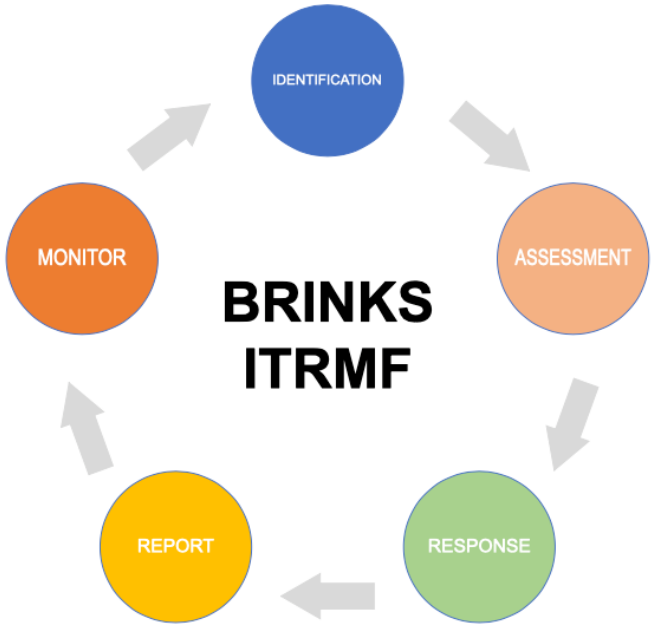
Contents

Objective

The objective of Global IT Risk Management is to manage and decrease the risk of exposure and compromise, while maintaining the confidentiality, integrity, and availability of digital information and related infrastructure assets.

This document will outline the Risk IT Management Framework (ITRMF) and the steps in the procedure to identify, assess, respond, and monitor IT risk.

Brinks ITRMF



Scope

This procedure document outlines:

- Roles and Responsibilities and RACI Matrix
- Strategic Level Process Flow: Confidentiality, Integrity, and Availability (CIA):
  - Risk Identification
  - Risk Analysis
  - Risk Assessment (Impact/Likelihood)
  - Risk Prioritization (Risk Heat Map)
  - Risk Response
  - Risk Plan Validation
  - Risk Implementation
  - Risk Reporting
  - Risk Monitoring
- The Risk Statement (Risk Categories)

- Risk Management related to IT Third Parties (Vendors)
- Risk Management related to Mergers and Acquisitions (M&A)
- Risk Management related to Divestiture
- Risk Management Training

Roles and Responsibilities

Line of Defense	Role	Responsibility
All Lines of Defense	Risk Reporters / Risk Identifiers	These are the individuals (employees and nonemployees) 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.
First Line of Defense	Risk Mitigation Owners	These are the individuals (IT asset owners, IT Support Teams (Servers teams, Database teams, Network teams, etc.) who oversee the mitigation/remediation of risk identified and reported. They are responsible for completing a Risk Assessment in partnership with Global IT Risk Management (as applicable). They are also responsible for completing the Risk Response, Remediation/Action Plan, and Expected Remediation Date. They are accountable for how the Action Plan is implemented.
First Line of Defense	Risk Decision Owners	These are the individuals (Business owners, Applications Owners, Regional IT Leaders, IT/Business Service Owners, etc.) who oversee the Risk decision for all risks identified and reported in their area. They decide whether Brinks accepts the risk, mitigates the risk, or transfers the risk. They are responsible for the implementation

		and are accountable for the Risk Assessment (in partnership with Global IT Risk Management as applicable). They are also accountable for Risk Response Planning and the Action Plan.
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 to re-assess or re-respond as needed. They are consulted for reporting the risk identified. They also 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.
Second Line of Defense	Risk Manager	This is the individual who support and manage the risk analyst team, is responsible of coordinate task and resources to prioritize the risk, report the risk, validation of remediation plan, monitor (re-assess risk) identifies any roadblocks in their activities and acts as first point of contact for any escalation needed. Partner with the Senior Director, Risk and Compliance and Remediation team leads. This individual is accountable for all actions which the Risk Analysts are responsible for.
Second Line of Defense	Senior Director, Risk and Compliance	This is the individual who manages the Risk Analysts, identifies any roadblocks in their activities and acts as first point of contact for any escalation needed. This individual is accountable for all actions which the Risk Manager are responsible for.

