defined governance and exception management processes help ensure security decisions are documented, reviewed, and appropriately authorized. Together, these requirements establish a consistent, risk-based approach to protecting the systems and information supporting Zayo's services and customers.

Security accountability and responsibility

The Organization's security governance structure establishes accountability for protecting organizational and customer information across executive leadership, security teams, technology functions, business owners, personnel, and applicable suppliers.

Executive leadership provides direction and oversight of the security program, including consideration of material security risks, business priorities, and resource requirements. Designated security leadership is responsible for establishing and maintaining the enterprise security program, while business and technical control owners are accountable for implementing and maintaining controls within their areas of responsibility.

Zayo's documented requirements establish ownership, decision-making authority, approval responsibilities, escalation processes, and expectations for compliance with security policies and standards. Governance activities include security risk management, monitoring, reporting, corrective action, and periodic review of control requirements. Personnel are also expected to understand their security responsibilities, complete applicable training, and report suspected security incidents or weaknesses. This shared accountability model is designed to ensure security responsibilities remain clearly defined and integrated into business operations.



Acceptable Use Standards

The Organization establishes acceptable use requirements to promote the secure, responsible, and authorized use of company information, technology assets, communications systems, applications, and network resources.

Personnel are required to use organizational resources in accordance with approved business purposes, applicable security policies, and established access permissions. Requirements address the protection of authentication credentials, appropriate handling of sensitive information, authorized use of applications and technology services, and the prevention of activities that could introduce security risks or disrupt business operations.

Zayo also sets expectations for protecting company-managed devices, using approved systems and services, and reporting suspected misuse or security concerns. Unauthorized access, unapproved technology usage, circumvention of security controls, and inappropriate disclosure of organizational or customer information are subject to organizational restrictions. Acceptable use expectations are reinforced through personnel security responsibilities, training, and applicable compliance measures, helping establish consistent security-conscious behavior across the workforce.



Security Compliance

Zayo's compliance management framework is designed to support adherence to applicable legal, regulatory, contractual, customer, and organizational security requirements. Compliance is integrated into Zayo's broader information security governance and risk management program to promote accountability, effective oversight, and consistent application of security and compliance controls across business operations.

A central component of Zayo's compliance program is its Common Controls Framework (CCF), which provides a unified approach to managing security and compliance requirements across applicable regulations, industry standards, contractual commitments, and recognized security frameworks. The CCF consolidates overlapping requirements into common control objectives, supporting consistent control implementation while reducing duplication across multiple compliance obligations. Documented mappings maintain traceability between authoritative requirements, control objectives, supporting policies and standards, and accountable control owners. This structure supports efficient compliance assessments, audit readiness, identification of control gaps, and ongoing alignment with evolving regulatory and business requirements.

Zayo's compliance program incorporates periodic internal assessments, risk-based audits, independent reviews, control monitoring, and documented evidence requirements to evaluate adherence to established policies, standards, and applicable obligations. Defined responsibilities and oversight processes support the identification and evaluation of compliance risks, communication of relevant requirements, and monitoring of control effectiveness. Personnel and applicable third parties are expected to comply with established security and compliance requirements, with training and communication supporting awareness of individual responsibilities.

Zayo also maintains processes for identifying, documenting, escalating, and remediating compliance deficiencies and control weaknesses. Findings are evaluated according to risk and potential business impact, assigned to accountable owners, and tracked through corrective action and verification of effectiveness. Material compliance risks and significant findings are subject to appropriate management reporting and oversight. Policies, standards, control mappings, and supporting processes are periodically reviewed and updated to address changes in regulatory obligations, business operations, and the risk environment. Together, these measures establish a strong compliance management framework that supports transparency, accountability, audit readiness, and continuous improvement of the security controls protecting Zayo's operations and customer services.



Personnel Security

Zayo maintains a personnel security program designed to ensure employees, contractors, and other authorized personnel understand and fulfill their security responsibilities throughout their employment or engagement lifecycle.

The program establishes requirements for personnel screening and role suitability, employment terms, confidentiality commitments, security policy acknowledgements, workforce training, and appropriate assignment of security-related responsibilities. Screening and verification requirements are determined by applicable legal obligations, contractual commitments, position sensitivity, and associated risk.

