July 2026

Wood Mackenzie - Cybersecurity Approach

Change History

Date	Change made by	Nature of Change(s)
July 2026	Graeme Marsh	Annual review and updates
July 2026	Denise Fraser	Branding amendments

Contents

Cyber Security Overview

Wood Mackenzie is committed to providing world class security and culture, where security is integrated into every decision, process, and technology from the start. Risk and decision making is assessed throughout to ensure we manage threats and changing technologies using an established security framework.

Security is agile, inherent by design providing a security infrastructure with defense in depth protection through technology, process and people. All our development follows DevSecOps principles in every aspect of our design lifecycle to ensure sustainability and enhance delivery.

We don't compromise on security and all our Data Centres are accredited to rigorous international standards, including SOC 2 Type 2, NIST 800-53/FISMA, ISO 9001 and ISO 27001 demonstrating our commitment to robust security and quality management.

This document provides an overview of our security framework and culture, including – policies, principles, management systems, design, data protection, continuous vulnerability management, security monitoring, secure configuration of assets, access control management, network defense, security awareness and infrastructure management.

Cyber Security Framework

Wood Mackenzie is committed to protecting its information and systems and that of all of our customers.

To achieve this goal, we have developed a framework and Information Security Management System (ISMS) that is applicable across all areas of the business and 3rd parties.

The ISMS provides a framework of policies and procedures that includes all legal, physical, information and technical controls. The goal of the ISMS is to provide complete coverage of the activities and risks across our environments, including 3rd parties, in relation to Confidentiality, Integrity and Availability. The process is repeatable, measured and reported. We adhere to a continuous improvement process of security risk management for effective assessment and treatment of security risk.

Continuous security improvement is achieved through technical controls, supported by appropriate management and procedures.

Our Cyber Risk Governance Program includes an Executive Risk Management Team designed to fulfill the company's data responsibility objectives throughout all facets of the company. In collaboration with Wood Mackenzie's Compliance Council, the Cyber Risk Governance Program directs and prioritizes elements such as:

- Confidentiality Requirements
- Information Management
- Software Development
- Incident Management
- Network Security
- Access Control, Roles & Permissions
- Third Parties & Subcontractors
- Asset Management

- Business Continuity & Disaster Recovery
- Risk Management
- Physical Security & Infrastructure
- International Data Transfers
- Vendor Risk Review
- Change Management
- Information Backup & Recovery

For our Vendor Risk Management please see supplier commitment requirements included in our Supplier Code of Conduct available here.

This overview does not constitute any binding agreement nor establish any legally enforceable obligation. It is subject to modification at the sole discretion of Wood Mackenzie.

Executive Oversight & Governance

Executive Oversight

Wood Mackenzie's Executive Risk Management Team and the Compliance Council oversee the company's management of cybersecurity, including oversight of appropriate risk mitigation strategies, systems, processes, and controls. The Executive Risk Management Team and Compliance Council receive regular reports from Wood Mackenzie's Leadership about the company's cybersecurity risks, management review processes, overall health, and readiness to respond to an incident.

Cyber Risk Management Leadership Roles

The Compliance Council, which includes the top corporate executives, provides guidance and authority related to the enforcement of Wood Mackenzie's Framework, including the strategies, policies, procedures, processes, and systems established by management to identify, assess, measure, monitor, and manage risks. The Compliance Council also reinforces the corporate risk appetite and determines whether residual risk is acceptable.

The function of Enterprise Risk Management and Compliance (ERM&C) is to oversee and advise on implementation of the Framework throughout Wood Mackenzie. In doing so, the ERM&C division aggregates and assesses risk across the enterprise. Within the division are Wood Mackenzie's Cybersecurity and Information Risk Management functions that partner with Wood Mackenzie's corporate functions to help ensure that risk management strategies are implemented. The ERM&C division also hosts training and awareness sessions, sponsors working groups across the enterprise on critical security topics and provides centralized incident response.

Promoting a Culture of Awareness and Ownership with All Employees

Wood Mackenzie recognizes that all Wood Mackenzie employees and many third parties have significant roles and responsibilities in ensuring the fulfillment of Wood Mackenzie's risk management strategy and objectives. In summary, these roles and their responsibilities include:

- The Wood Mackenzie workforce (employees and third parties) are accountable for understanding and complying with all security policies, guidelines, and procedures, including Wood Mackenzie's Acceptable Use Policy, that establishes the responsibilities for the workforce when using company assets.

