



Information Technology (IT)

Governance and Risk Management Policy

UNObank, Inc.

IT Governance and Risk Management Policy	No: Policy no. 2024-RISK-072
Information Technology (IT) Governance and Risk Management Policy	Version : 1. 5
	Effectivity date: June 1, 2025
	Issued By: Technology and Risk Teams Owner: CTO and CRO

POLICY OWNERS

	Name	Designation and Department
Authored by	Janice Mata	IT Risk Manager, Risk Team
Last Updated by	Janice Mata	IT Risk Manager, Risk Team
Reviewed by	Raymond	Chief Risk Officer
	Luis Lorenzo Africa	Chief Technology Officer
Approved by	IT Steering Committee (ITSC)	
	Board of Directors	

POLICY STAKEHOLDERS

	Name	Designation and Department
Noted by	Saikat Sarkar	Deputy CEO
	Manish Bhai	CEO

Contents

1	Purpose	3
2	Scope	4
3	Governance Structure	5
3.1	Board of Directors (BoD)	5
3.2	Risk Oversight Committee (ROC)	6
3.3	IT Steering Committee.....	6
3.4	Senior Management	6
3.5	Technology Team (CTO, IT Function Heads, Managers and Members)	7
3.6	Business Units	7
3.7	Project Management Team	7
3.8	IT Risk Management Function (IT Risk Manager)	7
3.9	Internal Audit Team	8
3.10	External Auditors	9
4	IT Governance Framework.....	9
4.1	People.....	10
4.2	Policies, Process, Plans	11
4.3	Technology and Tools.....	11
5	IT Risk Management Framework/Process	12
5.1	Identify the risk.....	13
5.1.1	Types of Risks.....	13
5.1.2	Sources of IT Risks.....	14
5.1.3	IT Key Risk Indicators.....	15
5.1.4	IT Risk Assessment Triggers.....	15
5.2	Assess and measure the risk	16
5.3	Treat the risk.....	17
5.3.1	Prioritize the risk	17
5.3.2	Treat the risk.....	17
5.4	Report and monitor the risk	18
6	Policy Compliance	19
7	Definition of Terms	20
8	Appendices.....	22
9	Related Documents	25
10	Contact Information	25
11	Version Control.....	25

1 Purpose

This Framework aims to establish an effective and sustainable IT Governance and Risk Management policy across UNObank in compliance with the requirements of the Bangko Sentral ng Pilipinas (BSP) Circular No. 808.

Overall objectives for people, process, technology, information, partners and third parties:

- a. Confidentiality – to ensure that sensitive information is accessible only to authorized users, as well as to comply with legal and regulatory standards.
- b. Integrity – to ensure that systems are free from unauthorized alterations, ensuring that it operates correctly and as intended.
- c. Availability – to ensure a system's operational uptime and its ability to be accessible and functional when needed.
- d. Reliability – to ensure dependability of hardware, software, and network components in consistently delivering services effectively and efficiently.
- e. Control Design Effectiveness – to implement security controls and measures to manage IT risks more efficiently, reduce vulnerabilities, and protect valuable assets, ultimately supporting business continuity and resilience.
- f. Control Operating Effectiveness – to assess whether controls are implemented and how well it is functioning to manage identified risks.

IT Governance specific objectives are

- a. To define governance and management mechanisms necessary for a robust and holistic implementation of the Information Technology Risk Management.
- b. To ensure alignment between business and IT strategy on its people, process and technology to support the bank's business objectives.
- c. To ensure enterprise objectives are achieved by
 - evaluating stakeholder needs
 - customer-centric and stakeholder-centric decision-making and prioritization approach
 - monitoring performance, compliance, and progress against plans

IT Risk Management objectives are

- a. To ensure technology risks are identified, measured, monitored and mitigated.
- b. To verify that IT controls are effectively designed and consistently implemented to mitigate risks.
- c. To make sure IT risks are contained within the Bank's risk appetite.
- d. Ensure that risk-taking activities are managed within acceptable level while maintaining business value and opportunities for growth.
- e. Identify existing, potential, and emerging IT risks which the Bank may be exposed to, in relation to the use, ownership, operation, adoption of, and reliance to technology.
- f. Prioritize and monitor risk mitigation activities across the organization
- g. To enable executive decision-making for
 - Allocating IT budgets
 - Securing information technology systems
 - Outsourcing technology systems and services

The Framework will enable the Bank to achieve the following:

- a. Responsible risk-taking activities and initiatives
- b. Sound basis for decision-making and planning
- c. Proactive rather than re-active responses on risks
- d. Effective allocation and use of resources
- e. Effective incident management and reduction of losses
- f. Improved compliance to laws and regulations
- g. Improved stakeholders' confidence and trust

2 Scope

2.1 People / Organization

This policy applies to all relevant departments and/or units that are required to take concrete actions in establishing and implementing IT governance processes. It shall also cover Bank personnel who support use, fund, build and maintain the IT risk infrastructure of UNObank and the information contained therein.

This policy applies to all workforce, including executives, officers, managers, employees, contractors, consultants and third parties who have access to IT assets of UNObank and are bound by contractual agreements.

2.2 Process

This policy covers the aspects related to the Enterprise IT Governance and Risk Management across the organization.