Second Line of Defense	Senior Director, Governance Risk and Compliance	This individual is the Senior Leader for Governance, Risk and Compliance Team. They identify any roadblocks in the team's activities and act as the second point of contact for any escalation needed. They also act as a consultant and final decision maker regarding all Risk Management Program (process, people, and system) issues.
Second Line of Defense	IT Risk Committee	These individuals (Regional IT Leaders, IT-GSS Leaders, ERM leadership, etc.) are the group of stakeholders who should be 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, and resolve any roadblocks for implementation of the Remediation Plan.
	IT Compliance/ IT Governance	These are the individuals who will be consulted during the Risk Assessment stage. Their input will be key to provide a better identification, analysis and prioritization of the risks identified. They are also will be informed on any new controls to be implemented or failed controls, policy exceptions (IT governance).
Third Line of Defense	The Auditors	These individuals (Internal /External Auditors), are responsible for reviewing and assessing the Global IT Risk Management Program (process, policy, procedure and as applicable risk events). 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.
Third Line of Defense	Board of Directors	These individuals are to be informed on all risks reported, and any actions taken thereof.

RACI Matrix

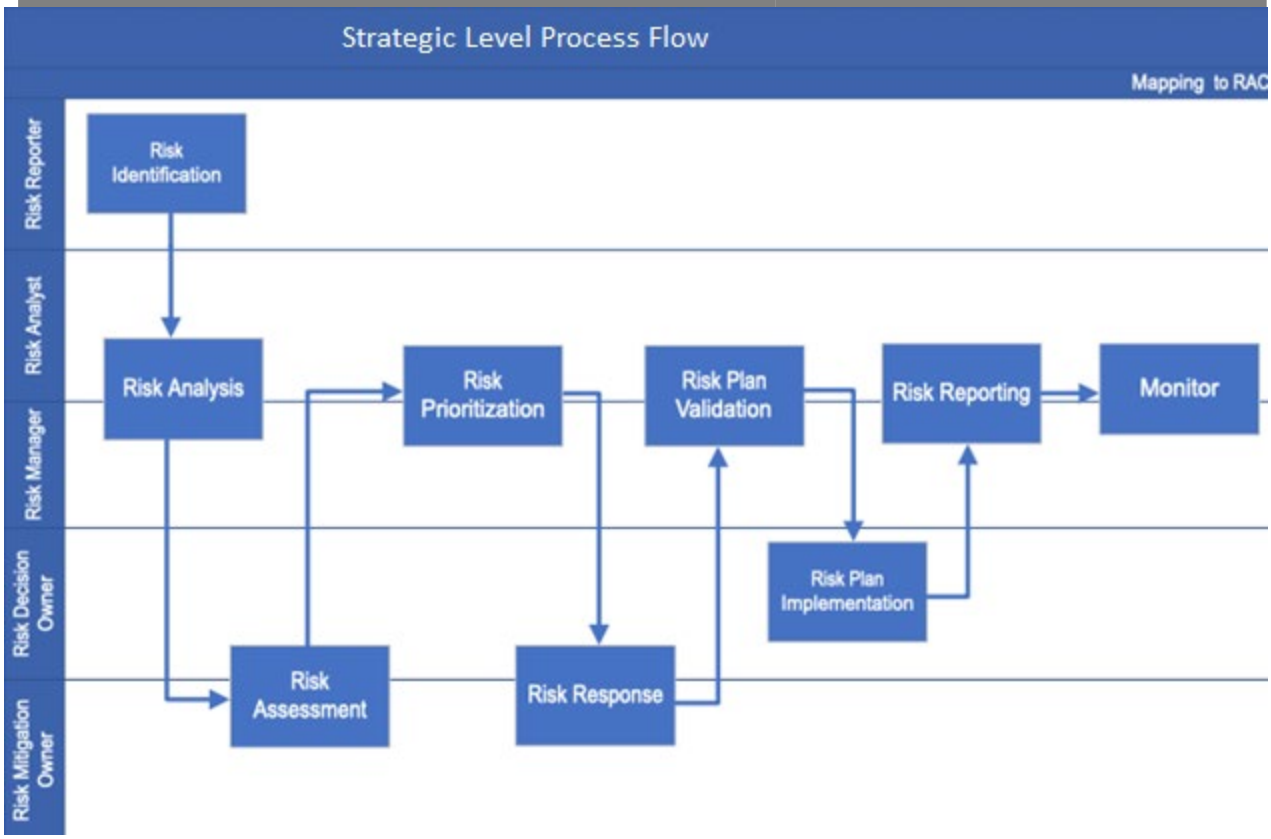
Below is the RACI Matrix (the responsibility matrix) that provides a high level description of the strategic tasks/activities mapped to the various roles.