Personnel are expected to complete relevant security awareness education and role-specific training, protect organizational and customer information, and report suspected security incidents or weaknesses. Changes in personnel responsibilities, transfers, and terminations are subject to established requirements addressing access modification or removal, return of organizational assets, and continuing confidentiality obligations. These measures are intended to reduce personnel-related security risks, promote a security-conscious workforce, and maintain accountability for safeguarding information throughout the workforce lifecycle.



Access Control Standards

Zayo's structured access control framework is designed to ensure that access to information systems, applications, networks, and sensitive information is restricted to authorized individuals and systems with a legitimate business need.

Access is governed by principles of least privilege, need-to-know, role-based authorization, segregation of duties, and individual accountability. Documented requirements address identity verification, access requests and approvals, account provisioning, privileged access, authentication, and secure remote connectivity. Multifactor authentication is required for applicable access scenarios, with additional safeguards established for privileged, administrative, and higher-risk access.

The Organization's security framework also establishes requirements for periodic access reviews, account monitoring, and modification or removal of access when responsibilities or employment relationships change. Access-related activities and approvals are subject to documentation and evidence requirements, supporting traceability and oversight. These controls are designed to reduce the likelihood of unauthorized access and ensure permissions remain aligned with approved business responsibilities throughout the identity lifecycle.



Artificial Intelligence

Zayo maintains artificial intelligence governance and security requirements designed to support the responsible, secure, and compliant use of AI technologies across its business operations. The program establishes expectations for the evaluation, approval, implementation, monitoring, and management of AI systems, including AI-generated responses or outputs that may affect customers, employees, or business operations. These requirements consider information security, privacy, regulatory obligations, ethical principles, and customer impact.

Zayo's AI governance requirements address defined ownership and accountability, authorized AI usage, risk assessment, data protection, human oversight, and appropriate transparency. AI systems and use cases are subject to risk-based review before production deployment, including consideration of cybersecurity threats, data sensitivity, model integrity, accuracy, reliability, potential bias, customer impact, and legal or regulatory requirements. Customer-affecting or automated-decision use cases require enhanced governance review, and AI-generated responses must be reviewed, verified, and fact-checked by appropriate personnel before use. The program also establishes requirements for protecting confidential information and intellectual property throughout AI development, configuration, and use.

Ongoing oversight includes monitoring AI systems for performance, security weaknesses, inappropriate or biased outputs, misuse, and changes in risk exposure. Documented requirements address reporting and escalation of AI-related concerns, including customer-affecting responses that may be inaccurate, harmful, discriminatory, or otherwise inappropriate. Corrective action may include review, revision, restriction, or deactivation of AI systems that do not meet applicable security, compliance, or risk-acceptance requirements. These safeguards are designed to promote responsible AI adoption while maintaining appropriate human accountability and protecting organizational and customer information.

Zayo is committed to delivering secure, reliable, and high-performance communications infrastructure and services. As part of our operations, we may utilize automation, analytics, and, in some cases, AI or machine learning technologies to support service delivery, network management, and customer experience improvements.

These technologies are primarily used to enhance operational efficiency, including activities such as network monitoring, traffic optimization, fault detection, and service assurance. Where automation or AI is applied, it is designed to augment human decision-making rather than replace it, and appropriate oversight is maintained by qualified personnel.

Zayo restricts the use of customer information in AI tools. Customer information may not be entered into or used with an AI tool unless the use has been specifically approved with applicable privacy, security, confidentiality, and contractual requirements addressed.

Zayo does not use AI or automated decision-making systems to make solely automated decisions that produce legal or similarly significant effects on customers without human involvement.

We are committed to responsible and transparent use of technology. Our implementation of AI and automation aligns with applicable laws, regulations, and industry best practices, including those related to data protection, privacy, and security.



Asset Management Standards

Asset management standards are designed to support the identification, ownership, inventory, protection, maintenance, and controlled disposition of organizational technology and information assets.

Documented requirements cover hardware, software, information systems, network infrastructure, cloud resources, and other technology assets supporting business operations. Asset management includes maintaining appropriate inventories, assigning accountable owners, identifying criticality and dependencies, and applying security requirements based on the asset's purpose, sensitivity, and associated risk.

