قـــــرارات

الهيئة العامة للرقابة المالية

قرار مجلس إدارة الهيئة رقم ١٣٩ لسنة ٢٠٢٣

بتاريخ ٢٠٢٣/٦/٢١

بشأن التجهيزات والبنية التكنولوجية

وأنظمة المعلومات ووسائل الحماية والتأمين

اللازمة لاستخدام التكنولوجيا المالية لمزاولة الأنشطة المالية غير المصرفية

مجلس إدارة الهيئة العامة للرقابة المالية

بعد الاطلاع على قانون تنظيم وتنمية استخدام التكنولوجيا المالية فـــى الأنـــشطة المالية غير المصرفية الصادر بالقانون رقم ٥ لسنة ٢٠٢٢ ؛

وعلى قانون حماية البيانات الشخصية الصادر بالقانون رقم ١٥١ لسنة ٢٠٢٠ ؛

وعلى قرار مجلس إدارة الهيئة العامة للرقابـــة الماليـــة رقـــم ٥٨ لـــسنة ٢٠٢٢ بشأن الشروط والإجراءات المتطلبـــة للتأســـيس والتـــرخيص والموافقـــة للـــشركات والجهات الراغبة فى مزاولة الأنشطة المالية غيـــر المـــصرفية مـــن خـــلال تقنيـــات التكنولوجيا المالية ؛

وعلى موافقة مجلس إدارة الهيئة بتاريخ ٢٠٢٣/٦/٢١ ؛

قـــــرر :

(المادة الأولى)

يُعمل بالقواعد المرفقة فى شأن التجهيزات والبنية التكنولوجية وأنظمة المعلومـــات ووسائل الحماية والتأمين اللازمة لاستخدام التكنولوجيا المالية لمزاولة الأنشطة الماليـــة غير المصرفية .

(المادة الثانية)

على الشركات والجهات الراغبة فى الحصول على ترخيص أو موافقة لمزاولة الأنشطة المالية غير المصرفية باستخدام التكنولوجيا المالية ، استيفاء المتطلبات الواردة بالقواعد المرفقة وملاحقها ، وكذلك المستندات اللازمة والتى تحددها الهيئة .

(المادة الثالثة)

يُنشر هذا القرار فى الوقائع المصرية ، ويُعمل به من اليوم التالى لتاريخ نشره .

رئيس مجلس إدارة
الهيئة العامة للرقابة المالية
د . محمد فريد صالح

أولاً - تعريفات

فى تطبيق أحكام القواعد الآتية يقصد بالمصطلحات التالية المعنى المبين قرين كل منها :

١- **التجهيزات (Facilities Infrastructure)** : البنية التحتية من مرافق وتجهيزات لازمة لمراكز المعلومات (الأساسية والبديلة) والتى تشمل التجهيزات اللازمة للوصول للمرافق العامة من الكهرباء والاتصالات والمياه والصرف ، والأنظمة الداخلية للكهرباء والتهوية والتبريد وكابلات الشبكات واكتشاف ومكافحة الحريق والأمن المادى والتحكم فى الدخول والمراقبة من خلال الدوائر التليفزيونية المغلقة .

٢- **البنية التكنولوجية (Technology Infrastructure)** : البنية التحتية من أجهزة ونظم لازمة لمراكز المعلومات (الأساسية والبديلة) والتى تشمل أجهزة الشبكات ونقل البيانات ، وأجهزة الحاسبات ووسائل التخزين والأجهزة الطرفية المخصصة ، وأنظمة البنية التحتية للتطبيقات ، وأنظمة البنية التحتية لقواعد البيانات .

٣- **أنظمة المعلومات (Information Systems)** : الأنظمة المكونة من تطبيقات (Applications) وقواعد بيانات (Databases) يتم تطويرها لتؤدى مهام محددة دعما لعمليات ودورات العمل المستهدفة ، وتساهم فى التنسيق بين المستخدمين الداخليين أو الخارجيين ، وقد تشمل تطبيقات "ذكاء اصطناعي" (Artificial Intelligence) لتوفير درجات أعلى من التشغيل الآلى (automation)والدقة والسرعة فى أداء المهام .