Activities	Risk Reporter/Identifier (anyone)	Risk Manager	Risk Analyst	IT Risk Committee	Risk Mitigation Owner	Risk Decision Owner	GRC Director	IT Compliance	IT Governance
Risk Identification	A	C	C	I	I	I	I	I	I
Risk Analysis	C	A	R	I	I	I	I	I	I
Risk Assessment - (RCSA)	C	C/I	C/I	I	R	A	I	C	C
Prioritize the Risk	C	A	R	I/C	I/C	I/C	C/I	I	I
Risk Response Planning and Action Plan	C	C/I	C/I	I	R	A	C/I	I	I
Validate Plan	C	A	R	I/C	I/C	I/C	C/I	I	I
Risk Implementation (Action Plan - Implemented)	C	C/I	C/I	I	A	R	C	I	I
Risk Reporting	C	A	R	I	I	I	C/I	I	I
Risk Monitoring (Re-assess/Re-respond) - (Identify replicated issues or Retire Risk)	C	A	R	I	I	C	C	I	I

RACI DEFINITIONS	
R - RESPONSIBLE	The Individual(s)/Team who does the work. At least one person should be responsible for each activity/task/work package. That is, this role is "Responsible" for completing the task or deliverable.
A - ACCOUNTABLE	The Individual/Team ultimately answerable for the successful completion of the activity/task/work package. There should be only one individual/Team accountable for each activity/task. That is, this role "Accountable" has the final accountability for the task's completion.
C - CONSULTED	This is the Individual(s) who provides inputs based on impact or provide their expertise that is subject-matter experts whose input is required as needed. That is, this role "Consulted" is an adviser to a task.
I - INFORMATION	This is the Individual(s) who is kept in loop and progress is provided to. The role "Informed" is kept up to date on task completion, the progress or status updates of the task(s) only as applicable.
R/A/I	Combine Roles
A/C	Combine Roles
C/I	Combine Roles

The Strategic Level Process Flow: Confidentiality, Integrity, and Availability (CIA)

The Brinks Global IT RMF (Risk Management Framework) consists of 5 Main processes. Each one is outlined below.



Risk Identification

This is the first step in the ITRMF, whereby the risks are identified and documented in the system of record by the Risk Identifier/Risk Reporter. The Risk Reporter can be the first, second, or third line of defense, as it is the responsibility of every employee and contractor to report any risks discovered. The Risk Reporter completes the Risk Identification Form.

Risk Analysis

The Risk Analyst reviews and analyzes the risk reported (via the Risk Identification Form) to ensure that it is valid and not a duplicate of another reported risk. They also review the following (but not limited to):

- the system reported,
- the asset and/or data at risk,
- the Owners (Business and Technical),
- the scope of the impact,
- the location of the asset and/or source of risk,
- the line of business impacted

The Risk Analyst will transfer the information to the Risk Register to conduct the Risk Assessment in partnership with the Risk Mitigation Owner. The Risk Analyst uses the Risk Heat Map to

determine the prioritization of the risk reported in comparison to other risks. (See Risk Heat Map under Risk Prioritization).