- Internally designated data owners report to and are empowered by the executive management of their respective Wood Mackenzie business and have full accountability for the security of the business unit's segment of products and services.
- Application owners are responsible for the overall procurement, development, integration, modification, and operation and maintenance of application systems supporting Wood Mackenzie businesses and functional units.
- Systems owners are responsible for providing the technology services for the set of application systems and related infrastructure supporting Wood Mackenzie businesses.

Awareness and Training

Wood Mackenzie provides the members of its workforce, including personnel and partners, cybersecurity awareness education and training to enable them to perform their information security-related duties and responsibilities consistent with Wood Mackenzie policies, procedures, and agreements. These safeguards include:

- Employees must acknowledge and adhere to key Wood Mackenzie information security policies upon hiring and on an annual basis thereafter.
- Employees also receive information security training tailored to specific job functions upon hiring and thereafter on an annual basis.
- Employees with elevated system privileges and those with information security responsibilities receive a more intense level of training relative to their specific functions.
- Wood Mackenzie conducts unannounced enterprise phishing assessments targeting our workforce, with additional training enrollments for individuals that fail the assessment.

Policies and Governing Documents

Policies governing our operations are written and designed to embed industry leading controls designed to mitigate risk to Wood Mackenzie and our customers.

Executive management approves the overarching risk policy, the information security framework, and the related supporting policies that collectively reinforce and advance our comprehensive cyber risk culture.

Wood Mackenzie employees, contractors, and third parties are responsible for ensuring compliance with all information security policies.

External Audits, Certifications, and Attestations

Wood Mackenzie's control environment, including controls related to cybersecurity described in this document, are regularly subject to independent testing from both internal and external audits. A closed-loop corrective action process manages any potential exceptions identified during audits.

International Data Transfers

Wood Mackenzie has adopted appropriate policies, procedures, contracts, and security measures to ensure that cross-border transfer of data meets government and client expectations.

Risk Identification and Management

Risk Management & Assessment

Wood Mackenzie's process for security risk management aligns with enterprise strategic objectives and defines expectations for the organization to identify, assess, and manage risk. Wood Mackenzie conducts various risk assessments with our businesses, no less than annually to understand cybersecurity risk to organizational operations. Results from risk assessments are escalated based on materiality, within our security governance structure, to ensure appropriate risk treatment, including treatment plans and risk acceptance where appropriate. The results also inform Wood Mackenzie's cyber risk management strategy, objectives, and key initiatives.

The security function maintains a suite of Top Risks, each assigned to an accountable Top Risk Owner (TRO). These risks are subject to formal assessment on an annual basis and are re-evaluated following any material events or incidents.

The risk response process requires identification and input from the TRO and aligned top risk, the business owner and affected process owners. The Information Risk Management team oversees plans for control activities to implement risk responses and to identify costs, benefits, and execution responsibilities of control and process owners.

Asset Management

Wood Mackenzie has an established asset management policy and associated procedures to ensure the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistently with their relative importance to business objectives and Wood Mackenzie's risk strategy. The policy includes assets managed on premises as well as those supported by third-party hosting and cloud-based services.

Information assets are clearly identified, documented, and regularly updated in a centrally managed inventory, which includes designated business, data, application, and system owners.

- Wood Mackenzie classifies data based on the value and sensitivity of the information to the organization. Specific handling and data security controls are defined and deployed depending on data classification.
- Software installed on any machine connecting to Wood Mackenzie or any member company network must be used only for authorized business purposes.

A number of safeguards are utilized including:

- An established and maintained detailed Enterprise Asset Inventory
- Active Discovery tooling
- Passive Asset discovery
- Established and maintained software inventory
- Automated software inventory tools

Supply Chain Risk Management

Wood Mackenzie has established a third-party risk management policy and supporting processes to identify, assess and manage supply chain risk. The policy requires that vendors are assessed and tiered based on their risk to the company. Vendors are then subjected to varying levels of due diligence and ongoing monitoring that aligns with the inherent risk of services they provide.