The Organization's security framework establishes controls for authorized asset usage, software management, maintenance, configuration changes, and asset lifecycle activities. Asset inventories and supporting records are intended to provide visibility into technology resources, support risk and vulnerability management, and facilitate appropriate protection throughout their operational life. Equipment removal, return, decommissioning, and disposal are subject to applicable security and information-handling requirements. These controls support accountability, operational continuity, and the protection of customer and organizational information associated with managed assets.



Data Protection and Retention

Zayo maintains data protection and records management requirements designed to safeguard organizational and customer information throughout its lifecycle, including collection, creation, processing, storage, transmission, retention, archival, and secure disposal.

Data protection requirements are determined by information sensitivity, classification, business purpose, and applicable legal, regulatory, and contractual obligations. Safeguards include authorized access, appropriate confidentiality protections, secure storage and transfer methods, encryption where required, and measures intended to preserve information integrity and prevent unauthorized disclosure.

Zayo's records management standards establish requirements for records ownership, retention, preservation, controlled access, and secure disposition. Information must be retained according to applicable schedules and obligations, with additional requirements addressing legal holds, investigations, and circumstances requiring preservation beyond ordinary retention periods. Once authorized for disposal, information and associated media are subject to appropriate secure destruction or sanitization requirements. This lifecycle-based approach is intended to protect customer information while supporting responsible retention, regulatory compliance, and the reduction of unnecessary data exposure.



Data Classification, Handling, Storage, and Transmission

Zayo maintains a data classification and handling program designed to ensure organizational and customer information receives safeguards appropriate to its sensitivity, business value, and applicable legal, regulatory, and contractual requirements.

The program establishes four primary sensitivity classifications: Public, Internal Use, Confidential, and Restricted. Information is classified to determine appropriate access restrictions, storage protections, transmission methods, sharing permissions, retention requirements, and disposal controls. Higher-sensitivity information is subject to additional safeguards designed to prevent unauthorized access, disclosure, alteration, or loss.

Zayo's standards require sensitive information to be handled through authorized systems and approved information-transfer methods, with encryption and other protective controls applied according to classification and risk. Sharing information with external parties is governed by appropriate authorization, confidentiality protections, and applicable contractual obligations. Information owners and responsible personnel are expected to maintain appropriate classification and handling practices throughout the data lifecycle. This structured approach is intended to support consistent protection of customer and organizational data regardless of how it is stored, processed, or exchanged.



Privacy Protection

Zayo's privacy and data protection framework is designed to safeguard personal information and support compliance with applicable privacy laws, regulatory requirements, contractual obligations, and organizational security standards. The framework establishes requirements governing the collection, use, processing, storage, sharing, retention, and disposal of personal information throughout its lifecycle.

Zayo's privacy requirements incorporate principles of lawful and transparent processing, purpose limitation, data minimization, accuracy, confidentiality, and accountability. Personal information is subject to safeguards appropriate to its sensitivity, classification, intended use, and applicable obligations. The framework addresses privacy governance, defined responsibilities, information inventories, authorized access, secure information handling, and oversight of personal data shared with or processed by third parties. Privacy considerations are also incorporated into the design and modification of systems, services, and business processes through risk-based assessments and privacy-by-design requirements.

Zayo establishes requirements for responding to applicable individual privacy rights, including requests relating to access, correction, deletion, and other rights provided under relevant laws. Privacy incident management requirements address the identification, escalation, investigation, documentation, remediation, and notification of potential personal data breaches. Personal information is subject to defined retention and secure disposition requirements, with appropriate oversight of third-party processing and international data transfers. Through these controls, Zayo seeks to promote responsible information handling, maintain transparency and accountability, and protect the privacy of individuals whose personal information is processed in connection with its business operations and services.



Cloud Security

Zayo maintains documented cloud security requirements designed to protect information, applications, infrastructure, and services hosted or managed within cloud environments. Cloud security is governed through Zayo's broader information security, technical security, operational management, and third-party oversight requirements.

These requirements address the evaluation and authorized use of cloud services, definition of security responsibilities, protection of information, identity and access management, secure connectivity, monitoring, and configuration and change management. Cloud environments are subject to security requirements appropriate to their business criticality, data sensitivity, operational dependencies, and associated risks.

