P2012 - Risk Management Policy

Contents

Purpose:

The purpose of this policy is to help ensure Integrity Marketing Group ("Integrity") has a consistent basis for measuring, controlling, monitoring, and reporting risk across the organization. This policy is a formal acknowledgement of Integrity's commitment to Risk Management.

Scope:

This policy applies to all processes, procedures, and technologies in Integrity's business environment, and all associated risks.

Statement:

Roles & Responsibilities

Integrity Security Governance Committee: The Integrity Security Governance Committee is responsible for the development, implementation, maintenance, and enforcement of this policy.

Integrity IT: The Integrity IT team is responsible for assuming the role of Risk Manager and is responsible for collecting input from periodic risk assessments, the organization's threat and vulnerability activities, and other internal processes to identify all security risks facing the organization. Taking into account Integrity's business needs, the Integrity IT team must also collaborate with the Security Governance Committee to develop the company's organizational risk tolerance. In addition to identifying sources of security risk, Integrity IT must track previously identified risks in a risk register.

Business Unit IT: Business Unit IT Teams are responsible for conducting any security risk assessments delegated to them by the Information Security Governance Committee, the Chief Compliance Officer, or the Integrity IT team as necessary.

Policy Statement

Risk Management is an integral part of Integrity's decision-making process for all areas of information security and is incorporated within the strategic and operational planning processes at all levels across the organization.

Risk assessments must be conducted on all new projects, systems, and vendors to ensure that the resulting exposure to additional risk is acceptable and formally approved before onboarding. Risk assessments must also be performed periodically for existing technologies to confirm that the organization's entire threat landscape and risk profile are understood. All risk assessment responsibilities are delegated by the Integrity IT team.

The Integrity IT team is also responsible for collecting risk information from the company's broader security processes. This includes information provided by threat intelligence, vulnerability management activities, and lessons learned from past incidents or incident simulations.

Risk register items guide the Integrity IT team in advising the Information Security Governance Committee and help to provide a complete picture of the company's risk profile. Risk assessment results are also used to determine potential security improvements that align with Integrity's business needs and risk tolerance.

Each identified risk must be analyzed to understand its potential impact and provide input and guidance for deciding on the most appropriate form of remediation or mitigation. Upon completion of the analysis phase, the Security Team provides the Integrity IT team with recommended steps to remediate identified risks. In the event a decision is made to forgo remediation efforts, acceptance of an identified risk must be proposed by the Integrity IT team and approved by the Information Security Governance Committee.

The risk register will guide efforts to remediate or mitigate risks with the intent to reach acceptable levels of risk for any project, system, or vendor. Final decisions on risk mitigation plans or acceptance of residual risks must be made either by the Information Security Governance Committee or by the Integrity IT team, if delegated. These decisions are also tracked in the risk register.

Risk*: The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, given the potential impact of a threat and the likelihood of that threat occurring.

Risk Register: A comprehensive list of identified risks facing the organization, including suggestions for mitigation and all progress made towards remediation or mitigation.

Policy Sections:

Policy Compliance

Section Name: Policy Compliance

Statement:

Compliance Measurement

The Integrity Security Governance Committee will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Integrity Security Governance Committee in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A contractor found to have violated this policy may be subject to an immediate termination of the right to access Integrity's systems and may also include the termination of Integrity's engagement with the contractor's employer.

Policy References:

Document Name	Category	Document Author	Document Owner
P2002 - Asset Management	2000 - Information Technology	Jeremy Hart	Matthew R Williams
P2004 - Data Classification Policy	2000 - Information Technology	Matthew R Williams	Matthew R Williams

P2012 - Risk Management Policy		
Document Author	**Name:** **Title:** **Email:**	Matthew R Williams Senior Director, Cybersecurity & Cloud Engineering, CISO matthew.williams@integrity.com
Document Owner	**Name:** **Title:** **Email:** **Approved Date:**	Matthew R Williams Senior Director, Cybersecurity & Cloud Engineering, CISO matthew.williams@integrity.com 1/30/2025
Legal Management Approval	**Name:** **Title:** **Email:** **Approved Date:**	Duncan William McQueen Assistant General Counsel duncan.mcqueen@integrity.com 3/27/2025
Executive Management Approval	**Name:** **Title:** **Email:** **Approved Date:**	Harsh Singla Chief Technology Officer Harsh.Singla@integrity.com 4/8/2025

Last Published Date: 4/8/2025

Document Version Number 2.0