Management of Information and Related Technology Governance Manual

دليل ادارة وحاكمية المعلومات والتكنولوجيا المصاحبة لها

Arab Banking Corporation Jordan

بنك المؤسسة العربية المصرفية الأردن

January 2025

كانون الثاني2025

First: Introduction

أولا: المقدمة

IT considered as one of the most important pillars within Bank ABC, which exhibited by Bank's adoption to COBIT framework, to achieve Bank's strategic objectives.

This Framework (COBIT) maintains the required balance for achieving bank's ultimate benefit while reducing risk levels. Also enabling the Bank to manage IT in a comprehensive and balanced manner that conforms to its objectives and ensures the optimal exploitation of its resources. This integrates efforts in all areas to achieve the desired benefits for internal and external stakeholders.

تعتبر تكنولوجيا المعلومات واحدة من اهم الركائز في بنك المؤسسة العربية المصرفية، وتجلى ذلك بإعتماد البنك لإطار حوكمة وإدارة المعلومات والتكنولوجيا المصاحبة لها لتحقيق الأهداف الاستراتيجية للبنك.

يحفظ إطار حوكمة المعلومات (COBIT) التوازن بين تحقيق الفائدة العظمى للبنك مع تخفيض مستويات المخاطر. كما يمكّن البنك من إدارة تكنولوجيا المعلومات بطريقة شاملة ومتوازنة تتوافق مع اهدافه وتضمن الاستغلال الامثل لموارده. مما يؤدي الى تكامل الجهود في جميع المجالات لتحقيق الفوائد المرجوة من تكنولوجيا المعلومات لأصحاب المصلحة الداخليين والخارجيين.

Note: This manual should be read together with bank's corporate governance manual.

ملاحظة: يجب أن يقرأ هذا الدليل بالتوافق مع دليل الحاكمية المؤسسية الخاص ببنك المؤسسة العربية المصرفية.

Second: Definitions

ثانيا: التعريفات

The Board: The Board of Directors of the Bank / Jordan.

المجلس: مجلس إدارة بنك المؤسسة العربية المصرفية/ الأردن.

Governance of information and related technology:
The distribution of roles and responsibilities and description of relationships between different parties and stakeholders (such as the Board of Directors and Executive Management) in order to maximize the organization's value added by following the optimal approach that ensures a balance between expected risk and return, adopting the rules, bases and mechanisms necessary for decision-making, and identifying the bank's strategic directions and objectives as well as the relevant mechanisms to control and monitor compliance in order to ensure the bank's sustainability and development.

حاكمية المعلومات والتكنولوجيا المصاحبة لها: عملية توزيع الأدوار والمسؤوليات وتوصيف العلاقات بين الأطراف والجهات المختلفة وأصحاب المصالح (مثل المجلس والإدارة التنفيذية) بهدف تعظيم القيمة المضافة للمؤسسة باتباع النهج الأمثل الذي يكفل التوازن بين المخاطر والعوائد المتوقعة، وذلك من خلال اعتماد القواعد والأسس والآليات اللازمة لصنع القرار وتحديد التوجهات الاستراتيجية والأهداف في البنك وآليات مراقبة وفحص امتثال مدى تحققها بما يكفل ديمومة وتطور البنك.

Management of information and related technology: a set of ongoing activities that fall under the responsibility of the Executive Management. Such activities involve planning achieving the strategic goals including alignment and regulation, construction and development activities including purchase and implementation, operating activities including delivery of services and support, as well as monitoring activities

حاكمية إدارة المعلومات والتكنولوجيا المصاحبة لها: مجموعة من الأنشطة المستمرة التي تقع ضمن مسؤولية الإدارة التنفيذية. تتضمن هذه الأنشطة التخطيط بغرض تحقيق الأهداف الاستراتيجية بما يشمل الموائمة والتنظيم، انشطة البناء والتطوير بما فيها الشراء والتنفيذ، انشطة التشغيل بما في ذلك تقديم الخدمات والدعم، ونشاطات

including measurement and evaluation to ensure continuous achievement of the bank's strategic goals and directions.

Governance and Management Objectives: A set of practices and activities stemming from the organization's policies that are necessary to achieve the IT/Alignment Goals.

IT/Alignment Goals: A set of primary and secondary goals relating to the governance and management activities of information and related technology that are necessary to achieve the Enterprise Goals.