- a. IT Operations
- b. IT Governance/ Management
- c. Information Security
- d. IT Outsourcing/Vendor Management
- e. IT Projects
- f. Electronic Banking/Electronic Products and Services
- g. Development and Acquisition
- h. Communication Networks
- i. Change and Release Management
- j. IT Risk Management (such as IT Risk Assessment /ITRA)

2.3 Technology

This policy covers

- IT Infrastructure
- Applications / Software / Systems (SaaS, On-Premises, any other)
- Hardware such as laptops, physical security controls, mobiles used for the organization

3 Governance Structure

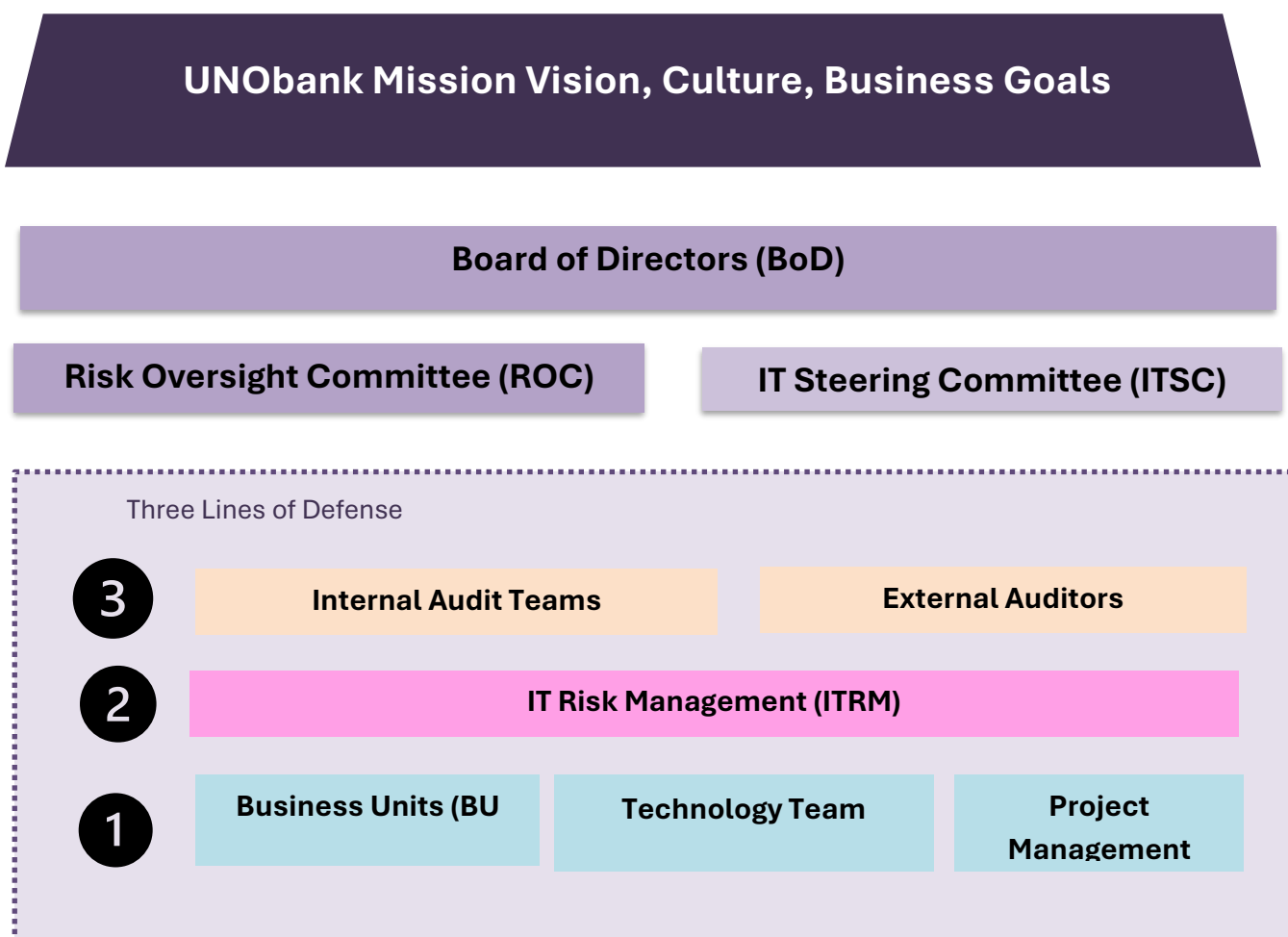


Figure 1.0 Governance Structure

3.1 Board of Directors (BoD)

- Define and regularly assess the organization's IT Strategy, IT Risk Appetite and IT Profile and ensure these are aligned with the organizational goals
- Establish governance over IT Strategy and IT Risk by implementing policies, standards and procedures that supports the IT Strategy, IT Risk Framework and IT Risk Appetite.

- Provide adequate resources such as people and technology to support the processes to detect, identify, assess, mitigate, measure and monitor IT Risks and keep them within the organization's risk appetite.
- Responsible for establishing IT Governance and Risk Management across the organization's people, process and technology.
- Ensure that the right resources are allocated effectively to support business objectives and enhance overall productivity.
- Promote clear and open communication of risk-related information between the Bank and its stakeholders, including employees, management, customers, investors, and regulatory bodies.
- Delegate the IT oversight function to a Board Level Committee (ITSC, RoC)

3.2 Risk Oversight Committee (ROC)

- Discuss and review the IT risk universe and the top priority bank-wide risks to be monitored for the year.
- Identify emerging risks that are not in the risk profile and adjust the rankings in accordance with strategic priorities.
- Monitor the effectiveness of the ITRA implementation.

3.3 IT Steering Committee

- Oversight on both long-term and short-term implementation of IT strategies such as staffing, organization and funding for IT operations and projects.
- Guide the business units and/or divisions on issues with wide-spread implications on technology and regulatory policies
- Address policy and process issues to assure transparency, within UNObank both domestically and regionally, as applicable.
- Serve as liaison between the Executive Committee and the Compliance Steering Committee
- Will hold regular meeting to progress on IT Strategies, status of IT risks.
- Ensure effective implementation of ITRA.
 - Review the overall result of the ITRA exercise.
 - Review and monitor status of the implementation of risk mitigation plans.

3.4 Senior Management

- Ensure that concerned units participate in the ITRA exercise.
- Ensure corrective actions are taken to mitigate risks identified during ITRA
- Review and re-align controls and processes subject to the initiative(s) and recommended improvements resulting from ITRA.
- Prioritize actionable items based on its relative importance considering the risk and impact to operations and business objective of the Bank.

