IT Risk Management Policy

The Wood IT risk management framework identifies and assesses digital, information and technology security risk to enable awareness, prioritization, decision making and mitigation. A 'security by design' approach is applied to identify business needs regarding operations, information security and business continuity. Risk management is applied to support an effective and robust security posture.

Purpose:

The purpose of this IT risk management policy is to clearly define Wood's approach to the management of its information and digital technology risks. Risk assessments are used to identify threats, vulnerabilities and to determine the likelihood and magnitude of harm that could come to an information asset, and Wood as an organisation. By determining the risk exposure, Wood will be in a better position to decide how much of that risk should be mitigated and what controls should be used to achieve that mitigation.

Scope:

This policy and its supporting controls, processes and procedures apply to:

- All information assets owned by Wood.
- All workers and includes employees and contingent workers, non-Wood workers including contractors, joint ventures, third parties, or other agents (hereafter referred to as "user") engaged by Wood worldwide.

The application of this policy is mandatory and should be understood and, where appropriate, followed by the group's joint ventures. Where these policies are not followed, this should be reported to the IT SVP Centre of Excellence.

Risk management is a continual process. During the operational delivery and maintenance of the services in scope, there will be many instances where risk management and risk assessment activities will be necessary. These include but are not limited to the following:

- Cyber security
- Identity, authentication, and access management
- Data protection policies, procedures, and systems
- Legal and Regulatory compliance
- All data, IT assets, applications and systems owned or managed by Wood
- IT software development and data management life cycle
- Change and release management
- Enterprise and Systems Architecture
- Third Party management
- IT Business Continuity, Incident Response and Disaster Recovery
- Host Security
- IT Infrastructure and Operations

Some information assets may necessitate the use of specific regulatory standards to mitigate risk and achieve compliance.

Policy Requirements:

IT Risk Ownership

- All operational, tactical, and strategic IT risks are assigned to the accountable IT VP, known as the Risk Approver and their authorised delegate known as the Risk Owner. The owner(s) have ultimate responsibility for controls, risk treatment, review or response and scheduled updates as well as assigning activities associated with risk treatment plans to relevant responsible parties.
- The Risk and Compliance (RC) manager is responsible for supporting the Risk Owners as well as tracking action plans and validating control effectiveness to mitigate risk within current IT risk appetite and tolerance levels.
- The RC manager is accountable for monitoring and reporting to the ITLT on all IT risks.
- The control operator is the person or group who manage the control required to mitigate risks responsible for developing, managing, and completing IT risk treatment plans in accordance with the appetite, tolerance and risk decision applied by the risk owner.
- The risk owner may depend on, or assign tasks to, other responsible parties inside or outside of Wood. Those dependences will be documented in the IT risk register or related action plans as required.
- The responsible party is the specific individual assigned the duty of ensuring that activities are completed successfully by the control owner.

IT Risk Management

- Risk assessments must be performed on all information assets that house, process, transfer, or access Wood-controlled information and address unauthorised access, use, disclosure, disruption,

modification, and/or destruction of information or the information system.

- Risk assessments must identify known potential threats, vulnerabilities, existing controls to determine the likelihood of their occurrence and the magnitude of the impact of those threats should they occur.
- Risk assessments must be performed as follows:
  - If the asset is owned/operated by Wood, upon initial acquisition of an information system.
  - If the asset is owned/operated by a third party on behalf of Wood, prior to initial establishment of service agreements.
  - Existing risks are reviewed where required, or whenever a significant change is made to the asset or its controls, whichever comes first.
- The RC manager is accountable for ensuring that IT identifies, and documents risks in the IT risk register and supports IT activities to identify threats, vulnerabilities, risk impact and likelihood required for the assessment of risk.
- The IT risk approver is accountable for determining the appetite and tolerance for all risks documented on the IT risk register.
- Risk assessments must be conducted by the responsible party who have appropriate knowledge and understanding of the risk/control being assessed as determined by the risk owner.
- The risk approver, in consultation with the IT Leadership Team (ITLT) and Chief Information Officer (CIO), is accountable for all risks assigned to their function and will decide if the risk will be treated, transferred, terminated, or tolerated.
- All action plans must be documented and kept up to date in the IT risk register by relevant action owners.
- Risk action plans must be monitored, tracked to ensure they are completed and assessed to assure IT controls are improved and or remain effective after the action plan is implemented.

Definitions:

Information Assets - Any Wood or customer information that is essential to an organisation's business and therefore needs to be protected appropriately. Information assets includes hardware (including desktop, laptop, tablet computers and mobile devices), software (both purchased and licensed but also freeware), information (not limited to electronic media such as databases, websites, electronic files but also paper and other forms including unrepresented information in the form of knowledge of the employees).

Reference Documents:

- IT Acceptable Use Policy
- Information Security Policy
- IT Risk Management Procedure
- IT External Compliance Landscape

Name	Stephen Brooks
Position	SVP IT Centre of Excellence
Date	22 July 2024