Enterprise Goals: A set of objectives relating to the corporate governance and Enterprise management that are necessary to achieve stakeholder's needs and objectives of this code.

Senior Executive Management: It includes the bank's CEO, Executive Vice President, Senior Vice President, Head of Internal Audit, Head of Compliance and Risk Management Department Manager, as well as any of the bank's employees who holds an executive power parallel to any of the powers of the said executives and who directly reports to the CEO.

Stakeholders: Any person that has an interest in the bank, such as shareholders, employees, creditors, customers, external suppliers or concerned regulatory authorities.

Cyber Resilience: The banks' ability to anticipate, endure, contain, and quickly recover from a cyber-attack.

Cyber Security: Protecting the confidentiality, integrity and availability of the banks' information and information assets in cyberspace from any cyber threat, through a set of relevant means, policies, instructions, and best practices.

المراقبة بما فيها القياس والتقييم لضمان ديمومة تحقيق أهداف البنك وتوجهاته الاستراتيجية

أهداف الحاكمية والإدارة: مجموعة الممارسات والنشاطات المنبثقة عن سياسات المؤسسة واللازمة لتحقيق أهداف المعلومات والتكنولوجيا المصاحبة لها.

أهداف المعلومات والتكنولوجيا المصاحبة لها (أهداف التوافق): مجموعة الأهداف الرئيسية والفرعية المتعلقة بنشاطات الحاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها واللازمة لتحقيق الأهداف المؤسسية.

الأهداف المؤسسية: مجموعة الأهداف المتعلقة بالحاكمية والإدارة المؤسسية واللازمة لتحقيق احتياجات أصحاب المصالح وأهداف هذا الدليل.

الإدارة التنفيذية العليا: تشمل المدير العام، نواب الرئيس التنفيذيين، نواب الرئيس الرئيسيين، رئيس التدقيق الداخلي، رئيس مراقبة الامتثال ومدير دائرة إدارة المخاطر، بالإضافة إلى أي موظف في البنك له سلطة تنفيذية موازية لأي من سلطات المذكورين ويرتبط وظيفياً مباشرة بالمدير العام.

أصحاب المصالح: أي ذي مصلحة في البنك مثل المساهمين أو الموظفين أو الدائنين أو العملاء أو الموردين الخارجيين أو الجهات الرقابية المعنية.

التكيف السيبراني: قدرة البنك على توقع الهجمات الالكترونية وتحملها واحتوائها والتعاقي منها بسرعة.

الأمن السيبراني: الحفاظ على سرية وسلامة وتوافر المعلومات وأصول المعلومات التابعة للبنك ضمن الفضاء السيبراني من أي تهديد سيبراني عن طريق مجموعة من الوسائل والسياسات والتعليمات وافضل الممارسات ذات الصلة.

Third: Scope:

This manual and guide include all bank's IT-based operations in various branches and departments. All stakeholders and related parties concerned with applying the instructions, each fitting to attached role and location.

ثالثا: نطاق التطبيق:

يشمل هذا الدليل كافة عمليات البنك المرتكزة على تكنولوجيا المعلومات بمختلف الفروع والإدارات، وتعتبر جميع الأطراف أصحاب المصالح معنية بتطبيق التعليمات كل بحسب دوره وموقعه.

Fourth: Key stakeholders and their responsibilities:

Chairman and Members of Board of Directors: Assigning the responsibilities of overall direction of the governance, supports and provide needed funds as required.

CEO, EVPs, and SVPs:

Assigning the responsibilities of hiring qualified experienced people in Bank's operations and characterize mapped tasks and responsibilities.

IT Head, Steering Committee of Information, and related technology:

Fulfilling mapped responsibilities with all related stakeholders, recommending the necessary resources.

Internal and External Audit:

To evaluate and audit the allocation of resources and concerned management, I&T projects, and bank's linked operations concentrated on a specialized technical review, also internal audit to participate as independent consultant and observer when required.

Risk, compliance, and legal departments:

Risk main role Integrates risk governance and management overall I&T governance and management within the bank. Legal are involved to provide a legal advice and guidance on matters of law and legal protection for sales, purchasing, customer support, licensing, and other, as compliance Keeping

رابعا: الاطراف ذوي العلاقة ومسؤولياتهم:

رئيس واعضاء مجلس الإدارة:

تحديد مسؤوليات التوجيه العام والموافقة على المسؤوليات ضمن نطاق الحاكمية وتقديم الدعم والتمويل اللازمين عند الحاجة.