3.5 Technology Team (CTO, IT Function Heads, Managers and Members)

- Establish an IT Governance Organizational Structure
- Implement an IT Governance Program.
- Define and implement IT Governance policies, process and guidelines
- Define and implement IT controls for every IT service
 - Preventive, detective and corrective controls
 - Physical, Organizational and Technical controls
- Implementation of ITRM processes
 - Identify, assess, mitigate and monitor IT Risks resulting from incidents, new or enhanced products, new or enhanced vendors services, external environment or failed IT Controls.
 - Perform Risk Control Self-Assessment (RCSA) and address identified gaps.
 - Complete IT Risk Assessment (ITRA) and Outsourcing Risk Assessment (ORA) for new/enhanced products/process/systems/third parties/projects.
- Plan, build, run and monitor activities in alignment with the direction set by the governance body to achieve the organizational strategies and objectives.
- Perform self-assessments on a periodic basis to gauge control effectiveness and performance and early identification and remediation of emerging or changing of existing risks.
- Perform ITRA for new or enhanced products, business process, technology or tools and third parties.

3.6 Business Units

- Perform self-assessments on a periodic basis to gauge control effectiveness and performance and early identification and remediation of emerging or changing of existing risks.
- Perform ITRA for new or enhanced products, business process, technology or tools and third parties.
 - The Heads of Business Units are ultimately accountable for carrying out the ITRA process and may designate personnel who shall be responsible for accomplishing and completing the ITRA.
 - The designated personnel are expected to gather inputs from the appropriate parties who handle specific activities covered in the scope of assessment to ensure accurate information on the identification of risks and adherence to control for the self-assessment.

3.7 Project Management Team

- Identify and assess risks related to IT projects and develop strategies to mitigate it.
- Manage changes to project scope, schedule, and resources.
- Enhance the resilience of IT projects against uncertainties and increases the likelihood of achieving project objectives.

3.8 IT Risk Management Function (IT Risk Manager)

- Establish business-aligned risk management frameworks

- Responsible for ensuring that the ITRM policy and overall risk management strategy are aligned with the organizations business objectives.
- Determine the IT risk appetite of the organization.
- Validates the bank's IT Profile
- Maintains IT risk policies, processes, guidelines, standards.
- Develop, monitor and oversee the implementation of IT Risk Management Framework and Program
- Monitor and ensure IT and business functions operate in accordance with the bank's IT Governance and Risk Management policies, standards and processes.
 - Validates if IT controls are effectively designed and consistently implemented.
 - Perform incident and problem management oversight.
 - Manages the IT Risk Register.
 - Coordinate risk mitigation plans among the different business units
- Monitor the bank's current risk profile, posture and exposure, status of risk remediation activities and critical risks and ensure current IT risk profile is within its risk appetite and report these to Senior Management, Board-Level Committee such as ITSC and ROC and the Board.
 - Present the top priority bank-wide risks to the Senior Management, Board Level Committees such as ITSC and ROC.
- ITRA-related responsibilities
 - Ensure ITRA is executed based on defined triggers/scope
 - Facilitate conduct of ITRA-related exercises or activities
 - Coordinate with the concerned units in the ITRA implementation, recommendations and/or identified action items.
 - Collect, analyze and recommend actions based on ITRA results
 - Ensure periodic reporting of the ITRA results to relevant stakeholders and Committee/s.

3.9 Internal Audit Team

- Independent IT Audit function with direct reporting relationship to the Board of Directors or its Audit Committee
- Responsible for providing an independent assessment and evaluation of the implementation and effectiveness of the ITRM processes such as ITRA.
- Conduct control validation activities. As risks evolve due to advancements in technology, existing controls may lose their effectiveness over time. Therefore, it is essential to test these controls regularly.
- Determine the IT Audit universe, IT Audit Scope and IT Audit Frequency, Audit Rating System.
- Conduct independent assessment of technology people, process and technology.
 - IT Governance
 - IT Organization Roles and Responsibilities

- IT Risk Management Framework
 - IT Policies
 - IT Controls
 - IT Risk Appetite
 - IT Risk
 - Outsourced IT Functions
- To ensure first and second line have identified, assessed and mitigate existing IT Risks; regulatory compliance and monitor status of identified risks and its mitigating controls
 - Implement IT Audit program(s) that is commensurate with the bank's size, complexity, scope of activities IT Profile and Risk profile and IT Risk Appetite.

3.10 External Auditors

- UNObank shall seek regular assurance that IT assets are appropriately secured and that their IT security risk management framework is effective. This may be executed through a formal external assessment program that facilitates a systematic assessment of the IT security risk and control environment over time.
- The bank shall engage an independent assessor to perform vulnerability assessment and penetration testing at least annually. The independent assessment report shall be reported to the risk oversight committee and the Board including the treatment or remediation plan. CISO shall be responsible in reviewing and monitoring the implementation of the treatment and remediation plan as necessary.

4 IT Governance Framework

The Bank will establish a holistic approach to IT governance based on COBIT 5 Framework.