Risk Statement

When risks are being identified, as part of risk reporting and analysis, a risk statement is associated with each risk. The risk will be categorized as follows:

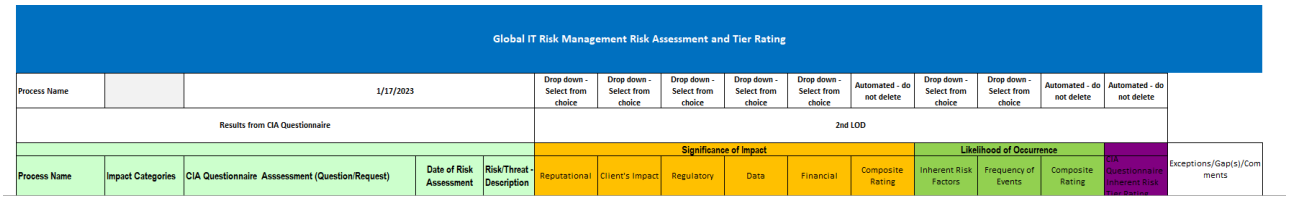
- Financial
- Reputation
- Regulatory
- Data
- Client Impact

The Risk Categories are defined as follows:

Risk Category	Definition
Financial Risk	The risk of Brinks losing money in an endeavor. Examples include, but are not limited to: - Fines or penalties for non-compliance
Reputational Risk	The risk of Brinks suffering from the loss of a good reputation or a devalued brand name. Examples include, but are not limited to: - A stolen and/or misused I.P. (Intellectual Property)
Regulatory Risk	The risk of Brinks failing compliance with standard applicable regulation. Examples include, but are not limited to: - IT Control Failures
Data Risk	The risk of Brinks losing business due to poor data governance or poor data protection. Examples include, but are not limited to: - Loss in data confidentiality, integrity, or availability
Customer Impact	The risk of any of the above risks affecting the clients of Brinks.

Risk Assessment

The objective of the risk assessment is to determine the impact and likelihood of the identified risk. This helps drive the risk response and planning. The assessment of the likelihood is based on occurrences and projected future occurrences. Within the Significance of Impact category, risks are evaluated for impact to reputation, clients, regulatory compliance, data loss or corruption, and financial loss. For Likelihood of Occurrence, this is determined using inherent risk factors and frequency of occurrence. This also defines the risk level as referenced in the Risk Prioritization.



Global IT Risk Management Risk Assessment and Tier Rating																	
Process Name		1/17/2023			Drop down - Select from choice	Drop down - Select from choice	Drop down - Select from choice	Drop down - Select from choice	Drop down - Select from choice	Automated - do not delete	Drop down - Select from choice	Drop down - Select from choice	Automated - do not delete	Automated - do not delete	
Results from CIA Questionnaire					2nd LOD										
					Significance of Impact						Likelihood of Occurrence				
Process Name	Impact Categories	CIA Questionnaire Asssessment (Question/Request)	Date of Risk Assessment	Risk/Threat - Description	Reputational	Client's Impact	Regulatory	Data	Financial	Composite Rating	Inherent Risk Factors	Frequency of Events	Composite Rating	CIA Questionnaire Inherent Risk	Exceptions/Gap(s)/Comments

The Risk Assessment is composed of two questionnaires:

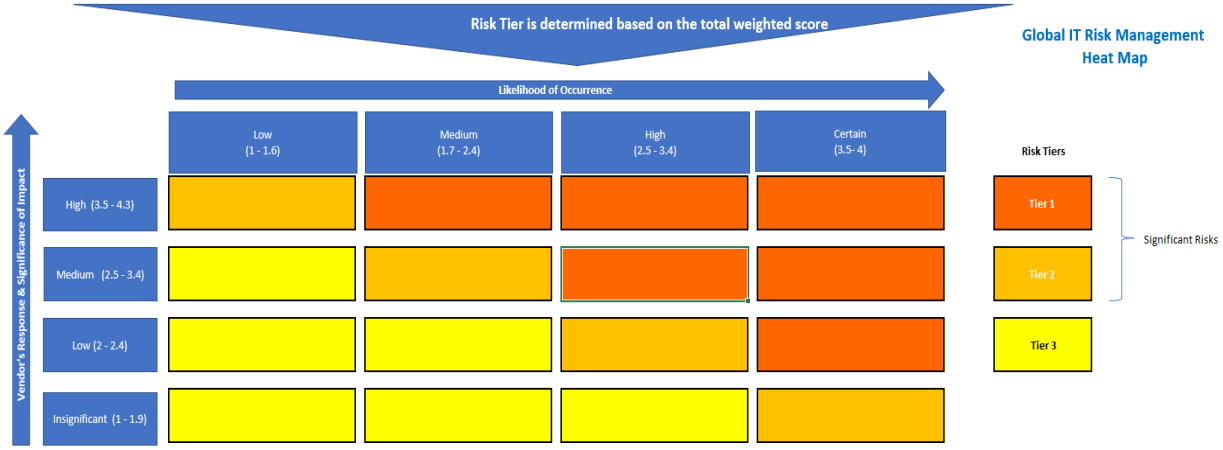
1. The Business/Information Security Questionnaire
2. The Cyber Security Questionnaire

All information in both of these questionnaires will come from the Risk Identification Form (RIF).

Risk Prioritization

Risk Prioritization (also known as the Risk Heat Map) is derived from the Risk Assessment, and orients the risk in relation to other risks reported so that resources can be applied appropriately to the risk priority.

Risk Heat Map:



Risk Response

The Risk Analyst will make recommendations for how Brinks should respond to the risk – whether to Mitigate, Accept, Avoid, or Transfer the risk (see table below):

Response	Description	Owner
Mitigate	Mitigating the risk is where the Risk Mitigating Owner identifies what drives the impact and likelihood of the risk, and makes a recommendation that would reduce the impact and/or likelihood to a more tolerable level. For example, the Risk Mitigating Owner may recommend strengthening a network security gap so that the likelihood of a cybersecurity incident is reduced.	Risk Mitigating Owner
Accept	Accepting the risk is where a business unit notes that the potential benefits of a risk outweigh the potential loss of that risk, or when the loss of the risk is significantly less than the cost of taking action to reduce it. The aim is not to totally eliminate risk. Some risk will be accepted by Brinks.	Risk Decision Owner
Avoid	Risk Avoidance is where the source of the risk is removed such that the risk is removed. If the source of the risk can be removed from the environment, the risks related to that source are eliminated. Additionally, risk avoidance could comprise of providing training and enforcing policies.	Risk Decision Owner
Transfer	Transfer is where the ownership and liability of the risk is moved to a party separate from Brinks. When a risk is transferred, Brinks is no longer responsible for the loss or benefit related to the risk.	Risk Decision Owner

Risk Plan Validation

The Risk Analyst (and/or Risk Manager, as applicable) validates the remediation plan, remediation date, and applicable controls. This includes, but is not limited to:

- Confirming that there has been no impact to any upstream or downstream processes/databases/applications/system/network/controls in the completion of the remediation plan
- Request evidence that the remediation has been completed.
- Setting up meetings to review the remediation/mitigation plans completed (as applicable)
- Challenging the potential sustainability of the plan (as applicable)

Once this has been validated by the Risk Analyst (and/or Risk Manager, as applicable), the remediation status is “closed”.

Risk Plan Implementation

If the Risk response is to mitigate, and the Risk Plan has been validated, the Risk Mitigation owner will follow through the Risk Remediation plan to implementation. This is then reported to the risk management team and to the appropriate stakeholders to ensure that the risk is closed in the risk register.

Risk Reporting

Risk reporting is a proactive approach for managing and communicating risk. To help drive transparency, and bring visibility.