Suppliers are required to acknowledge and commit to compliance with a Supplier Code of Conduct, which includes privacy and confidentiality provisions.

Defense-In-Depth Security

To provide for the security and resiliency of its systems and assets, Wood Mackenzie has deployed a defense-in-depth strategy of protective solutions, including the following:

Identity Management and Access Control

Wood Mackenzie has established policies, procedures, and associated system functionality to 1) limit access to physical and logical assets and associated facilities to authorized users, processes, and devices, and 2) manage access consistent with the assessed risk of unauthorized access.

Our principles are based on 'least privilege', 'need to know' and 'zero trust' methodologies, these are strictly enforced and monitored.

These controls include but are not limited to:

- Information access is governed by the principle of least privilege, where information access is limited to that which is necessary to perform job responsibilities.
- Access to Wood Mackenzie information is controlled through a managed process that addresses authorizing, modifying, and revoking access, as well as a periodic review of information system privileges.
- Web filtering functionality is deployed to manage Internet access. Internet search or access requests are routed through the filter, which blocks access to inappropriate or potentially harmful websites and otherwise enforces corporate and regulatory policy compliance.
- Remote access to Wood Mackenzie information assets is controlled through multi-factor authentication.
- Vendor access to any information assets is governed by associated data classification handling requirements.

Physical Security

Wood Mackenzie has deployed policies, procedures, and supporting systems so each of its facilities, including data centers and storage facilities, have appropriate physical access controls in place to protect it from unauthorized access. Those controls include but are not limited to the following:

- Physical access management systems are deployed for Wood Mackenzie facilities, including data centers and storage facilities.
- CCTV monitoring on a 24/7 basis is often deployed at points of access to Wood Mackenzie facilities and within Wood Mackenzie controlled secure spaces, including those with high concentrations of sensitive data.
- Physical and printed media and other types of physical assets are disposed of by confidential means, such as shredding or confidential disposal services.
- Visitors to Wood Mackenzie facilities must present a valid government ID and be escorted by a Wood Mackenzie employee.

Data Protection

Wood Mackenzie has deployed controls to provide assurance that information and records (data) are managed consistently with the company's risk strategy and governing data principles to protect the confidentiality, integrity, and availability of the data. These controls include but are not limited to the following:

- Data is classified according to a data classification and handling policy.
- Data is controlled and managed in accordance with the data handling requirements set forth in the policy, which considers our Wood Mackenzie global workforce, compliance requirements for offshore access, and customer requirements for data sharing and segregation.
- Sensitive data is restricted to only authorized individuals, and such data is protected (i.e., tokenized, encrypted, etc.) in accordance with industry's best practice methods when stored or processed.
- Non-publicly available data is encrypted by industry-leading protocols and algorithms when in transit or at rest.
- Data is encrypted on any mobile device that has the capability to store Wood Mackenzie information, including mobile devices, laptops, notebooks, and smartphones.
- Data is encrypted at rest on any media used for purposes of disaster recovery, business continuity, and archiving.
- Data storage is encrypted for any remotely accessible Wood Mackenzie information assets, including but not limited to web-accessible resources and file-sharing systems.
- Development and testing environments are separated from production environments.

- Data is retained in accordance with our global records management policy, in alignment with business need, and per applicable laws and regulations.
- Wood Mackenzie follows industry standards for data disposition and destruction that involves methods specific to the media or storage type, so information cannot be retrieved or reconstructed in the event the storage device is either reused or destroyed.
- Data is encrypted in transit utilizing TLS 1.2.
- Data is encrypted at rest utilizing AES-256 encryption.

Application and Infrastructure Security

Wood Mackenzie has established security policies that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities, as well as processes and procedures that are maintained and used to manage the protection of information systems and assets.

Perimeter Security

- Wood Mackenzie's network is architected to restrict access to only authorized users for authorized services for both external and internal parties. These include:
  - Multiple firewall devices at external access points into the network prevent intrusion, limit accessible services, and isolate Wood Mackenzie's network from those of customers and other third parties.
  - Firewalls protect Internet-facing infrastructure and applications. There are firewalls between demarcation zones and Wood Mackenzie's internal network.
  - Firewalls restrict access between network segments to allow only authorized personnel access to specifically configured services.