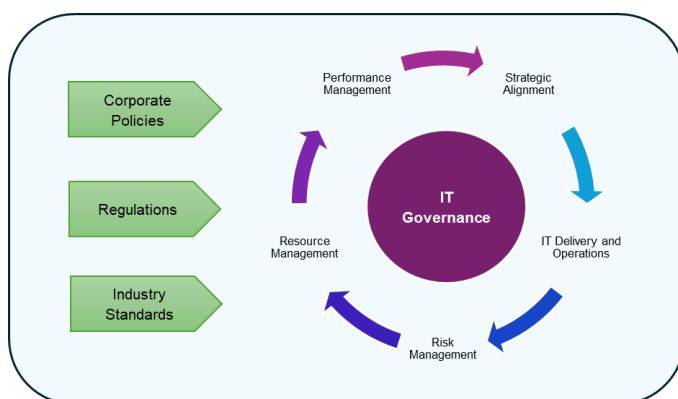


Figure 2.0 Governance Framework

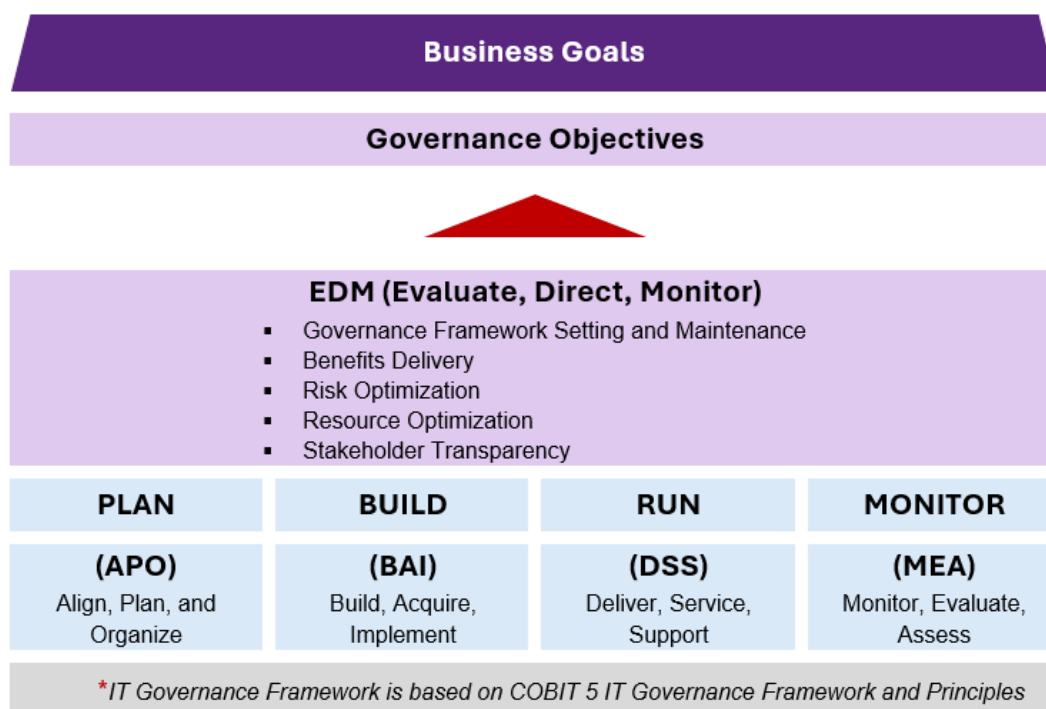


Figure 3.0 Governance – COBIT 5 Framework

4.1 People

The Bank shall establish an organization of IT functions to effectively deliver IT services to the Bank which will be led and governed by the Country CTO.

IT Services/Functions are

- Application Delivery
- Application Development
- Application Support
- Endpoint Management
- Infrastructure Management
- IT Security
- IT Governance
- Business Continuity Management – IT DRP
- Data-related Services
- Project Management

Refer to the Appendices for the Technology roles that will support the IT services/functions.

The Bank shall establish an organization of IT Risk function and roles to effectively maintain the bank's IT risk within its risk appetite and will be led and governed by IT Risk Head/Manager who directly reporting to the Chief Risk officer.

4.2 Policies, Process, Plans

The Bank shall establish, maintain and regularly communicate policies, processes, plans, standards, guidelines and inventories to support its IT Governance and Risk Management objectives.

- Define services and service level agreements (SLA) that must be monitored and measured in terms understandable to the business units. Establish SLA baselines and measure performance against it.
- There should be a regular monitoring of IT plans versus its actual implementation.
- Establish a framework for management of IT-related projects that will govern the process of developing, implementing, and maintaining major IT systems.
- Implement an effective outsourcing oversight program that provides the framework for management to understand, monitor, measure, and control the risks associated with outsourcing and the performance of third parties.
- Establish quality assurance (QA) and quality control (QC) procedures for all significant activities, both internal and external, to ensure that IT is delivering value to the business in a cost-effective manner and promotes continuous improvement through ongoing monitoring.
- Review policies annually.
- Technology functions will implement internal controls that are
 - Preventive, detective and corrective
 - Physical, Organizational and Technical

Refer to the appendices for list of policies, processes, plans, standard, guidelines and inventories to establish and maintain.

4.3 Technology and Tools

Technology and tools should be provided to IT organization to enable them in delivering its services to the business and should be compliant to company and regulatory requirements.

Refer to appendices for list of technology and tools.

5 IT Risk Management Framework/Process

The bank shall maintain a risk framework that identified all potential risks (internal and external), assess the likelihood and impact of the risk, drives the appropriate selection of IT risk response or treatment activities, and monitors its control implementation or risk acceptance.

The ITRM processes shall be integrated into the enterprise-wide risk management processes to allow UNObank to make well-informed decisions involving business plans and strategies, risk responses, risk tolerance levels and capital management, among others.



Figure 4.0 IT Risk Management (ITRM) Process

IT Risk Assessment (ITRA) IT Risk Assessment (ITRA) is a systematic risk process for identifying, assessing, mitigating, monitoring, and reporting of IT risks. It follows the ITRM process.

Refer to the ITRM Process Roles and Responsibilities table as guideline on who will be accountable, responsible, consulted and informed in the implementation of the Risk Management Process and ITRA.

