1. Purpose and Scope

The purpose of this policy is to document the basic principles and policies that are fundamental to Brink's Global Technology in accordance with industry best practices. The policy assists in the following:

- Promote a secure and stable technology environment
- Managing and decreasing the risk of exposure and compromise
- Protecting and maintaining the confidentiality, integrity, and availability of digital information and related infrastructure assets

Additionally, the policy provides the basic boundaries for more detailed procedures and standards. In the event of a conflict between these policies and applicable law, applicable law will take precedent.

This policy applies globally to all Brink's legal entities, employees, contractors, and vendors doing business on behalf of Brink's.

The scope of this policy is to:

- Define risk management as it relates to Global IT
- Provide a global IT framework for measuring and controlling risk
- Manage and reduce risk exposure of control failures
- Enable confidentiality, integrity, and availability of digital information and related infrastructure assets
- Identify critical support activities, including, but not limited to:
    - cadence of periodic risk assessments
    - annual policy reviews and updates
    - reporting policy exceptions and training

2. Policy Statement

2.1 Global IT Risk Management defines Risk Management as the ongoing process of identifying, assessing, and responding to risk. To manage risk, Brink's should understand the likelihood that an event will occur and the potential resulting impacts. With this information, Brink's can determine the acceptable level of risk for achieving organizational objectives and can express this risk tolerance. With an understanding of risk tolerance, Brink's can prioritize cybersecurity activities, enabling Brink's to make informed decisions about cybersecurity expenditures. Implementation of risk management programs offers Brink's the ability to quantify and communicate adjustments to their cybersecurity programs. Brink's may choose to handle risk in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery of critical services. The Framework uses risk management processes to enable Brink's to inform and prioritize decisions regarding IT Risk.

2.2 The goal of Global IT Risk Management is not to eliminate all risk but to enable Brink's to identify, prioritize, manage, mitigate, and respond to risks in the IT environment while protecting the confidentiality, integrity and availability of information and services provided.

2.3 Risk Assessment Framework

Brink's current state of IT organization is assessed against each identified IT Risk/Threat based on the below risk assessment process:

2.3.1. Once the risk has been identified and reported, the Global IT Risk Management Team conducts an assessment to determine the risk level and priority based on the CIA (Confidentiality Integrity and Availability) method. If an M&A, a new project, or an enhancement to our current IT environment, the Risk Management (RM) team conducts a risk assessment to determine the risk level and priority based on the CIA (Confidentiality Integrity and Availability) of the controls through the use of an Information Security questionnaire (Cloud or SIG LITE) and reviewing the audits or compliance reports (for example SOX, SOC1 / SOC2, SAE-3402, etc.) documentation provided by the M&A, a new project, or an enhancement to our current IT environment to ensure that it is in alignment with Brinks IT controls, and to ensure that there are effective controls in place. Additionally, the Risk Management team will ensure that evidence is in place for validation.
2.3.2. The risk assessment and analysis determine the rating of an identified risk. The risk rating determines the impact and likelihood of the risk to IT processes/operations.
2.3.3. Risks are put into a Heat Map to orient the risk in relation to others identified. The measurement of risk (and scale) is outlined in the Risk Management Procedures. Risks rated as Tier 1 or Tier 2 will be monitored annually by the Global IT Risk Management Team.

2.4. These Risk Categories are included in the Risk Register and Risk Reporting:

- Financial
- Reputation
- Legal
- Regulatory Compliance
- Data (includes but not limited to protection and privacy)
- Client Impact

2.5. Exceptions to this policy must follow the Global Technology Policy Exception Process and Procedure.

2.6. Training and Awareness:

2.6.1. The Global IT Risk Management Team offers training and awareness of this policy, as needed / requested to the first line of defense.

3. Roles and Responsibilities

3.1. Compliance: All employees, contractors and consultants are required to comply with the policies. An employee found to have violated any Brink's policy may be subject to disciplinary action, up to and including termination of employment. If a contractor or vendor violates a Brink's policy, Brink's may pursue its remedies under the contract, including without limitation, termination of the contract. Management should seek guidance from HR and the Legal Department on these issues.

3.2. Global IT Risk Management provides a framework for Brink's to identify, assess/measure, and report global IT risk.

3.3. For implementing the framework for Global IT Risk Management, Brinks outlines the below Roles and Responsibilities in accordance with the three lines of defense:

3.3.1. First Line of Defense:

- **Risk Reporters / Risk Identifiers:** These are the individuals (employees and non-employees) who identify and report a risk event occurring within Brink's processes (Applications, OS, Networks, Database, etc.). Brinks employees/contractors are responsible for identifying and reporting risk events through the risk identification form.