- Web application firewalls are deployed to protect web applications from malicious activities such as cross-site request forgery, cross-site scripting (XSS), and SQL injection.
- Secure e-mail gateway services supported by dynamically updated threat intelligence feeds are deployed to evaluate inbound e-mail traffic, blocking or quarantining e-mails exhibiting suspicious characteristics. Examples of these controls are reputation filters for known malicious senders or those that spoof otherwise trusted senders, content filters for spam or malware, and threat filters for phishing or other non-malware based social engineering threats such as business e-mail compromise attempts.
- Vulnerability and penetration assessments are proactively performed to simulate an external attacker, so Wood Mackenzie can enhance its defenses, with findings remediated within internally defined service level agreements.

Secure Development and Change Management

Wood Mackenzie has developed and published a secure development policy and related procedures, which are designed to provide assurance that secure coding practices are infused throughout Wood Mackenzie's software development life cycle (SDLC), and to uphold data quality standards and practices, from initial planning through disposal of the system. Significant development requirements include but are not limited to:

- Development adheres to secure standards set forth by the Open Web Application Security Project (OWASP) and the Application Security Working group (ASWG).
- Development staff are trained in current secure coding practices.
- Wood Mackenzie and its member companies follow a SDLC process that undergoes reviews by Wood Mackenzie Risk and Compliance division.
- Production code is reviewed using security checkpoints throughout the software development life cycle to enable consistent application of security.
- Changes follow a formal change control procedure to enable the security and integrity of the information and information system.
- Static code scanning and/or dynamic code scanning is performed for systems, and systems must be void of any known vulnerabilities rated as high or critical prior to release to production.

Secure Configuration Management

Wood Mackenzie's configuration management policy and related procedures are designed to ensure that consistent and secure configuration baselines are established and maintained across the Wood Mackenzie Ltd. enterprise to encompass relevant components such as endpoints (laptops, desktops, browsers, and mobile devices), operating systems, application services, virtualization, and cloud services. Specific controls include but are not limited to:

- Maintaining baseline configurations as current, using automated mechanisms to reflect approved changes.
- Following a formal change control process that includes oversight from a change advisory board (CAB).
- Automating change control process, and other mechanisms, such as file integrity monitoring, to detect and prevent unauthorized changes.
- Enforcing access restrictions, logging, and log review of changes to confirm changes are properly approved.
- Deploying automated mechanisms to verify correct operation of security functions upon system startup and restart and to provide notification and alerts of failed security tests.
- Scanning cloud-based environments weekly to identify any configuration changes not consistent with baseline configuration standards and security rules.

Endpoint Security

Wood Mackenzie has enacted policies and procedures to manage endpoints, prevent vulnerabilities whenever feasible, and otherwise identify and promptly remediate the occurrence of vulnerabilities. These include but are not limited to:

- Wood Mackenzie patch management program is based on best practices, including maintaining a current inventory of IT components, risk rating these components for patch relevancy, monitoring vendor patches, establishing a patch deployment schedule based on applicability and risk rating, and following a controlled change management process for patch deployment, testing, and release to production.
- Endpoint detection and response software is installed on endpoints to prevent malware and provide forensic capability to assist with incident response.
- Antivirus/antimalware software is installed on Wood Mackenzie endpoints, and employees are prohibited from disabling such software.
- Endpoint data loss prevention software is installed on endpoints that restricts use of removable media.

Continuous Monitoring

Wood Mackenzie establishes logging and monitoring capabilities to enable the ongoing review and reconstruction of user activities and timely detection of potential vulnerabilities, malicious activity, security violations, performance, and processing exceptions.

- User-related audit logs are maintained for a wide range of system activities and regularly reviewed for indications of anomalous activities. Activities that are logged and monitored include but are not limited to successful and unsuccessful login attempts; actions performed by privileged users; changes, additions, or deletions to any account with root or administrative privileges; and the creation, deletion, and modification of system-level objects. Logs maintained by Wood Mackenzie are attributable to a unique user, and time synchronization technology is leveraged to assist with the maintenance of an accurate audit trail.
- System components and applications are configured such that audit logs, network telemetry data (e.g., packet metadata), and security events from across the enterprise are captured in a centralized Security Incident and Event Monitoring (SIEM) system.
- Wood Mackenzie performs frequent scans to monitor for potential vulnerabilities to applications, networks, operating systems, and cloud services. Those potential vulnerabilities are assigned severity ratings that determine the required remediation timeframe.
- Database activity monitoring is employed for critical database systems with regular review for suspicious or anomalous activity.
- Data loss prevention (DLP) software is deployed to monitor potential data exfiltration and generate triggers for incident management purposes and provide logging for forensic purposes.