المدير العام ونوابه ومساعديه:

تولي مسؤوليات تسمية الأشخاص ذوي الخبرة المناسبين في عمليات البنك وتوصيف مهامهم ومسؤولياتهم.

رئيس إدارة تكنولوجيا المعلومات، اللجنة التوجيهية للمعلومات والتكنولوجيا المصاحبة لها ومدراء المشاريع:

تولي تنفيذ المسؤوليات والمهام المحددة مع جميع أصحاب المصلحة ذوي الصلة، والتوصية بالموارد اللازمة بالخصوص.

التدقيق الداخلي والخارجي:

على التدقيق الخارجي والداخلي العمل على مراجعة وتقييم ما يخص توزيع الموارد وإدارتها و المشاريع الخاصة بتكنولوجيا المعلومات و جميع العمليات المرتبطة باعمال البنك ، كذلك المشاركة بما يمثل دور التدقيق الداخلي في الامور التنفيذية كمستشار ومراقب مستقل عند الحاجة.

المخاطر والامتثال والشؤون القانونية :

من اهم ادوار إدارة المخاطر في البنك، تكامل حوكمة وإدارة المخاطر مع حوكمة تقنية المعلومات والتكنولوجيا المصاحبة لها داخل البنك. وتشارك الدائرة القانونية في تقديم المشورة والتوجيهات القانونية بشأن المسائل القانونية والحماية القانونية كالمبيعات، وعمليات الشراء، ودعم العملاء،

bank activities in strict compliance with all related regulations (internally and externally, ensuring bank is compiled).

والتراخيص وغيرها. أما دور دائرة الامتثال ضمان الامتثال لجميع التعليمات ذات الصلة (سواء كانت تعليمات من قبل جهات تشريعية سواء كانت في الأردن او دولية ملزمة) في أنشطة البنك.

Fifth: Principles of Governance and Management Information and Related Technology:

The Governance and Management of Information and Related Technology includes implementation of several policies, practices and procedures that supported by bank's structures (hierarchical) and set work duties ensuring the fulfillment of IT strategic objectives in the bank which stemmed from the bank's strategic objectives in line with the availability of controls to prevent unwanted events, or to pre-mitigated.

The governance and management of information and related technology rely on six principles for the governance system as follows:

1. Provide value to stakeholders
2. Holistic approach: A governance system for the banks' I&T is built from several components that can be of different types and that work together in a holistic way.
3. Dynamic governance system: This means that each time one or more of the design factors are changed (e.g., a change in strategy or technology), the impact of these changes on the EGIT system must be considered.
4. Governance Distinct from Management.
5. Tailored to bank needs: using a set of design factors as parameters to customize and prioritize the governance system components.
6. End-To-End Governance System

خامسا: مبادئ حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها:

تتضمن حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها تطبيق مجموعة من السياسات والممارسات والإجراءات المدعومة بالهياكل التنظيمية، والمهام الوظيفية المحددة والمتكاملة لضمان تحقيق الأهداف الاستراتيجية لتكنولوجيا المعلومات في البنك، والتي تنبثق من أهداف البنك الاستراتيجية مع توفير الضوابط التي تمنع وقوع الأحداث غير المرغوبة، أو اكتشافها وسرعة احتوائها.

وترتكز حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها على ستة مبادئ أساسية للنظام وهي على النحو الاتي:

1. تحقيق القيمة المرجوة التي تلبي احتياجات اصحاب المصالح.
2. المنهجية الشاملة: يتم بناء نظام حوكمة المعلومات والتكنولوجيا المصاحبة لها في البنك من خلال عدد من عناصر التمكين التي تعمل معًا بطريقة شمولية.
3. نظام حاكمية (ديناميكي): هذا يعني انه وفي حال تغير عامل أو أكثر من عوامل تصميم هذا الإطار (على سبيل المثال تغير في استراتيجية المؤسسة أو التكنولوجيا) يمكن النظر في تأثير هذه التغيرات على نظام الحاكمية في البنك وتحديثه لمواكبة واستيعاب هذه التغيرات وتلبية الاحتياجات الجديدة.
4. فصل الحاكمية عن الإدارة.
5. إطار عمل مصمم ليلبي احتياجات البنك، من خلال استخدام عوامل التصميم المؤثرة في تشكيل إطار حاكمية تكنولوجيا المعلومات لتكييف وترتيب أهمية وأولوية عناصر التمكين.
6. نظام حاكمية متكامل.