The risk management team provides the risk register to ensure transparency related remediation status, expected remediation date, and risk prioritization (Heat Map) as well as awareness of risks that have been escalated.

After a risk has been identified, assessed, and response prepared, the risk is reported to the appropriate stakeholders. The method by which the risk is reported will be done using the Risk Heat Map for risk prioritization.

This ensures that risk decision owners can organize resources accordingly.

Risk Monitoring

Risk Monitoring is when the mitigating controls (or the risk itself, as applicable) are monitored for any residual risk.

The Global IT Risk Management Team will monitor and report any risks that may have a material impact to the CIA (Confidentiality, Availability, and Integrity) of Brinks data and IT services (such as security incidents, business availability and continuity).

Global IT Third Party Risk Management

Brinks conducts business transactions and services with third parties (vendors). Third Party vendors are responsible for compliance with Brinks IT Third Party Risk Management Policies and Procedures. To ensure that the activities of our vendors comply with our policies, our third party

risk management program is designed to be part of our second line of defense where the following processes are outlined:

- Onboarding
- Third Party Risk Assessment
- Risk Review and Risk Analysis
- Escalation
- Monitoring Risk
- Third Party Remediation, Validation / Response to Risk
- Offboarding and Termination

For more information, please refer to the Global IT Third Party Risk Management Policy and Procedure.

Mergers and Acquisitions - Security Requirements

When Brinks acquires or merges with a new entity, there are specific risks that are to be assessed through due diligence to ensure that Brinks itself is not unsuspectingly put at risk. Potential M&A risks to check for include, but are not limited to:

- Check for undefined implementation processes to bring the new company in compliance with Brinks policy/procedures
- Check for exposure to potential or actual financial losses.
- Check for lack of process controls in place, or lack of process controls that align with Brink's policy
- Check for IP (Intellectual Property) that has been compromised or leaked
    - Additionally, the company's source code must be validated as wholly owned by the company and not a derivative of GPL (or other) source code and/or that proper attribution exists for derivative works.
- Check for the company's credentials or data found on the dark web
- Check for internet-facing systems/infrastructure vulnerable to cybersecurity risk
- Check for sufficient cybersecurity (via the company's Processes and Procedures). This includes:
    - ISO 27001 Information Security Management System
    - Risk Management System with executive sponsorship/ownership of remediation of risk
    - Contractual language with both clients and vendors with respect to cybersecurity
    - A current and accurate CMDB including cloud services, all websites, points of presence, software used in the environment with up to date licenses.
        - Additionally, EOL licenses, platforms and software should be checked. (applications/databases/networks/systems should be updated to a supported version)
    - An Independent verification of security controls by an ISO/IEC 27001:2022 certification, a SOC2 completed within one calendar year of the projected M&A date, and a completed SIG

- Any cloud service providers must be compliant with ISO/IEC 27017:2015, and NIST SP 800-210 and/or NIST SP 800-146
  - Additionally, all data stored or processed in, or transmitted to cloud environments will need to conform to ISO/IEC 27018:2019, NIST 800-53, NIST SP 800-210.
- The company must have no previous, current, or impending litigation or regulatory action (such as, but not limited to GDPR regulatory issues)
- The company must disclose previous, current, or impending security incidents and mitigation actions in place.
  - Additionally, the company must disclose all security incidents reported in the last 12 months and must have an incident management process in place.

- Check for upcoming or expired security certifications/assurances (including, but not limited to third party attestation reports)
- Check for Penetration Testing with unacceptable results, or lack of recent Penetration Testing
- Check for any lack of the company's Security Documentation prior to the M&A (including, but not limited to):
  - IT Controls (ITSOX, SOC 1, and SOC 2) and Control Documentation
  - GDPR compliance documentation
  - PCI certification and compliance documentation
  - PII compliance documentation
  - Additional regulation(s) Brinks would become subject to as part of the M&A
  - Policy and procedures related to Information Security
  - Insurance Policies and policy change history related to:
    - Cybersecurity
    - Data Breach Loss / Data Privacy
    - IT Infrastructure
  - New Hire Provisioning Processes/Procedures for employees and contractors (background investigation and onboarding)
  - Reports and results related to Privacy Impact Assessment
  - Playbooks:
    - Business Resiliency (Disaster Recovery, Business Continuity, and crisis management plans)
    - Incident Response Plans
  - IT Change Management
  - Ensure that secure Software Development Life Cycle Management processes/procedures are in place
    - Ensure that secure coding practices and frameworks are adhered to (for example, NIST SP 800-218)