- Wood Mackenzie User and Entity Behavioral Analytics (UEBA) incorporates machine learning to enhance user and peer group behavioral analysis. Machine learning enables risk scoring to be applied to potential anomalies that reflect the likelihood of a threat related to anomalous behavior. Wood Mackenzie UEBA automatically triggers and prioritizes incident response events.
- Wood Mackenzie Security Operations Center (SOC) operates on a 24/7/365 basis to monitor, identify, respond to, and remediate any incidents that threaten the confidentiality, integrity, and availability of Wood Mackenzie's information systems. The SOC leverages data from Wood Mackenzie security components such as firewalls, intrusion protection systems, and authentication platforms, as well as other sources.

Response and Recovery Planning

Incident Response Program (IRP)

Wood Mackenzie has established an IRP that includes policies and procedures that encompass the life cycle of incident management. Wood Mackenzie has defined roles and responsibilities in detail for each stage of the IRP, as outlined below. Personnel must successfully complete training before being assigned IRP responsibilities and at least annually thereafter.

Wood Mackenzie's ER&C organization oversees IRP planning, deployment, and execution for the entire IRP life cycle.

IRP phase	Key activities
Preparation	Incident response procedures are defined in detailed for potential scenarios. Communications and coordination procedures are defined in detail. Plans are communicated and periodically tested.
Identification	Incidents are assessed and classified according to Incident Classification criteria defined in the Wood Mackenzie incident response policy. The appropriate teams are activated and investigate the incident including collecting evidence and performing root-cause analysis.
Containment	Approaches are defined and deployed to limit the impact of the incident. This includes limiting the incident to affected hosts and affected assets and providing notification in accordance with applicable laws and contractual obligations.
Eradication	The root cause of the incident is identified. As appropriate, affected systems are removed from production environment, any malware is securely removed, systems are hardened and patched, and updates are applied.
Recovery	Affected systems and devices are restored and returned to the business environment in a manner that ensures no threat remains.
Lessons Learned	Analysis is performed to ultimately learn from incident and potentially improve future response efforts and incident documentation is completed.

Business Continuity Program (BCP)

Wood Mackenzie has established a BCP consisting of policy and supporting procedures to protect the safety of Wood Mackenzie personnel, guests, and business partners, and to enable the timely recovery of services and information systems to conform to business management, regulatory, and customer requirements. BCP components include:

- Crisis management plans
- Emergency response plans
- Risk and vulnerability assessments

- Business impact analysis
- Business continuity planning
- Pandemic plans

Data Backup

All Wood Mackenzie businesses and functional areas create and manage a data backup plan to fulfill BCP and disaster recovery requirements in accordance with the Wood Mackenzie Business Continuity Management Policy and applicable laws and regulations.

Vulnerability Management and Patching

The end-to-end process is detailed below, whereby patch listing releases are reconciled and managed on a continuous basis to avoid security decay. New alerts are managed through threat intelligence and risk assessment processes to enable most appropriate updates and operational requirements are met.

Process Phases Summary:

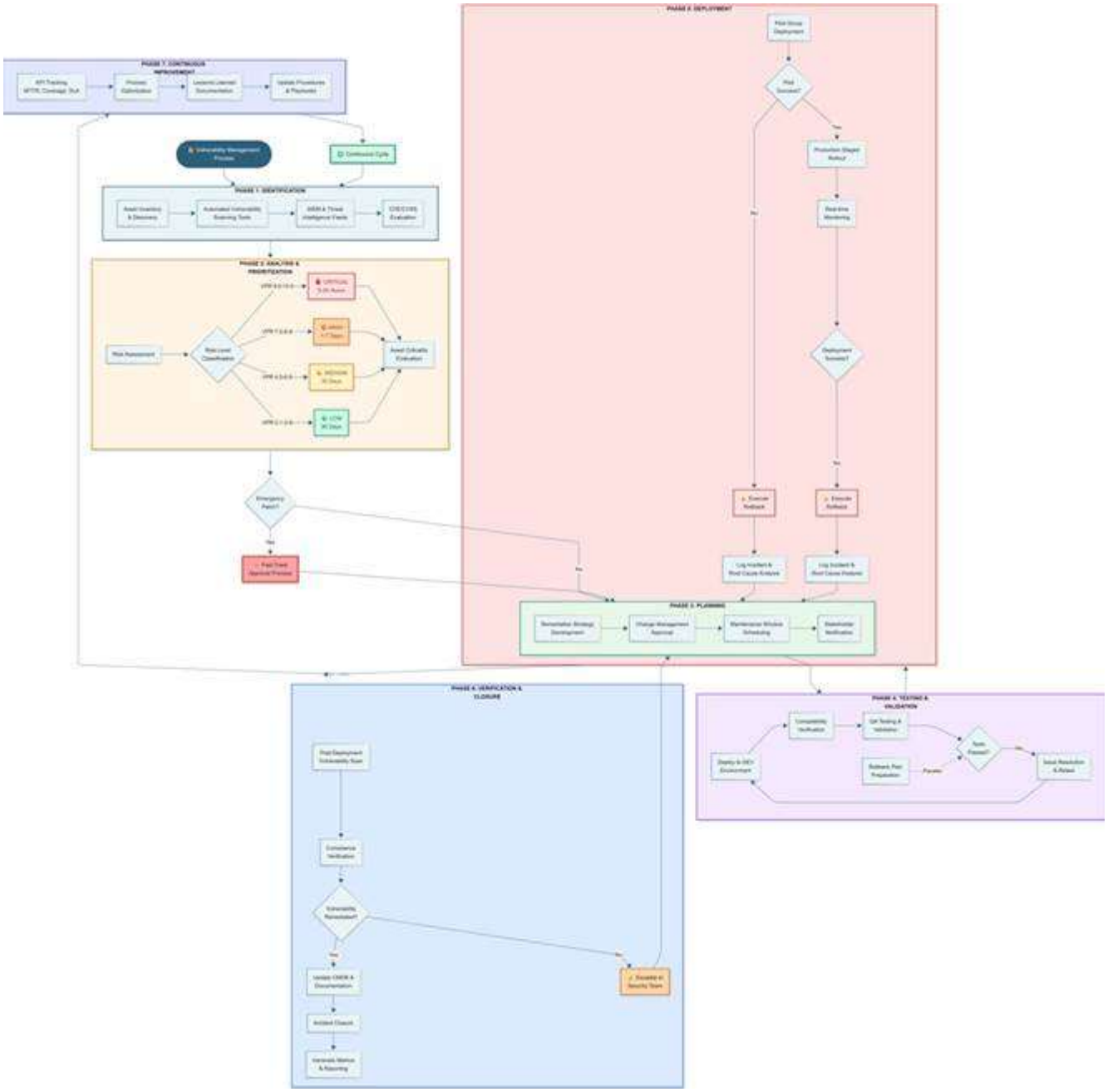
1. Identification
2. Analysis & Prioritization
3. Planning
4. Testing and validation
5. Deployment
6. Verification & Closure
7. Continuous Improvement

Regular monitoring for vendor security updates and utilizing industry RSS feeds and sites to understand possible exposures and news of security alerts are performed. All patch fixes are regression tested within a production replicated (but non-production operated) environment prior to patching or applying fix.

Software Inventory is tracked to ensure vulnerabilities and patches are identified and addressed in line with requirements and prioritization. Vulnerabilities are risk assessed against Tenable VRP scoring and CVSS.

Our continuous vulnerability management process ensures we remediate based on risk in order to prioritize action and minimize the window of opportunity on any vulnerability.

Vulnerability Management & Patching Process (Use zoom to see details)



Appendix 1 Information Security Policy Framework – Summary of all related policies and procedures

Overview

The Wood Mackenzie Information Security Policy Framework establishes fundamental principles for protecting Wood Mackenzie's information resources, ensuring compliance with internal and external regulations, and upholding client reputation. This Appendix summarizes all of our key Security Policies.