Sixth: Goals of Governance and Management of Information and Related Technology

Governance and Management of Information and Related Technology aims to achieve:

1. Meeting stakeholder needs and realizing bank's objectives and trends by achieving IT/Alignment goals to guarantee:
   a. Providing quality information as a pillar supporting decision-making mechanisms at the bank.
   b. Prudent management of IT resources and projects optimize resources utilization.
   c. Providing a technological infrastructure that support and enables the bank to achieve its objectives.
   d. Upgrading bank's various operations by employing efficient and reliable technological systems.
   e. Management of IT risks providing necessary protection for bank's assets.
   f. Assisting in achieving compliance with the requirements of laws, regulations, and instructions, also compliance with the strategy, policies, and internal banks' procedures.
   g. Improving the internal control system.
   h. Optimizing the level of users' satisfaction resulted of information technology through meeting work needs efficiently and effectively.

سادسا: أهداف حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها:

تهدف حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها لتحقيق ما يلي:

1. تلبية احتياجات أصحاب المصالح وتحقيق توجهات وأهداف البنك من خلال تحقيق أهداف المعلومات والتكنولوجيا المصاحبة لها، وبما يضمن:
   أ. توفير معلومات ذات جودة عالية كمرتكز يدعم آليات صنع القرار في البنك.
   ب. إدارة حصيفة لموارد ومشاريع تكنولوجيا المعلومات، تعظم الاستفادة من تلك الموارد.
   ت. توفير بنية تحتية تكنولوجية تمكن البنك من تحقيق أهدافه.
   ث. الارتقاء بعمليات البنك المختلفة من خلال توظيف منظومة تكنولوجية كفؤة وذات اعتمادية متميزة.
   ج. إدارة لمخاطر تكنولوجيا المعلومات توفر الحماية اللازمة لموجودات البنك.
   ح. المساعدة في تحقيق الامتثال لمتطلبات القوانين والتشريعات والتعليمات بالإضافة الى الامتثال الى استراتيجية وسياسات وإجراءات العمل الداخلية.
   خ. تطوير نظام الرقابة الداخلي.
   د. تعظيم مستوى الرضا عن تكنولوجيا المعلومات من قبل مستخدميها بتلبية احتياجات العمل بكفاءة وفعالية.

i. Managing services of external parties entrusted with carrying out operations, tasks, services, and products.
2. Achieving comprehensive governance and management of information and related technology.
3. Adopting business practices and rules in governance and management of IT operations, projects, and resources.
4. Segregating Board's operations, functions, and responsibilities in the field of governance from falling under the responsibility of Executive Management regarding information and related technology.
5. Strengthening self-control and independent control mechanisms in addition to examining compliance in the areas of governance as well as management of information and related technology towards improved performance and continuous development.

ذ. إدارة خدمات الأطراف الخارجية الموكل إليها تنفيذ عمليات ومهام وخدمات ومنتجات.
2. تحقيق الشمولية في حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها.
3. تبني ممارسات وقواعد العمل والتنظيم كنقطة انطلاق يتم الارتكاز والبناء عليها في مجالي حاكمية وإدارة عمليات ومشاريع وموارد تكنولوجيا المعلومات.
4. فصل عمليات ومهام ومسؤوليات المجلس في مجال الحاكمية عن الخضوع لمسؤولية الإدارة التنفيذية بخصوص المعلومات والتكنولوجيا المصاحبة لها.
5. تعزيز آليات الرقابة الذاتية والرقابة المستقلة وفحص الامتثال في مجالي حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها وبما يساهم في تحسين وتطوير الأداء بشكل مستمر.

Seventh: Committees:

سابعا: اللجان:

1. IT Governance Committee

The committee composition and its methodology:

- The Board set up IT governance committee from its members, three members, members with an experience and/or strategic knowledge and with adequate skills and knowledge to understand and manage Information and related technology also Cyber Risks.
- The Committee permitted to invite any of bank's executives to attend the meetings thereof to seek their opinion, which includes internal audit staff and members of the Senior Executive Management (such as information technology director) or external audit staff.
- The Board specifies the Committee's objectives, responsibilities, and authorities under a specific charter, and review updates are reflected to related charters continuously.
- The committee briefs and submit periodic reports to the Board.
- The Committee meets at least four times a year.
- The Committee should keep documented minutes of meetings.