- Ensure that secure Hardware Development Life Cycle Management processes/procedures are in place
- All licenses (including current and expired) for products that would be acquired by Brinks due to the M&A (including, but not limited to products used for network endpoints, servers, cloud and infrastructure)

Acquisition Phase 1 (implementation and validation)

After the Due Diligence has been completed, and after an assessment of security and vulnerability is conducted, and any risks related to the M&A have been identified, assessed, responded, and reported, check for the following controls that will need to be implemented and monitored:

- Any employees and contractors added during the M&A should be added to the HRIS system and internal network of Brinks.
- Background checks and cybersecurity procedure training should be conducted for any added employees and contractors (as applicable).
- All applications/databases/networks/systems/processes/controls should be added to Brinks inventory in the system of record.
- All applications/databases/networks/systems/processes/controls should be added to the scope of review
- A pen test covering all physical and digital assets of the M&A should be performed (unacceptable Pen Tests must be remediated prior to integration with the Brinks network)
- All added applications/databases/networks/systems should be updated to a supported version to avoid risks related to unsupported versions
- All laptops and servers should have vulnerability management scanning and endpoint security installed
- Firewalls, and other cybersecurity controls should be updated to include the added applications/databases/networks/systems/processes/controls (as applicable)
- The Company should ensure that all applications/databases/networks/systems/processes/controls are aligned to Brinks Policy for IT Compliance, ITSOX, SOC 1, and Internal Audit (as applicable).
- All playbooks, plans, and other Business Resilience (Disaster Recovery, Business Continuity, Crisis Management, etc.) program documentation should be updated to include the added applications/systems (as applicable)

Acquisition Phase 2 (Consolidation and Integration)

After the controls in Phase 1 have been implemented and monitored, if residual risk is discovered, the following additional controls should be consolidated and integrated by Brinks:

- To confirm compliance with Brinks standards, 60 days after integration, Brinks Cybersecurity will need to conduct a post-integration security assessment.
- If the M&A included adding physical and digital assets, an alignment will need to be performed on them. This will ensure alignment with Brinks security posture, including endpoint protection.

- Access to Brinks Networks by endpoint devices will need to only be available via a Brinks approved VPN and security posture check.
- All assets added due to the M&A will need to be connected to Brinks identity providers (including, but not limited to, federated identities).
- All network connections will need to terminate in the Demilitarized Zone (DMZ). They should not terminate directly into Brinks Networks servers.

Divestiture

When Brinks divests one of its entities/resources, there are specific risks that are to be assessed through due diligence related to the divestiture such that Brinks does not unsuspectingly encounter risk. Examples of divestiture related risks include, but are not limited to:

- Data integrity issues related to access rights and identity information
- Proper controls not separated
- Systems not well defined
- New cybersecurity vulnerabilities opened due to the divestiture
- Issues related to improper deprovisioning
- Unplanned IT outages

To mitigate such divestiture-related risks, as part of the IT separation road map, due diligence will be conducted to review which IT Security areas remain within Brinks and which will not. This includes, but is not limited to:

- Asset Management:
  - Data Center shared Environment (the Data center and associated physical plant components)
  - An Asset Inventory updated to cover all Brinks security controls
  - Service-specific hardware infrastructure, to ensure all Brinks security controls are in place during the divestiture process.
  - A control taxonomy including all attested control owners
- Network and Connectivity:
  - Disabled access to the network and communications (LAN-WAN-TELCO), and disabled access to all network connectivity (Links, VPN Tunnels, etc.) after divestiture is completed
  - Validated and cleaned network device configurations and network configurations after divestiture process is completed
  - A control taxonomy including all attested control owners
- Identity Management and Access Management:
  - Remote access management audit and review (user, Systems, API, etc.) to all systems in scope during the divestiture process.
  - Disabled database access (audit and review) to all databases in scope during the divestiture process.
  - Application access following Brinks UAR (User Access Review)
  - Active Directory groups following Brinks UAR (User Access Review)

- A control taxonomy including all attested control owners
- Reviewed and Audited System Logs and access logs for any component that was in scope during the divesture process.