Table 1.0 ITRM Process Roles and Responsibilities		
Accountable/Responsible	Consulted	Informed
Process : Identify the risk (mainly via ITRA, other IT risk-related identification processes are ORA, RCSA, ISRA, TPISA, DPIA)		
<ul style="list-style-type: none"> CTO IT Function Heads IT Governance Officer System/Application Business owner and Technology owner IT Process owner Business Process Owner Project Manager Vendor Business Owner CISO (via ISRA, TPISA) DPO (via DPIA) 	<ul style="list-style-type: none"> IT Risk Manager CRO 	<ul style="list-style-type: none"> Management Committee ITSC OC ROC BoD
Process : Assess and measure the risk		
Risk owner (who is accountable for managing the risk, can be any of the following) <ul style="list-style-type: none"> CTO IT Function Heads IT Governance Officer System/Application Business owner and Technology owner IT Process owner 	<ul style="list-style-type: none"> Technology Team IT Risk Manager 	Same as above

<ul style="list-style-type: none"> ▪ Business Process Owner ▪ Project Manger ▪ Vendor Business Owner ▪ CISO (via ISRA, TPISA) ▪ DPO (via DPIA) ▪ Senior Management ▪ Board 		
Process : Treat the risk		
<ul style="list-style-type: none"> ▪ Risk Owner ▪ Risk Treatment Action Owner 	<ul style="list-style-type: none"> ▪ Technology Team ▪ Control Owner ▪ IT Risk Manager 	Same as above
Process : Monitor and report the risk and control status		
<ul style="list-style-type: none"> ▪ Risk owner ▪ Risk Treatment Action Owner ▪ IT Risk Manager 	CTO CRO	Same as above

5.1 Identify the risk

The bank shall identify all foreseeable internal and external threats to its bank's people, process and technology that would prevent it from achieving its business objectives, IT Strategic Plan and risk objectives.

5.1.1 Types of Risks

- a. Strategic Risk - The risk to income and capital arising from unfavorable business decisions on IT-related investments or improper implementation of those decisions.
- b. Compliance Risk – The risk to income and capital arising from the violations of, or non-conformance with laws, rules and regulations, prescribed practices, or ethical standards.
- c. Operational Risk – The risk to income and capital arising from problems with service or product delivery. The risk is a function of internal controls, IT systems, employee integrity and operating processes.
 - Emerging Technology risk
 - Infrastructure risk
 - Integrity risk
 - Project risk
 - Relevance risk
 - Schedule risk
 - Talent risk
- d. Reputational Risk – The risk to income and capital arising from negative public opinion, which impacts the ability of the Bank to create new relationships or services or to continue servicing existing relationships.

5.1.2 Sources of IT Risks

- a. People – human error, lack of skills, malicious intent, lack of resources, management issues
- b. Process – IT Operations, Business Processes
 - IT Service Continuity – This relates to IT service outages and unreliability, which cause disruption to the business.
- c. Technology – Applications, Infrastructure, Devices (both internal and externally provided)
 - Information Assets – This relates to damage, loss or exploitation of information assets held within the IT system.
 - Applications – This relates to failures in the IT applications, which interact with internal and external users and include a combination of packaged software and customized software that will to some extent be integrated together.
 - Infrastructure – This relates to failures in the IT infrastructure, which pertains to the various centralized and distributed computer (i.e., operating systems, databases) and network resources upon which applications are hosted and run.
- d. Business Strategy – This relates to the IT's inability to execute the business strategy.
- e. Third-party, Service Providers and Vendors – This relates to IT service providers failing to deliver their contractual obligations, which impact the Bank's IT systems and services.
- f. Projects – This is concerned with IT projects failing, which may be attributable to timing, quality and scope of the project.

5.1.3 IT Key Risk Indicators

Table 2.0 IT Risk Indicators	
Associated Risk	Measurable KRI
Service interruption	Number of applications/infra/systems without SLA (vendor-provided)
	Availability of systems
	Accessibility of systems
	Delayed batch processing
ISP Failure	Number of ISP outages
Loss of data	Number of system backup failures due to software failure
Lack or misappropriation of IT budget	IT Budget Variance (IT Budget vs IT Actual Spending)
Lack or misappropriation of IT personnel	Average Service Request Resolution Time
Unaddressed critical incidents	Number of critical incidents
	Critical Incident Average resolution time
	Number of Critical Incidents with Breached Resolution SLA
Loss of hardware/physical assets	Number of company issued phones or laptops without monitoring software installed
Anonymous data leak	Number of active default database administrator accounts
Non-compliance to Data Privacy laws	Average Response Time to Data Privacy Requests/Inquiries
	Number of reportable data breaches that were not reported to regulator

5.1.4 IT Risk Assessment Triggers

ITRA is required for and triggered for

- New Products or Major Product changes
- New Systems/Infrastructure or major changes to systems/infra
- New/Changed IT Processes
- New Vendor or changes in services of existing vendors
- Annual review for Critical Systems
- Invalid or expired ITRAs

Invalid or expired ITRAs occur when ITRA is missed for a major change or release and therefore the existing ITRA applies to a previous or old version of the infrastructure or application.

ITRA must be integrated and embedded in related processes to ensure it is triggered when required. If possible, risk management tools should enforced ITRA.

Refer to the ITRA process document for the ITRA questionnaire/template.

5.2 Assess and measure the risk

IT Risk assessments shall be performed at enterprise-wide level, at least annually. Through these activities, the Bank shall identify all foreseeable internal and external threats to people, process and technology, the likelihood and impact of the threats, and the adequacy of existing controls to mitigate the identified and expected risks.

ITRA process documentation provides the ITRA questionnaire and assessment guidelines.

Risk assessment ranks and prioritizes the risks based on its inherent and residual risk levels. Refer to the Risk Matrix on how to determine inherent and residual risks and prioritize them.

Table 3.0 Risk Matrix			
Term	Description		
Probability	Factors to consider are uncertainties, risk sources, likelihood, events, scenarios, controls and their effectiveness.		
Impact	Evaluate end user, operational, financial, reputational, regulatory, legal, strategic impact.		
Inherent Risk	Inherent risk represents the amount of risk that exists in the absence of controls.		
Residual Risk	Residual risk is the amount of risk that remains after controls are put in place.		
Inherent/Residual Risk Level = Probability x Impact			
	Impact		
Probability	High (3)	Medium (2)	Low (1)
High (3)	High (9)	High (6)	Medium (3)
Medium (2)	High (6)	Medium (4)	Low (2)
Low (1)	Medium (3)	Low (2)	Low (1)
Risk Assessment			
Risk Event	Probability	Impact	Inherent/Residual Risk Level
Risk Event	High/Medium/Low	High/Medium/Low	Probability x Impact

Other factors to consider when assessing 'Probability' and 'Impact' are

- Any incidents, audit findings, other assessment results, regulatory interactions, customer complaints, and any issues and/or actions relating to the risks.
- Information technology issues and deviations and emerging technology risks
- Changes in the regulatory environment including regulatory change, regulatory focus, enforcement, or external audit reports.
- Divergence of opinions, biases, perceptions of risks and judgements, quality of the information used, the assumptions and exclusions made, any limitations of the techniques

and how they are executed. These influences shall be considered, documented and communicated to decision makers.