1. لجنة حاكمية تكنولوجيا المعلومات:

تشكيل اللجنة وآلية عملها:

- يتم تشكيل لجنة حاكمية تكنولوجيا المعلومات من قبل المجلس من ضمن اعضاءه. والتي يشكلها ثلاثة أعضاء على الأقل من ذوي الخبرة و/ أو المعرفة الاستراتيجية في تكنولوجيا المعلومات، بالإضافة إلى أشخاص يتمتعون بالمهارات والمعارف المناسبة لفهم وإدارة المخاطر السيبرانية.
- للجنة الصلاحيات بدعوة أي من إداريي البنك لحضور اجتماعاتها للاستعانة برأيهم بما فيهم المعنيين في التدقيق الداخلي وأعضاء الإدارة التنفيذية العليا (مثل رئيس إدارة تكنولوجيا المعلومات) أو المعنيين في التدقيق الخارجي.
- يحدد المجلس اهداف اللجنة ومسؤولياتها وصلاحياتها بموجب ميثاق محدد، ويتم عكس نتائج المراجعات والتحديثات الدورية على المواثيق بسكل مستمر.
- تقوم اللجنة برفع تقارير دورية للمجلس.
- تجتمع اللجنة بشكل ربع سنوي على الأقل.
- تحتفظ اللجنة بمحاضر اجتماعاتها موثقة.

Committee responsibilities:

- Adopting the strategic goals of information, related technology, and appropriate organizational structures, including steering committees at the level of Senior Executive Management, to ensure the achievement of bank's strategic objectives, achieve better value added from IT resources projects and investments, and necessary tools usage with standards to control these objectives and to assure proper achievement.
- Adopting the general framework for the management, control and monitoring of IT projects and resources, consistent with the acceptable international practices in this regard, particularly COBIT, and fulfilling the requirements of instructions.
- Adopting the importance and priority of the Governance and Management Objectives and their relevance to Banks' Goals and IT/Alignment Goals with related components. To be based on a study (at least annually) considering COBIT 2019 framework design factors

مهام ومسؤوليات اللجنة:

- اعتماد الأهداف الاستراتيجية لتكنولوجيا المعلومات والهياكل التنظيمية المناسبة بما في ذلك اللجان التوجيهية على مستوى الإدارة التنفيذية العليا، بما يضمن تحقيق الأهداف الاستراتيجية للبنك وتحقيق أفضل قيمة مضافة من مشاريع واستثمارات موارد تكنولوجيا المعلومات، واستخدام الأدوات والمعايير اللازمة لمراقبة والتأكد من مدى تحقق ذلك.
- اعتماد الإطار العام لإدارة وضبط ومراقبة موارد ومشاريع تكنولوجيا المعلومات يحاكي أفضل الممارسات الدولية المقبولة بهذا الخصوص ويتوافق مع أهداف ومتطلبات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها.
- اعتماد أهمية وترتيب أولوية الاهداف المؤسسية ومدى ارتباطها بأهداف التوافق وأهداف الحاكمية والإدارة بالإضافة لارتباطها بباقي عناصر التمكين، وذلك بناءً على دراسة نوعية و/أو كمية تعد لهذا الغرض بشكل سنوي على الأقل تأخذ بعين الاعتبار عوامل التصميم المؤثرة في تشكيل إطار حاكمية تكنولوجيا

framework guidance, aligned with Bank's vision and strategies.

- Adopting the Enterprise Goals, and the IT/Alignment Goals.
- Adopting RACI Chart in the primary operations of IT governance.
- Making sure of existence of framework for IT risk management that complies with the overall general framework of the risk management at the bank.
- Approving the overall IT resources and projects budgets in line with the bank's strategic objectives.
- Generally supervising and reviewing the progress of IT operations, resources, and IT projects through the IT steering committee.
- Reviewing main issues highlighted in the IT audit reports through Audit Committee and follow-up in taking the necessary actions to address deviations.
- Making recommendations to the Board to take the necessary actions to correct any deviations.
- Adopting Cyber Security Policy.
- Adopting Cyber Security Program.
- Examining compliance with Cyber Security Policy and Program.

المعلومات بما يتناسب مع خصوصية واستراتيجيات البنك.