Zayo's standards also address cloud service agreements, applicable geographic and legal considerations, operational monitoring, service continuity, and the controlled transition or termination of cloud services. Cloud providers are subject to relevant supplier security and contractual requirements, supporting oversight of services involving organizational or customer information. These measures are intended to establish appropriate accountability and maintain security protections across the lifecycle of cloud-based services.



Network Security

Zayo maintains network communications security requirements designed to protect the confidentiality, integrity, and availability of information exchanged across its network infrastructure, internal systems, remote connections, and external communication pathways.

The network security program incorporates layered protections, including network segmentation, security zones, boundary controls, traffic filtering, authorized connectivity, and monitoring for suspicious or unauthorized activity. Connections between environments with different trust levels are subject to defined security requirements, while access to network services and communication protocols is restricted according to authorized business needs.

The program also establishes requirements for secure remote access, protection of publicly accessible systems, network configuration management, and encryption of sensitive information transmitted across untrusted networks. Network-related security events and information flows are subject to appropriate logging and monitoring requirements. These safeguards are intended to reduce unauthorized network access, limit exposure between interconnected environments, and support the secure and reliable delivery of Zayo's network and communication services.



Physical Security

Zayo maintains a physical and environmental security program designed to protect personnel, facilities, equipment, and information assets against unauthorized access, physical damage, environmental threats, and operational disruption.

Security requirements are established according to facility criticality, operational purpose, and risk. Physical protections include designated security perimeters, controlled building and restricted-area access, visitor management, authorized access credentials, and appropriate security monitoring. Facilities housing critical infrastructure or sensitive information are subject to additional access restrictions and protective measures based on their security classification.

The program also addresses equipment protection, secure working areas, environmental safeguards, maintenance activities, and the appropriate handling or disposal of physical assets and storage media. Physical access permissions and security-related events are subject to documented control and accountability requirements. These measures support the protection of Zayo's physical infrastructure, reduce the likelihood of unauthorized interference, and contribute to the operational continuity of facilities supporting customer services.



Secure Development

Zayo maintains security requirements governing the design, development, implementation, and modification of information systems and technology solutions. These requirements are intended to incorporate security considerations throughout the system lifecycle and reduce the introduction of vulnerabilities into production environments.

Zayo's systems design and implementation standards address security requirements during solution planning, architecture, development, testing, deployment, and operational transition. Controls include security risk considerations, appropriate access restrictions, secure configurations, authorized changes, testing and validation, and the protection of sensitive information within development and supporting environments.

Changes to production systems are subject to established change management requirements intended to ensure that modifications are appropriately reviewed, authorized, tested, and documented. Security responsibilities extend to the teams supporting applications, platforms, infrastructure, and associated services. This approach is designed to identify and address security weaknesses before deployment and maintain appropriate safeguards as systems evolve, supporting the reliability, confidentiality, and integrity of services delivered to customers.



Change Management

Zayo's formal change management program is designed to ensure modifications to its technology infrastructure, applications, networks, systems, configurations, and supporting services are appropriately evaluated, authorized, tested, implemented, and documented. The program is intended to minimize the risk of unauthorized or disruptive changes while preserving the security, reliability, and availability of systems supporting business operations and customer services.

Changes are managed through established processes that consider the nature, scope, risk, and potential impact of proposed modifications. Documented requirements include change classification, risk and impact assessment, approval, implementation planning, testing, communication, and verification. Security, privacy, operational, and customer impacts are evaluated as applicable, with additional review and oversight requirements for higher-risk or customer-impacting changes. Changes to production environments are expected to follow appropriate authorization and testing requirements before implementation.

The program also distinguishes between standard, normal, and emergency changes, allowing expedited handling when necessary to restore services, respond to critical incidents, or address material operational or security risks. Emergency and other significant changes are subject to documentation and appropriate retrospective review. Change records, approvals, testing results, implementation outcomes, and post-implementation assessments support accountability and traceability. These controls are designed to reduce unplanned service disruption, maintain configuration integrity, and provide a consistent, controlled approach to changes affecting Zayo's infrastructure and services.



Supplier Security

Zayo maintains a supplier security and third-party risk management program designed to address risks associated with vendors, service providers, contractors, and other external organizations that support its operations or access organizational and customer information.