٤- **وسائل الحماية والتأمين (Protection & Security Mechanisms)** : الآليات والمنهجيات المستخدمة لتوفير الآتي:

١- القدرة على منع وقوع المخاطر التكنولوجية (Technology Risk Prevention) التى من شأنها فقد الخصوصية والسرية (Confidentiality) ، أو السلامة والتكامل (Integrity) ، أو التوافر والإتاحة (Availability) ، للبنية التحتية للتجهيزات أو للبنية التحتية للبنية التكنولوجية أو لأنظمة المعلومات شاملة التطبيقات والبيانات .

٢- القدرة على التحمل والمرونة للتعافى واستعادة الإمكانيات والوظائف والبيانات بعد وقوع المخاطر (After-Risk Recovery & Resiliency) .

٥- المخاطر التكنولوجية (Technology Risk) : أى من التهديدات (Threats) أو نقاط الضعف (Vulnerabilities) الناشئة عن الاعتماد على البنية التكنولوجية وعلى أنظمة المعلومات فى أداء الأعمال والتى من شأنها حال وقوعها التأثير سلبًا على القدرة فى استمرار أداء تلك الأعمال .

٦- مرونة التحمل التكنولوجية (Technology Resiliency) : قدرة البنية التكنولوجية وأنظمة المعلومات على التحمل واستعادة الإمكانات والوظائف المستهدفة بعد وقوع خطر تكنولوجى .

٧- المخاطر السيبرانية (Cyber Risk) : أى من التهديدات (Threats) أو نقاط الضعف (Vulnerabilities) الناشئة عن اتصال البنية التحتية للتكنولوجيا الداخلية بالشبكات الخارجية أو الشبكة العالمية للتواصل (الإنترنت) .

٨- مرونة التحمل السيبرانية (Cyber Resiliency) : قدرة البنية التكنولوجية وأنظمة المعلومات على التحمل واستعادة الإمكانات والوظائف المستهدفة بعد وقوع خطر سيبرانى .

٩- أمن البيانات (الأمن السيبراني) فى مزاولة الأنشطة المالية غير المصرفية (NBFS-Cybersecurity) : إجراءات وعمليات تقنية وتنظيمية من شأنها الحفاظ على خصوصية البيانات وسريتها وسلامتها ووحدتها وتكاملها فيما بينها .

١٠- المنصة الرقمية المستخدمة فى مزاولة الأنشطة المالية غير المصرفية (NBFS-Digital Platform) : نموذج أعمال قائم على استخدام الوسائل التكنولوجية فى مزاولة الأنشطة المالية غير المصرفية وفى عرض المنتجات والخدمات المرتبطة بها على الأشخاص الراغبين فى الحصول عليها ، ويسمح بتبادل البيانات والمعلومات اللازمة لإتمام هذه التعاملات .

١١- الجهات الراغبة فى تقديم خدمات التعهيد (Outsourcing Technology Service Provider) : جهة تقدم خدمات تكنولوجية عن طريق اتفاقية تعهيد (Outsourcing Agreement) يكون الطرف العاهد (Outsourcing Party) هو المستفيد من الخدمة ويكون الطرف المعهد إليه (Outsourcee) هو مقدم الخدمة .

١٢- أنظمة التكنولوجيا الحرجة (NB-Critical-System) : نظام أو تطبيق يؤدى فشله إلى إضعاف قدرة الشركات والجهات العاملة فى الأنشطة المالية غير المصرفية عن الوفاء بالتزاماتها للمتعاملين أو للهيئة العامة للرقابة المالية .

١٣- بيانات العميل (Client Data) : بيانات تتعلق بالعميل أو حساباته أو الحسابات المرتبطة بالمنتجات المالية غير المصرفية أو المعاملات المرتبطة بتلك المنتجات المالية غير المصرفية .