- اعتماد مصفوفة الأهداف المؤسسية، وأهداف المعلومات والتكنولوجيا المصاحبة لها.
- اعتماد مصفوفة المسؤوليات تجاه العمليات الرئيسية لحاكمية تكنولوجيا المعلومات.
- التأكد من وجود إطار عام لإدارة مخاطر تكنولوجيا المعلومات يتوافق ويتكامل مع الإطار العام الكلي لإدارة المخاطر في البنك.
- اعتماد الموازنة الكلية لموارد ومشاريع تكنولوجيا المعلومات بما يتوافق والأهداف الاستراتيجية للبنك.
- الإشراف العام على سير عمليات وموارد ومشاريع تكنولوجيا المعلومات من خلال تقارير ومحاضر إجتماعات اللجنة التوجيهية لتكنولوجيا المعلومات.
- الاطلاع على اهم الملاحظات الواردة في تقارير تدقيق تكنولوجيا المعلومات من خلال لجنة التدقيق ومتابعة اتخاذ ما يلزم من إجراءات لمعالجة الانحرافات.
- التوصية للمجلس باتخاذ الإجراءات اللازمة لتصحيح أية انحرافات.
- اعتماد سياسة الأمن السيبراني.
- اعتماد برنامج الأمن السيبراني.
- فحص الامتثال لسياسة وبرنامج الأمن السيبراني.

2. <u>IT Steering Committee:</u>

The committee composition and its methodology:

- The IT Steering Committee formed and chaired by the CEO and members from senior executives, including IT head, Risk Management Department Manager, Cyber and Information Security Department Manager, and the Head of Internal Audit.
- The Committee permitted inviting any employee to attend its meetings.
- The Committee meeting at least once every three months.
- The Committee documents meetings in proper minutes of meeting.

2. <u>اللجنة التوجيهية لتكنولوجيا المعلومات:</u>

تشكيل اللجنة وآلية عملها:

- يتم تشكيل لجنة برئاسة المدير العام وعضوية مدراء الإدارة التنفيذية العليا بما في ذلك رئيس إدارة أنظمة المعلومات ومدير إدارة المخاطر ومدير دائرة الامن السيبراني وحماية المعلومات، بالإضافة لمدير التدقيق الداخلي.
- يمكن للجنة دعوة أي موظف لحضور اجتماعاتها.
- تجتمع اللجنة اربع مرات سنويا على الاقل.
- توثق اللجنة اجتماعاتها بمحاضر أصولية.

<u>Committee responsibilities:</u>

- Reviewing annual plans to achieve Banks' strategic objectives approved by the Board and overseeing implementation-ensuring completion also monitoring internal and external factors affecting the same on a continuous basis.
- Linking Enterprise goals to IT/Alignment goals, approving and reviewing on an ongoing basis ensuring the achievement of bank's strategic objectives and the purposes of the instructions, identifying, and reviewing set of Measurement standards, assigning concerned Executive Management staff to continuously monitor such standards, and informing the Committee thereof.
- Adopting the importance and priority of Governance and Management Objectives and their relevance to Enterprise Goals and IT/Alignment Goals, in addition to related components. This Adoption based on annual reviews and study considering design factors of COBIT 2019 framework guidance, aligned with Bank's specificity and strategies.
- Endorse results of above-mentioned study to Governance Committee.

<u>مهام ومسؤوليات اللجنة:</u>

- مراجعة الخطط السنوية لتحقيقالاهداف الاستراتيجية المقرة من قبل المجلس، والإشراف على تنفيذها لضمان تحقيقها ومراقبة العوامل الداخلية والخارجية المؤثرة عليها بشكل مستمر.
- ربط مصفوفة الأهداف المؤسسية بمصفوفة أهداف المعلومات والتكنولوجيا المصاحبة لها واعتمادها ومراجعتها بشكل مستمر وبما يضمن تحقيق الأهداف الاستراتيجية للبنك، ومراعاة تعريف مجموعة معايير للقياس ومراجعتها وتكليف المعنيين من الإدارة التنفيذية بمراقبتها بشكل مستمر.
- اعتماد أهمية وترتيب أولوية أهداف المؤسسة ومدى ارتباطها بأهداف التوافق وأهداف الحاكمية والإدارة بالإضافة لارتباطها بباقي عناصر التمكين، وذلك بناءً على دراسة تعد لهذا الغرض بشكل سنوي على الأقل تأخذ بعين الاعتبار العوامل المؤثرة في تشكيل إطار حاكمية تكنولوجيا المعلومات، بما يتناسب مع خصوصية واستراتيجيات البنك.