- Highly uncertain events with severe consequences can be difficult to quantify. In such cases, using a combination of techniques generally provides greater insight.

5.3 Treat the risk

5.3.1 Prioritize the risk

Risk treatment plans are prioritized based on inherent risk level and its corresponding risk appetite. Risk prioritization enables the Risk owners, ITSC, ROC and BoD decide which risks should be given with higher priority. The Management or the Board of Directors can choose to raise the profile of a risk for reasons including but not limited to non-financial influences, strategic business concerns and other priorities. High inherent risks are top priority, medium next and low risk last.

5.3.2 Treat the risk

The risk owner shall assess the design and operating effectiveness of existing risk controls or lack thereof; and determine the appropriate risk treatment. Refer to Table 3.0 for guidance.

Table 4.0 Risk Treatment	
Risk Treatment	Description
Avoid	Eliminates the risk by avoiding the activity or product entirely since the risk-taking activity creates more risk than bringing value to the organization.
Reduce	Minimizing the probability or impact of risk by enhancing existing controls or introducing additional control.
Transfer	Transferring the responsibility to address the risk to the third party that has greater control over the risk such as outsourcing, insurance, etc.
Accept	<ul style="list-style-type: none"> ▪ Acknowledges the presence of risk, however, remediation of vulnerability may be too costly that outweighs the benefit or when all applicable controls are already exhausted, but the remaining risk is impossible to be lowered down to the acceptable level. ▪ Acceptance of risk requires approval and continuous monitoring.
Inherent Risk	Risk Treatment
High (H)	<ul style="list-style-type: none"> ▪ Risk is intolerable. Risk owner to discuss the actions to address the risk with the ITSC. ▪ Risk treatment plan can either be REDUCE, TRANSFER, or AVOID. ▪ Corrective/preventive action is required. Resolution should be immediate or within the specified period. If the long-term resolution will be completed for a longer period, an interim workaround while waiting for the corrective action should be implemented as much as possible to mitigate the risk.
Medium (M)	<ul style="list-style-type: none"> ▪ Risk owner to monitor risk exposure and present to ITSC for review. ▪ Risk treatment plan can either be REDUCE, TRANSFER, or AVOID. ▪ Corrective/preventive action is required. Resolution should be within an acceptable/reasonable time frame as approved by the Risk Owner. ▪ Risk acceptance will require the documented approval of the Risk Owner/s.
Low (L)	<ul style="list-style-type: none"> ▪ Risk exposure is tolerable. Risk owner to monitor risk exposure. This can be addressed through standard procedures. ▪ Mitigating actions not required. Risk monitored to ensure risk levels have not changed.
Residual Risk	Risk Treatment
High	<ul style="list-style-type: none"> ▪ Risk is intolerable. Risk owner to discuss the actions to address the risk with the ITSC. ▪ Risk treatment plan can either be REDUCE, TRANSFER, or AVOID.

	Corrective/preventive action is required. Resolution should be immediate or within the specified period. If the long-term resolution will be completed for a longer period, an interim workaround while waiting for the corrective action should be implemented as much as possible to mitigate the risk. <ul style="list-style-type: none">No Risk Acceptance allowed.						
Medium	<ul style="list-style-type: none">Risk exposure should be monitored and presented to ITSC for review and monitoring.ACCEPTANCE of risk may be allowed but will require approval of the Risk Owner/s, sign-off should be documented.						
Low	Mitigating actions not required. Risk monitored to ensure risk levels have not changed.						
Risk Treatment and Assessment							
	Inherent Risk Assessment			Risk Treatment	Residual Risk Assessment		
Risk Event	Probability	Impact	Inherent Risk		Probability	Impact	Residual Risk
Risk Event	H/M/L	H/M/L	Probability x Impact	Avoid/Mitigate/Transfer/Accept	H/M/L	H/M/L	Probability x Impact

5.4 Report and monitor the risk

The Bank shall continually assess its residual risks and ensure these remains within its risk appetite.

Table 4.0 Risk Monitoring									
Risk Event	Inherent Risk	Risk Treatment	Residual Risk	Action	Action Owner	Due Date	Actual Completion Date	Action Status	Risk Status
	Probability x Impact	Avoid/Mitigate/Transfer/Accept	Probability x Impact						Open/Closed

- Monitoring and review shall take place in all stages of the process including planning, gathering and analyzing information, recording results and providing feedback.
- The result of monitoring and review shall be incorporated throughout the organization's performance management, measurement, and reporting activities.
- Timely, accurate, and complete risk monitoring and assessment reports shall be submitted to management to provide assurance that established controls are functioning effectively, resources are operating properly and used efficiently, and IT operations are performing within established parameters.
- The risk management process and its outcomes shall be documented and reported through appropriate mechanisms, which aims to

- communicate risk management activities and outcomes across the organization
 - provide information for decision-making
 - improve risk management activities
 - assist interaction with stakeholders, including those with responsibility and accountability for risk management activities
- e. Decisions concerning the creation, retention and handling of documented information shall consider the use, sensitivity and the external and internal context of the information.
- f. Reporting is an integral part of the organization's governance and shall enhance the quality of dialogue with stakeholders and support top management and oversight bodies in meeting their responsibilities. Factors to consider for reporting include, but are not limited to
- differing stakeholders and their specific information needs and requirements
 - cost, frequency and timeliness of reporting
 - method of reporting
 - relevance of information to organizational objectives and decision-making
- g. ITRA Submission, Review and Approval
- ITRA questionnaire/template will be completed by the Business Unit (BU) and will be reviewed and approved by its BU Head within a deadline established by IT Risk Manager / Team.
 - The Business Unit shall submit the accomplished ITRA to the IT Risk Manager / Team via ITRisk@uno.bank.
 - The IT Risk Manager / Team will review and challenge the submitted ITRAs as appropriate against the minimum requirements set out in this policy and provide feedback to the Business Units.
 - The IT Risk Team will keep an inventory of all completed ITRA and monitor progress of ITRA that are yet to be submitted.
 - The Business Unit shall retain a copy of the finalized ITRA and all supporting correspondences for document updating, resolution monitoring and audit purposes.