Scope of security policies

Applies to: - All employees (full and part-time) and contractors across Wood Mackenzie and affiliates - All Wood Mackenzie information (physical, electronic, cloud-based) - All locations and vendor/cloud service providers

Core Policy Framework

Data Protection & Privacy

- **Data Classification**: Classify all data by sensitivity and apply appropriate security controls
- **Workforce Information Handling**: Protect personal workforce data per privacy standards
- **Data Destruction & Disposal**: NIST 800-88 compliant sanitization procedures
- **Data Storage & Archiving**: Periodic backups with approved systems per regulatory requirements
- **Clean Desk**: Remove sensitive materials from workspaces when not in use

Access & Identity Management

- **Identity & Access Management**: Principle of least privilege; unique user IDs; periodic access reviews; multi-factor authentication
- **Acceptable Use**: Systems for business purposes only; no unauthorized software or streaming services
- **BYOD Standards**: Secure personal device usage with mandatory company policy compliance

Infrastructure Security

- **Physical Security**: Control physical access to facilities, data centers, and storage facilities; video surveillance
- **Network Security**: Firewalls, authentication, encryption, network segmentation; business communications only
- **Wireless Networking**: Approved equipment only; segmented networks with authentication; rogue access points prohibited
- **Cloud Services**: Requires SARB (Security Architecture Review Board) approval; must adhere to all security policies
- **Mobile Communications**: Subject to Mobile Device Policy; theft or loss = security incident requiring immediate reporting

Technical Controls

- **Encryption**: Required per data classification and regulatory/contractual requirements
- **Database Security**: Protect sensitive data; unique DBA accounts; comprehensive inventory; vendor-supported versions
- **Vulnerability & Patch Management**: Continuous monitoring of vulnerabilities; controlled patch deployment per defined lifecycle
- **Configuration Management**: Industry baseline security configurations for all system components
- **Security Logging & Monitoring**: Maintain logs for detection/investigation; protect against tampering; time synchronization
- **Software Use & Virus Protection**: EDR (Endpoint Detection and Response) software mandatory on all workstations; no disabling

Development & Operations

- **Secure Development**: Security integrated into systems development lifecycle; separate dev/test from production environments
- **Asset Management**: All assets documented in centralized CMDB with designated owners
- **Backup Management**: Regular backups per business requirements and applicable regulations
- **Business Continuity Management**: Formal contingency plans for critical business processes

Risk & Incident Management

- **Risk Management**: Annual risk assessments; assessments after significant changes; documented risk acceptances/mitigations
- **Incident Management**: Monitor, identify, respond to, and remediate security incidents; mandatory reporting by all individuals
- **Third-Party Risk Management**: Security requirements for all vendors; regular monitoring, audits, and due diligence

Awareness & Training

- **Security Education & Awareness**: Training upon hiring and periodically; role-based training for security responsibilities

Compliance Requirements

Wood Mackenzie must comply with applicable federal, state, and local laws including:

- **GDPR** (General Data Protection Regulation)
- **CCPA** (California Consumer Privacy Act)
- **HIPAA** (Health Insurance Portability and Accountability Act)
- **PCI DSS** (Payment Card Industry Data Security Standard)
- **GLBA** (Gramm-Leach-Bliley Act)
- **FCRA** (Fair Credit Reporting Act)

Compliance Assurance: - Independent compliance reviews conducted regularly - Protection of PII (Personally Identifiable Information) - Protection of PHI (Protected Health Information) - Safeguarding of Wood Mackenzie Intellectual Property - Confidentiality, integrity, and availability of information systems

Exceptions & Enforcement

Control Exceptions and Risk Acceptance (CERA)

Policy Control Exceptions and Risk Acceptance require formal approval: - Standard/Medium Risk: Business Unit Head and Top Risk owner approval required - High Risk: Compliance Council/ERMC (Enterprise Risk Management Committee) approval required
Exceptions documented per Wood Mackenzie Risk Policy requirements.