- Making recommendations for the allocation of financial and non-financial resources necessary to achieve governance and management objectives, with the support of efficient human resources in the right place.
- Arranging IT projects and programs by priority.
- Monitoring the level of technical and technological services, raising efficiency, and improving them on a continuous basis.
- Making the necessary recommendations to IT Governance Committee
- Providing IT Governance Committee with minutes of meetings thereof on an immediate basis.

- رفع توصية بمخرجات العمليات أعلاه الى لجنة حاكمية تكنولوجيا المعلومات للموافقة والاعتماد.
- التوصية بتخصيص الموارد المالية وغير المالية اللازمة لتحقيق اهداف الحاكمية والإدارة والاستعانة بالعنصر البشري الكفوء والمناسب في المكان المناسب.
- ترتيب أولويات المشاريع الكبرى في إدارة تكنولوجيا المعلومات.
- مراقبة مستوى الخدمات الفنية والتكنولوجية والعمل على رفع كفاءتها وتحسينها بشكل مستمر.
- رفع التوصيات اللازمة للجنة حاكمية تكنولوجيا المعلومات.
- تزويد لجنة حاكمية تكنولوجيا المعلومات بمحاضر اجتماعاتها أولاً بأول.

Eighth: Related Departments tasks and responsibilities:

The responsibility of the related departments at the bank is assuring that all tasks were implemented from them and in compliance with governance code, as following:

Information Technology Department:

- Provide information technology services that meets the bank operation's needs.
- Execute projects in a project management frame in time and financial budget under the related international standards.
- Assuring the integrity of applied software and the resources of technology within the bank operations.
- Applying the security systems, the best international best practices as well as the bank policies and procedures.

Cyber and Information Security Department:

- Directly supervising the development of the cyber security program and policy and ensuring the implementation of, and continuously reviewing and updating the same.
- Assessing the adequacy and efficiency of the cyber security program and policy.
- Continuously reviewing the effectiveness of the protection controls adopted in the company's cyber security policy
- Identifying and assessing cyber risks.
- Recommend the applicants of the best international practices regarding the information security with the consistence of the policies and bank strategies.

Business Continuity Unit:

- Develop the bank business continuity plan.
- Oversee the execution of business continuity plan.
- Prepare periodic testing results reports and pursue the solutions of the resulting problems.
- Prepare and update the business continuity management policy.
- Develop Business Continuity Plan for Cyber Security Scenarios /Incidents and conduct regular testing.

Human Resources Management

- Raising the competitive level of skills generally for the bank employees and especially for the information technology

ثامنا: مهام ومسؤوليات الإدارات والدوائر المعنية في البنك:

تكون مسؤولية الإدارات والدوائر المعنية في البنك التأكد من أن كافة المهام المنفذة من قبلهم تتم بما يتوافق مع دليل الحاكمية، مع الالتزام بأحكام هذا الدليل. وتتوزع هذه المسؤولية على النحو الاتي:

إدارة أنظمة المعلومات:

- تقديم خدمات تكنولوجيا معلومات تلبي متطلبات عمليات البنك.
- تنفيذ المشاريع ضمن إطار إدارة المشاريع من حيث الزمن والموازنة المالية وتحت مظلة القواعد والمعايير الدولية المتبعة بهذا الخصوص.
- التأكد من تكامل البرمجيات التطبيقية وموارد التكنولوجيا ضمن عمليات البنك.
- تطبيق الأنظمة الخاصة بأمن وحماية المعلومات وأفضل الممارسات الدولية وكذلك سياسات وإجراءات البنك.

دائرة الامن السيبراني وحماية المعلومات:

- الإشراف بشكل مباشر على وضع برنامج وسياسة الأمن السيبراني وضمان تنفيذهما والعمل على مراجعتها وتحديثهما باستمرار.
- تقييم مدى كفاية و كفاءة برنامج وسياسة الأمن السيبراني .
- مراجعة فعالية ضوابط الحماية المعتمدة في سياسة الأمن السيبراني لدى البنك بشكل مستمر.
- تحديد و تقييم المخاطر السيبرانية.
- التوصية بتطبيق أفضل الممارسات الدولية فيما يتعلق بأمن المعلومات بما يتفق مع سياسات واستراتيجية البنك بهذا الخصوص.