6 Policy Compliance

The Bank's Technology and Risk Management Departments are responsible for overseeing the implementation of this policy and compliance throughout UNObank.

The Risk Management function shall have a formal technology risk acknowledgement and acceptance process by the owners of risk to help facilitate the process of reviewing, evaluating, and approving any major non-compliance with this Policy.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, the Bank or a third-party service

provider, compliance exceptions to the policy requirement/s shall be duly authorized by the Country CTO and/or CRO. Each exception request shall include justification and benefits attributed to the waiver.

7 Definition of Terms

7.1 Abbreviations

Acronym	Meaning
BoD	Board of Directors
BSP	Bangko Sentral ng Pilipinas (Central Bank of the Philippines)
CCO	Chief Compliance Officer
CEO	Chief Executive Officer
CRO	Chief Risk Officer
CTO	Chief Technology Officer
COBIT	Control Objectives for Information and related Technology
DPIA	Data Privacy Impact Assessment
ISACA	Information Systems Audit and Control Association
ISRA	Information Security Risk Assessment
IT	Information Technology
ITG	IT Governance
ITRA	IT Risk Assessment
ITSC	IT Steering Committee
KRI	Key Risk Indicator
LoD	Line of Defense
ORA	Outsourcing Risk Assessment
RCSA	Risk Control Self-Assessment
ROC	Risk Oversight Committee
TPISA	Third Party Information Security Assessment

7.2 Definitions

Term	Definition
Audit finding	The result from a process that evaluates audit evidence and compares it against audit criteria.
Audit program	An action plan that documents what procedures an auditor will follow to validate that an organization is in conformance with compliance regulations.
Bank Information or Data	All data or information, regardless of physical form or characteristic, made or received in connection with the operational activities of the Bank that is in the possession or control of the organization.
COBIT 2019	Control Objectives for Information and related Technology version 2019 is a leading practice business framework developed by ISACA for the governance and management of IT.
COBIT 2019 components of governance system	These are 7 enablers/factors that individually and collectively influence the enablement of COBIT 2019 leading practice processes.

Term	Definition
Impact	Business impact reflects the potential consequences or severity of a risk event. This can be operational, financial, regulatory, strategic, reputational impact.
Inherent risk	Inherent risk represents the amount of risk that exists in the absence of controls.
Information Technology Environment	The policies and procedures that the Bank implements, the IT infrastructure (e.g., hardware, operating systems, etc.) and application software that it uses to support business operations and achieve business strategies.
Information Technology Risk	Refers to any potential adverse outcome, damage, loss, violation, failure or disruption associated with the use of or reliance on computer hardware, software, devices, systems, applications, and networks.
Information security program (ISP)	Information security program (ISP) refers to information security policies, standards and procedures, security operations, technologies, organizational structures, and information security awareness and training programs aimed at protecting the Bank's information assets and supporting infrastructure from internal and external threats.
Information security strategic plan (ISSP)	Information security strategic plan (ISSP) refers to the roadmap to guide the Bank in transforming the current state of security to the desired state considering business goals and strategies.
IT Audit	The periodic conduct of examination and evaluation of an organization's information technology infrastructure, policies and operations
IT Profile	As per BSP, refers to the inherent risk of a BSFI before application of any mitigating controls.
IT Risk Assessment (ITRA)	ITRA is an ITRM process and tool that facilitates systematic approach in identifying, assessing, mitigating, monitoring, and reporting of IT risks.
IT Risk Management	IT risk management (ITRM) refers to the process of identifying, assessing, mitigating, managing, and monitoring IT risks to ensure these are within acceptable levels.
IT Standards	Documented principles that establish requirements and processes that provide a reliable basis for shared expectations on how the Bank will comply with Information Technology related Bank policies, as well as national laws and regulations.
Likelihood	A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability. <i>Source: NIST SP 800-160</i>
Quality Assurance (QA)	QA activities ensure that product conforms to specification and is fit for use.
Quality Control (QC)	QC procedures identify weaknesses in work products and to avoid the resource drain and expense of redoing a task.
Residual risk	Residual risk is the amount of risk that remains after controls are put in place.
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. <i>Source: NIST SP 1800-25B</i>
Risk Appetite	The amount of risk that an organization is willing to accept to achieve its objectives. (source – ISACA)
Risk assessment	A process used to identify and evaluate risk and its potential effects. Includes assessing the critical functions necessary for the Bank to continue business operations, defining the controls in place to reduce Bank's exposure and evaluating the cost for such controls, and involves an evaluation of the probabilities of a particular event. (Source: ISACA)
Risk evaluation	The process of comparing the estimated risk against given criteria to determine the significance of the risk. (Source: ISACA)