The program establishes requirements for supplier identification, due diligence, risk assessment, contractual security obligations, and ongoing oversight. Supplier evaluations consider the nature of services provided, information sensitivity, access requirements, operational dependencies, and potential business impact. Suppliers are expected to maintain appropriate security safeguards, including authorized access, secure information handling, incident reporting, and protection of systems and data within the scope of their engagements.

Zayo's supplier oversight requirements extend throughout the relationship lifecycle, including onboarding, performance monitoring, reassessment, management of identified risks, and termination or transition. Contractual requirements address security responsibilities, information protection, notification obligations, and appropriate return or disposal of information. These controls are designed to reduce third-party exposure and maintain accountability for security requirements across Zayo's supply chain.



Risk Management

Zayo's enterprise risk management framework is designed to identify, assess, prioritize, manage, and monitor risks that could affect its information assets, technology infrastructure, business operations, regulatory obligations, and customer services. Risk management is integrated into Zayo's broader security governance program to support informed decision-making, appropriate resource allocation, and the protection of critical business activities.

The framework establishes a consistent methodology for evaluating risks based on their likelihood, potential impact, and relationship to defined organizational risk appetite and tolerance levels. Risk assessments consider threats, vulnerabilities, operational dependencies, technology changes, suppliers, and applicable business and compliance requirements. Identified risks are evaluated and prioritized using established criteria, with treatment strategies that may include mitigation, avoidance, transfer, or formal acceptance based on the circumstances and approved decision-making authority.

Zayo maintains requirements for documented risk ownership, risk registers, treatment plans, management reporting, and periodic reassessment. Risk monitoring activities address emerging threats, changes in business conditions, control effectiveness, and progress toward remediation. Material risks and exposures exceeding established tolerance levels are subject to appropriate escalation and governance oversight. This structure is designed to support proactive risk identification, accountable risk treatment, and continuous improvement of the security controls protecting Zayo's operations and customer services.



Vulnerability Management

Zayo maintains a vulnerability management program designed to identify, evaluate, prioritize, and remediate security weaknesses affecting information systems, applications, network infrastructure, and other technology assets.

Documented requirements establish a combination of vulnerability scanning, security assessments, penetration testing, and patch management to identify potential security exposures. Vulnerabilities are evaluated using risk-based considerations, including technical severity, asset criticality, business impact, and the potential consequences of exploitation. Remediation activities are prioritized according to established requirements, with patch deployment and corrective actions governed by applicable change management and validation processes.

The program also establishes requirements for tracking remediation activities, managing exceptions, documenting risk decisions, and retaining supporting control evidence. Security assessments and ongoing monitoring inform remediation priorities and improvements to the control environment. These measures are intended to reduce exposure to known vulnerabilities, support timely corrective action, and strengthen the security and resilience of systems supporting Zayo's operations and customer services.



Enterprise Resilience

Zayo Group, LLC has established and maintained an Enterprise Resilience Program that encompasses Business Continuity Management (BCM), Disaster Recovery (DR), and Crisis Management (CM), along with associated testing and continuous improvement activities.

Zayo's Enterprise Resilience Program is designed to support the continuity of operations and systems during disruptive events. The program integrates business continuity, disaster recovery, crisis management, and incident management into a unified framework that helps protect critical services, reduce operational impact, and support timely recovery.

Key Components

Business Impact Analysis and Continuity Planning

Zayo performs Business Impact Analyses (BIAs), risk assessments, and dependency reviews to identify critical business functions and supporting systems. These activities define recovery objectives and inform continuity strategies, which are documented in formal plans to guide response and recovery efforts.

Incident and Crisis Management

Zayo maintains an Incident Management Plan that establishes a structured, all-hazards approach for responding to significant disruptions. This framework enables coordinated decision-making, clearly defined roles and responsibilities, timely escalation, and effective communication across the organization.

Disaster Recovery, Backup, and Restoration

Zayo's disaster recovery capabilities are designed to restore critical systems, data, and services following an outage or disruption. These capabilities are supported by routine data backups, documented restoration procedures, and regular testing to validate recovery readiness.

Pandemic and Workforce Continuity Preparedness

The program includes workforce continuity planning to address scenarios such as pandemics or large-scale personnel disruptions. This includes remote work enablement, emergency procedures, and clearly defined role-based responsibilities to sustain operations.