وحدة خطة استمرارية الاعمال:

- تطوير الخطط الخاصة باستمرارية العمل في البنك.
- الإشراف على تنفيذ خطة استمرارية العمل.
- إعداد تقارير نتائج الفحوصات الدورية ومتابعة حل المشاكل الناتجة.
- إنشاء وتحديث سياسة إدارة استمرارية العمل.
- تطوير خطة استمرارية العمل للحوادث السيبرانية وفحصها بشكل مستمر.

إدارة الموارد البشرية:

- رفع مستوى المهارات التنافسية لكوادر البنك بشكل عام وكوادر تكنولوجيا المعلومات بشكل خاص من خلال

staff by training, to achieve the information technology department's goals.

- Coordinate with the related information technology departments to provide the appropriate training programs.
- Provide the human resources staff to generally execute the information technology projects according to the requirements of the governance and management of information and related technology code. In addition, provide the staff the required training in order to obtain specialized professional certificates (ISO، PMP، CISA).
- Provide the human resources staff to implement Cyber Security Program, and provide staff with the required professional certificates like ISO27001/2, CISM, CEH, NIST, CISSP
- Coordinate with Cyber and information Security Department Manager to provide the staff with awareness training regarding Cyber Security, and response plans.

التدريب، وذلك لغايات تحقيق أهداف دائرة تكنولوجيا المعلومات.

- التنسيق مع الدوائر المعنية بتكنولوجيا المعلومات من اجل توفير البرامج التدريبية المناسبة.
- توفير الكوادر البشرية اللازمة لتنفيذ مشاريع تكنولوجيا المعلومات بشكل عام وما تتطلبه "تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها" بشكل خاص، وتزويدها بالدورات التدريبية اللازمة من اجل الحصول على الشهادات المهنية المتخصصة مثل (ISO، PMP،CISA).
- توفير الكوادر البشرية اللازمة لتنفيذ برنامج الأمن السيبراني، وتزويدها بالدورات التدريبية اللازمة من أجل الحصول على الشهادات المهنية بهذا الخصوص مثل ISO، CISSP، NIST، CEH، CISM، 27001/2.
- التنسيق مع مدير دائرة الامن السيبراني وحماية المعلومات لتوعية وتدريب جميع الموظفين بخصوص الأمن السيبراني و أنواع التهديدات السيبرانية و خطط الطوارئ و طرق الاستجابة لحوادث الاختراق السيبراني .

Risk Management Department

- Provide assistance to other departments with the implementation of the approved risk management framework and the management of technology risks on the bank operations.
- Transparency in the disclosure of the benefits, cost, and information technology risk.
- In addition to responsibilities mentioned in Cyber and Information Security Governance and Management Code.

دائرة إدارة المخاطر:

- مساندة دوائر البنك المختلفة في تطبيق إطار إدارة المخاطر الموافق عليه، وإدارة المخاطر المتعلقة بتكنولوجيا المعلومات ضمن عمليات البنك المختلفة.
- الشفافية في الإفصاح عن تكاليف ومنافع ومخاطر تكنولوجيا المعلومات.
- بالإضافة الى المهام المدرجة في دليل حوكمة وإدارة الامن السيبراني وأمن المعلومات.

Compliance Department

- Assuring the compliance of information technology practices with the approved internal policies at the bank, regulations, and regulatory instructions.
- Assuring the compliance of information technology practices and its contribution in the bank's compliance with the regulations, systems, and instructions.

دائرة الامتثال

- ضمان امتثال ممارسات تكنولوجيا المعلومات للسياسات الداخلية المعتمدة لدى البنك والقوانين المعمول بها وتعليمات الجهات الرقابية.
- ضمان امتثال ممارسات تكنولوجيا المعلومات ومساهمتها في امتثال البنك للقوانين والأنظمة والتعليمات المتبعة.

Internal Audit Department

- Assuring the implementation of the instructions and reporting to the related parties according to the approved audit plan.
- Assuring the availability of efficient human resources staff and systems that help the department in their audit role regarding to this code perfectly.

دائرة التدقيق الداخلي

- التأكد من تطبيق التعليمات ورفع التقارير اللازمة للجهات المعنية وفقاً لخطة التدقيق المعتمدة.
- التأكد من توفر الكفاءات البشرية اللازمة والأنظمة المساعدة والتي تمكن الدائرة من القيام بدور التدقيق الخاص بهذا المجال على أكمل وجه.