Term	Definition
Risk identification	The process of determining and documenting the risk that the Bank faces. The identification of risk is based on the recognition of threats, vulnerabilities, assets and controls in the Bank's operational environment. (Source: ISACA)
Risk impact	The calculation of the amounts of loss or damage than the Bank may incur due to a risk event. (Source: ISACA)
Risk mitigation	The management of risk through the use of countermeasures and controls (Source: ISACA)
Risk monitoring	Maintaining ongoing awareness of an organization's risk environment, risk management program, and associated activities to support risk decisions. (Source: NIST SP 800-137)
Risk Owner	The group and individual(s) who are ultimately accountable for ensuring the risk is managed within risk appetite.
Risk prioritization	The ranking of material risks on an appropriate scale, such as frequency and/or severity. (Source: ISACA)
Risk reporting	The method of identifying risks tied to or potentially impacting an organization's business processes. The identified risks are usually compiled into a formal risk report, which is then delivered and communicated to the Bank's senior management and/or to various management teams. (Source: ISACA)
Risk tolerance	The acceptable deviation from the level set by the risk appetite and business objectives. (Source : ISACA)
Risk treatment	The tactics and strategies chosen to respond to a specific risk that will change its probability of occurrence and/or its impact. These can be avoid, reduce, transfer or accept the risk.
Senior Management/ Executive	Comprised of senior-level officers appointed to act on behalf of, and within the powers granted to them by, the BOD.
Technology resources	All devices, services, networks and other resources and technology related to the operational activities of the Bank, regardless of form or location, that are owned, provided, or administered by or through the Bank, or used to electronically store, process, or transmit information or data.
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability. Source: NIST SP 1800-15B
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. Source: NIST SP 1800-15B

8 Appendices

8.1 Technology roles that will support the IT services/functions.

- Chief Information Officer
- Chief Technology Officer
- IT Governance Officer
- IT Security Officer
- Project Managers

- Enterprise Architect
- Infrastructure Manager
- Service Managers
- Incident and Problem Managers
- IT Support – Level 0, Level 1, Level 2, Level 3
- Change Advisory Board (CAB)
- Change Managers
- Release Managers
- Development Team

8.2 List of policies, processes, plans, standard, guidelines and inventories to establish and maintain.

- *IT Governance and Risk Management Policy***
- *IT Service Catalog and IT Service Level Agreement**
- *System Development Lifecycle (SDLC) Policy**
- IT Operations Policy*
- Event Management
- *Incident Management*
- *Problem Management*
- Service Request Management
- Identity and Access Management Policy
- Information Security Policy
- IT Assets and Resource Management Policy*
- IT Asset Inventory (such as Systems/Cloud Infrastructure/API inventory)
- IT License inventory
- Physical and Environmental Security Policy*
- Information Classification Policy*
- Acceptable Use Policy*
- ITSC Charter
- *IT Risk Assessment Process****
- *IT Risk Appetite***
- IT Profile*
- IT Risk Universe***
- IT Risk Register**
- IT Control Register*
- *IT Strategy Plan**
- *IT Disaster Plan**
- IT Budget Plan*
- Segregation of Duties Policy*
- Change Management Policy*
- Release Management Policy*

- *Project Management Policy**
- IT Acquisitions Policy*
- Cloud Computing Policy*
- UNO Quality Policy
- Audit Charter****
- Internal IT Audit Assessment Framework****
- Annual Audit Plan****
- Audit Budget****
- *IT Audit universe*
- IT Audit Scope
- IT Audit Frequency
- IT Audit Rating System
- Internal IT Audit Assessment Report
- Documentation of IT Audits – work papers, audit reports, follow-up
- IT Audit Program(s)
- IT Audit Manual
- Roles and Responsibilities documentation for all Technology functions
- *Professional Development Programs for all Technology, Risk and Audit functions*

*to be maintained by CTO and /or its designate

**to be maintained by CTO, CRO and their designates

*** to maintained by CRO and/or its designate

****to be maintained by CCO and/or its designate

Italic and in violent font - required by BSP

8.3 List of technology and tools.

- Event (Alerts), Incident, Problem, Change and Release Tracking Tool
- Availability, Performance and utilization monitoring tool
- Project Management tracking tool
- Source code repository
- IT Assets Inventory Tool (example: systems inventory, API inventory, IT License inventory)
- IT Risk Register
- IT Controls Inventory

9 Related Documents

Document Reference no.	Document Name
2022-RISK-002	Risk Management Framework
2024-RISK-055	IT Risk Assessment Process
(to be provided)	IT Strategic Plan
2022-RISK-027	Information Security Program
(to be provided)	Project Management Policy

10 Contact Information

Submit all inquiries and requests for future enhancements to :

TechnologyPH@uno.bank
ITRisk@uno.bank

11 Version Control

This policy shall be subject to annual review to ensure relevancy.

This policy document and all its succeeding changes should be communicated and made available to all in scope.

The maintenance responsibility of this document shall be with the country CTO, CRO and/or their designates.

Effectivity Date	Version No.	Description of Change	Author(s)	Reviewer(s)	Approver(s)
July 2023	1.0	IT Governance Policy	Rizelle Flordeliz	Mae Cornejo	Luis Lorenzo Africa
July 2023	1.1	IT Risk Management Policy	Rizelle Flordeliz	Saikat Sarkar	Saikat Sarkar
October 2024	1.2	Revised and merged IT Governance and IT Risk Management Policy	Janice Mata	Luis Lorenzo Africa Vivian Perez	Luis Lorenzo Africa Vivian Perez Saikat Sarkar Manish Bhai ITSC
November 2024	1.3	Revised and merged IT Governance, IT Risk Management Policy and ITRA Policy	Janice Mata	Luis Lorenzo Africa Vivian Perez	Luis Lorenzo Africa Vivian Perez Saikat Sarkar Manish Bhai ITSC
January 2025	1.4	Updated the Governance Structure to put ROC and ITSC in the same level as both are board-level committees	Janice Mata	Luis Lorenzo Africa Raymond Apo	Luis Lorenzo Africa Raymond Apo Saikat Sarkar Manish Bhai ITSC

Effectivity Date	Version No.	Description of Change	Author(s)	Reviewer(s)	Approver(s)
May 2025	1.5	Updated IT Risk Assessment Triggers : Added annual ITRA for Critical Systems and invalid /expired ITRA	Janice Mata	ITSC	ITSC