Alternate Facilities and Operational Resilience

Where appropriate, Zayo maintains alternate facility and relocation strategies to ensure continued business operations in the event primary locations become unavailable.

Training, Testing, and Continuous Improvement

Zayo conducts regular training and testing exercises, including tabletop and functional tests, to validate the effectiveness of its plans and ensure personnel readiness. Plans are reviewed and updated periodically to reflect evolving business needs, risks, and operational changes.

Based on our review and ongoing program governance, Zayo attests that its Business Continuity Management and Disaster Recovery programs are:

- Documented and maintained in alignment with industry best practices
- Regularly tested to validate effectiveness and recovery capabilities
- Supported by training and awareness activities for relevant personnel
- Subject to continuous improvement through periodic review and updates

Zayo attests that it performs testing of its BCP and DR plans at least annually and that no material findings have been reported in its tests.



Incident Response

Zayo is committed to maintaining robust and adaptive Incident Management practices as part of its Enterprise Resilience program to safeguard our organization, stakeholders, customers, and sensitive information. In today's dynamic and interconnected business environment, organizations face an increasing array of cybersecurity threats and operational disruptions. To effectively address these challenges, Zayo's Enterprise Resilience program includes a comprehensive Incident Management Plan (IMP) that defines escalation procedures and guides the integrated response required to respond effectively, mitigate risks, and ensure business continuity.

- **Timely Detection and Response:** Implement a systematic approach to detect, analyze, and respond to security incidents promptly.
- **Minimize Impact:** Minimize the impact of incidents on business operations, data integrity, and customer trust.
- **Communication and Coordination:** Establish clear communication channels and coordination procedures to facilitate effective collaboration among internal and external stakeholders.
- **Documentation and Learning:** Document incident details, response actions, and lessons learned to continuously improve future incident response capabilities.
- **Preparation:** Clearly defined roles and responsibilities for incident response team members, regular training and awareness programs that enhance employees' ability to recognize and report incidents, and periodic testing and updating of incident response procedures
- **Identification and Classification:** Continuous monitoring and analysis of network activities, incident categorization based on severity and impact, and immediate identification of incidents through the use of monitoring tools and technologies
- **Containment, Eradication, and Recovery:** Defined procedures for isolating and containing incidents, swift eradication of threats and vulnerabilities, and efficient recovery processes to restore normal operations
- **Communication and Notification:** Establish communication protocols for internal and external stakeholders using a clear chain of command for incident reporting and escalation
- **Post-Incident Analysis:** Post-incident analysis to understand the root cause and improve incident response procedures and documentation of lessons learned and recommendations for continuous improvement

Zayo's Enterprise Resilience program treats all scenarios and events with equal urgency and tests during all real-time events. Outside of real-time events, the Incident Management Plan is tested on an annual basis through tabletop exercises and after incident reports. Events are managed and escalated appropriately using the ServiceNow platform. Each event is assessed, and required actions are documented in runbooks available to all employees in the ServiceNow Knowledge Base.



Procedures are updated as needed based on lessons learned following each event, and the Organization chooses one event per year to report as its formal test.

Per policy, Zayo does not share the entirety of the Incident Management Plan or other internal Enterprise Resilience program documents with external parties due to the sensitive information contained within.



Penetration Test Executive Summary

Zayo engaged a third-party to perform a web application penetration test of the ZInsights application. Testing and verification were conducted between April 13, 2026 and April 24, 2026, with the report issued on May 8, 2026. The assessment was designed to identify application-based threats and vulnerabilities, compare the application's security posture against industry best practices, and provide remediation guidance to reduce risk.

The assessment summary identified five low-severity findings. No critical, high, or medium severity findings were identified in the redacted executive summary provided for review.

Zayo treats vulnerability assessment results, including penetration test reports, as highly sensitive internal resources and does not share detailed reports externally. Detailed findings may include sensitive technical information such as testing scope, affected systems, exploitation context, and remediation details.

Zayo attests that all identified vulnerabilities are logged, prioritized based on risk and potential impact, assigned to responsible owners, and remediated, mitigated, excepted, or otherwise risk-treated in accordance with Zayo's vulnerability management process. Remediation is validated through appropriate follow-up activities, such as rescanning, testing, evidence review, or responsible-owner confirmation.