- Vulnerability and Penetration Testing:
  - PT (Penetration Test) on all networks, databases, systems, and devices involved in the divesture process
  - VA (Vulnerability Assessment): on all networks, databases, systems, and devices involved in the divesture process
  - Storage Media Destruction Process and Validation
  - Evidence of Media Destruction or Data erasure and Data retention after the divestiture is completed
  - A control taxonomy including all attested control owners.
- Data Management:
  - Validated PII, GDPR, SOX or PCI data in scope of the divesture process and updates on the Brinks controls taxonomy attested
  - Reviewed and disabled users or configurations made during the divesture process on any database.
- System Integrations:
  - All access (Network and User) assessed for any system in Brinks in scope for the divestiture.
  - Assessed Brinks security controls on any remaining systems in Brinks
- TPRM (Third Party Risk Management) & Risk Management
  - Access revoked from vendors to any Brinks components that were part of the systems or applications in scope of the divestiture process.
  - Validated Vendor Risk pending being transferred to the new organization
  - Reviewed risk pending in the Brinks Risk Register that need closure for all Brinks systems in scope for divestiture before starting the divestiture process.

Training

Training conducted by Global IT Risk Management for IT Regional leaders, service delivery teams and Business operations personnel includes but is not limited to the following topics:

1. Brinks ITRMF and Process
2. Risk Identification Form
3. Risk Assessment Questionnaires fulfilment for IT Owners
4. Risk Assessment Questionnaire fulfilment for C.I.A for Business
5. Accessing the Risk Register
6. Remediation Plans
7. Risk Reporting

Definitions

- **CIA (Confidentiality, Integrity, and Availability):** are the three aspects of data used to guide information security and risk management decisions.
- **First Line of Defense:** are the individuals who work in the day-to-day operations of a company. They are the managers of data and processes, and are therefore the first individuals responsible for identifying a risk.
- **Second Line of Defense:** are the individuals who oversee and assess risk reported by the first line of defense. They do not report assessed risk to the public, but are an internal-focused group in Brinks
- **Third Line of Defense:** are the individuals who oversee risk reported by the first or second line of defense. They are the individuals who inform external stakeholders of discovered risk and remediation steps planned and taken. They are an externally-focused group in Brinks
- **GDPR (General Data Protection Regulation):** is the regulation where the personal data of EU citizens are protected against misuse.
- **PCI DSS (Payment Card Industry Data Security Standard)**: is the regulation where the data of cardholders are protected against misuse.
- **PII (Personal Identifiable Information**): is any information that can be used to directly or indirectly identify an individual.
- **Risk Assessment:** is the evaluation of potential risk that may be involved within an activity of a process flow.
- **Risk Heat Map:** is a graphic representation of the likelihood and impact of risk which drives prioritization
- **Risk Identification Form:** is the form that a risk reporter fills out when a potential risk is discovered.
- **Risk Management Framework (RMF):** is the overall process by which risk is identified, assessed, and monitored.
- **Risk Plan/Risk Remediation Plan:** is the plan of action on how management will respond to the risk after an assessment is conducted.
- **SOC 1:** is a regulation surrounding financial risk reporting in the US
- **SOX (Sarbanes-Oxley Act)**: is the regulation established by Congress in 2002 that is used to mitigate fraudulent practices.

References

- GITP-027 Global Technology Third Party Vendor Risk Management Policy
- GITP-008 Global Information Security Management Policy
- Access Review Procedures