- **Risk Mitigation Owners:** These are the individuals who oversee the mitigation/remediation of identified risks. This means completing a Risk Assessment, Risk Response, Remediation/Action Plan, and Expected Remediation Date. They are also accountable for Risk Implementation (how the Action Plan is implemented).

- **Risk Decision Owners:** These are the individuals who decide whether Brinks accepts the risk, mitigates the risk, or transfers the risk. They are responsible for Risk Implementation, and are accountable for the Risk Assessment, Risk Response Planning and the Action Plan.

3.3.2. Second Line of Defense:

- **Risk Analyst:** These are the individuals who analyze and prioritize the risks identified. They are also responsible for validating the Action Plan and monitoring the risks identified and reported for further action. They are consulted for reporting the risk identified and partner with the first line of defense for any consultation related to the Risk Assessment, Risk Response and Action Plan, and Risk Implementation. They also identify any replicated issues and retire risks.

- Global IT Risk Director**:** This role manages the individuals and the program for IT Risk Management. May also perform risk analyst duties and tasks as needed.

- Global IT Risk and Compliance Sr. Director**:** This is the individual who manages the Risk Analysts, identifies, and clears or escalated any roadblocks and acts as first point of contact for any escalation needed. This individual is accountable for all actions which the Risk Analysts are responsible for.

- Sr. Director, Global IT Governance, Risk and Compliance**:** This is the individual who supports the Senior Risk and Compliance Manager by clearing roadblocks and acting as the second point of contact for any escalation needed. They act as a consultant and final decision maker regarding all Risk Management Program (process, people, and system) issues.

- **IT Risk Committee:** These stakeholders are regularly informed on all risks reported and any actions taken thereof. They are responsible for any unresolved escalated risk events. They advise the board of any risk strategy, address any risk issues, and monitor reported risk (or risk exposures). They assist the Global IT Risk Management Team with providing resources or removing roadblocks to implement the Remediation Plan.

3.3.3. Third Line of Defense:

- **The Auditors:** These individuals are responsible for reviewing and assessing the Global IT Risk Management Program (process, policy, procedure, and as applicable risk events) and reporting the results to leadership and the board. They examine the operational effectiveness and determine further risk exposure. As the third line of defense, they review evidence provided by the first line of defense to check for compliance with the Global IT Risk Management policy and external regulation.

- **Board of Directors:** These individuals are to be informed on all risks reported, and any actions taken thereof.

4. References

4.1. Principles: see GITP-001 Global Technology Policy Manual Principles document.

4.2. Related:

Risk Management Procedure
Global IT Risk Program Framework
GITP-027 Global Technology Third Party Vendor Risk Management Policy
Risk Identification Form (https://customerportal.brinksinc.com/en/web/brinks-resource-library/global-it-risk-management)

5. Definitions

5.1. Risk Register = the list of all identified risks with relevant controls and management response plans.

5.2. Risk Reporting = the process of reporting key identified risk to drive responsibility and accountability, and to bring awareness to Brink's IT senior leaders, ERM, IT Risk Committee, the board of directors, and the third line of defense. A risk response will also be provided as applicable.

6. Authorization

This policy is authorized by:

Patrick Benoit
Chief Information Security Officer

Policy Owner: Mark Armour, Sr. Director, Global IT Governance, Risk and Compliance

Additional Stakeholders: Miguel Araya, Global IT Risk Director
Lanre Lawson, Global IT Risk and Compliance Sr. Director
Jeff Gibson, Sr. Director Global IT

Rob Butcher, IT Engineering
Chris Foley, IT Operations
Sapna Thakor, Director Global IT Project Management Office

7. Change History

Revision	Date	Author	Revision History
1.0	08/26/2022	Carrie Rogers	Draft moved to current policy template
1.0	10/17/2022	Carrie Rogers	Update to template and Section 6
1.0	10/21/2022	Mark Armour	Review and updates
1.0	04/03/2023	Carrie Rogers	Review of final draft and updates
1.0	04/04/2023	Mark Armour	Review of final draft and updates
1.0	04/05/2023	Miguel Araya/ Lanre Lawson	Review of final draft and updates
1.0	04/07/2023	Jeff Gibson / Sapna Thakor	Review and Feedback
1.0	04/11/2023	Mark Armour / Carrie Rogers	Review and updates
1.0	04/13/2023	Patrick Benoit	Review, updates, and approval
1.0	04/25/2023	Hal Snedden	Review and Feedback
1.0	04/26/2023	Carrie Rogers/Lanre Lawson/Miguel Araya	Review and Updates
1.0	4/26/2023	Hal Snedden	Review and approval
1.0	05/12/2023	Mark Armour	Updated verbiage to 2.3.1.