Enforcement

- Violations may result in disciplinary action **up to and including termination of employment**
- Access to Wood Mackenzie systems is a **privilege, not a right**
- Access may be revoked or suspended at any time
- All activities subject to monitoring and examination

Key Governance Bodies

Compliance Council

- Chairs: Head of Compliance
- Provides guidance and authority for enforcement
- Approves control exceptions and risk acceptances
- Oversees enterprise-wide risk management framework

Security Council

- Members: Legal, Compliance, Data, and Security teams
- Ensures Information Security Policies are adopted and followed
- Meets formally on a monthly basis

Wood Mackenzie Workforce

- All employees and contractors responsible for compliance
- Must report security breaches (actual or suspected) immediately
- Report to: Business owner management and/or Help Desk
- Take reasonable steps to protect all systems and data

Key Principles & General Disclosure

☑ **Company Property**: All programs, data, and documentation are Wood Mackenzie property
☑ **No Privacy Expectation**: No expectation of privacy regarding system access, e-mail, or Internet activity
☑ **Monitoring Rights**: Wood Mackenzie reserves the right to examine all information on its systems
☑ **Data Protection**: Protect data from accidental or intentional damage, modification, destruction, or unauthorized disclosure
☑ **Immediate Reporting**: Report all security incidents immediately to security@woodmac.com
☑ **Confidential Treatment**: Treat all PII, PHI, and proprietary information as confidential unless authorized
☑ **Data Integrity**: Ensure data integrity, reliability, and availability per security policies
☑ **Annual Review**: Policies reviewed annually by Cyber Security Team
☑ **Upon Separation**: All data must be returned intact upon employment separation

Policy Review & Updates

Review Frequency: - Annual review by designated policy owners from Cyber Security Team - Review after any significant organizational or infrastructure changes - Assessment addresses development, implementation, maintenance, and dissemination

Contact Information

Policies Owner: Graeme Marsh, Head of Cyber Security

Summary of Critical Requirements

Compulsory Immediate Actions Required:

1. ☑ **Complete security awareness training upon hiring**
2. ☑ **Acknowledge and adhere to Information Security Policy Framework**
3. ☑ **Use systems only for authorized business purposes**
4. ☑ **Protect credentials and maintain unique user IDs**
5. ☑ **Report security incidents immediately**
6. ☑ **Maintain clean desk policy for sensitive information**
7. ☑ **Ensure EDR software remains active on all workstations**
8. ☑ **Classify and handle data according to sensitivity levels**

Prohibited Activities:

- ❌ Unauthorized software installation or use of unlicensed software
- ❌ Personal use of company systems for non-business purposes
- ❌ Disabling EDR/antivirus software
- ❌ Sharing credentials or using shared accounts
- ❌ Opening cloud service accounts without SARB approval
- ❌ Installing rogue wireless access points
- ❌ Using Wi-Fi hotspot functionality in office spaces without approval
- ❌ Instant messaging outside Wood Mackenzie Network
- ❌ Removing computer assets from Wood Mackenzie locations without authorization

Mandatory Reporting:

- Security breaches or suspected breaches
- Malware incidents or suspicious activity
- Loss or theft of mobile devices or company assets
- Unauthorized access attempts
- Data breaches or potential data exposure

Security Policy Framework

Policy Governance

Policy Owner:	Graeme Marsh, Head of Cyber Security
Applicable:	Internal and External
Classification:	[Public Policy]
Last updated:	July 2026
Additional information:	N/A

Strictly Private & Confidential

These materials, including any updates to them, are published by and remain subject to the copyright of the Wood Mackenzie group ("Wood Mackenzie"), or its third-party licensors (“Licensors”) as relevant. This document contains Business Confidential Information which is for Internal Use Only and should not be shared with third parties. Sharing this document requires prior approval from Wood Mackenzie’s Legal Department.

Copyright © 2026, Wood Mackenzie Limited. All rights reserved.

Wood Mackenzie™ is a trusted provider of data, analytics and insights, establishing us as the global research and consultancy business powering the natural resources industry. Our dedicated oil, gas & LNG, power & renewables, chemicals, and metals & mining sector teams are located around the world, giving our clients first-mover advantage. For more information visit: **woodmac.com**

WOOD MACKENZIE is a trademark of Wood Mackenzie Limited and is the subject of trademark registrations and/or applications in the European Community, the USA and other countries around the world.

Europe: +44 131 243 4400
Americas: +1 713 470 1600
Asia Pacific: +65 6518 0800
Email: contactus@woodmac.com
Website: www.woodmac.com

Wood Mackenzie