١٤- معلومات التعرف الشخصية (Personally Identifiable Information) : أى بيانات للعميل يمكن استخدامها لتمييز أو تتبع هوية الشخص .

١٥- الإدارة التنفيذية للشركة (Executive Management) : وتشمل الوحدات التنظيمية المسئولة عن العمليات التخطيطية على المستوى التنفيذى (Planning Processes – Executive Level) ، والإشراف والرقابة الداخلية على الإجراءات التطبيقية على المستوى التشغيلى (Internal Auditing on Applied Procedures – Operational Level) لوظائف وخدمات أعمال الأنشطة المالية غير المصرفية أو لوظائف وخدمات تكنولوجيا المعلومات الممكنة .

١٦- الإدارة التشغيلية للشركة (Operational Management) : وتشمل الوحدات التنظيمية المسئولة عن الإجراءات التطبيقية على المستوى التشغيلى (Applied Procedures – Operational Level) ، لوظائف وخدمات أعمال الأنشطة المالية غير المصرفية أو لوظائف وخدمات تكنولوجيا المعلومات الممكنة .

١٧- العمليات الاستراتيجية (Strategy Processes) : وتشمل العمليات (Processes) المحققة لاستراتيجية مستهدفة من خلال دورة حياة معينة (Intended Life Cycle) ، وتكون لكل عملية مجموعة من المدخلات (Inputs) ومجموعة من المخرجات (Outputs) ، وعلى أن تكون المخرجات من كل عملية من العمليات مدخلات لعملية أخرى (أو لعمليات أخريات) ، ويكون للمجموعة خصائص الدورية والتكرار (Cyclical Iterations) وعلى أن يتحقق من دورة حياة العمليات الاستراتيجية "أغراض وقيم مضافة" (Purpose & Value-add) تتطور مع كل تكرار للدورة . وتمثل "العمليات الاستراتيجية" المستوى الاستراتيجى لإطار العمل المستهدف (Intended Framework) .

١٨- العمليات التخطيطية (Planning Processes) : وتشمل مجموعة العمليات (Processes) المحققة لخطط مستهدفة ، تنفيذًا لاستراتيجية معينة ، وتكون لكل عملية مجموعة من المدخلات (Inputs) ومجموعة من المخرجات (Outputs) ، وعلى أن تكون المخرجات من كل عملية من العمليات مدخلات لعملية أخرى (أو لعمليات أخريات) ، وعلى أن يتحقق من مجموعة العمليات التخطيطية "الأغراض والقيم المضافة" للاستراتيجية المعينة . وتمثل "العمليات التخطيطية" المستوى التنفيذى لإطار العمل المستهدف (Intended Framework) .

١٩- الإجراءات التطبيقية (Applied Procedures) : مجموعة الإجراءات (Procedures) المطبقة لعمليات تخطيطية معينة ، ويكون لكل إجراء "حادث مشغل" (trigger events) كما يكون له "حالات ناتجة" (resulting state) والتى قد تكون "مشغِلة" لإجراء آخر أو لإجراءات أخرى ، وعلى أن يتحقق من مجموعة الإجراءات التطبيقية "الأغراض والقيم المضافة" للعمليات التخطيطية المعينة . وتمثل الإجراءات التطبيقية "المستوى التشغيلي" لإطار العمل المستهدف (Intended Framework) .

٢٠- الجهات المخاطبة :

- الشركات الراغبة فى الحصول على ترخيص لمزاولة الأنشطة المالية غير المصرفية من خلال تقنيات التكنولوجيا المالية تحت مظلة القانون رقم ٥ لسنة ٢٠٢٢
- الشركات والجهات الحاصلة على ترخيص من الهيئة بمزاولة أي من الأنشطة المالية غير المصرفية تحت مظلة قوانين أخرى ، والراغبة فى الحصول على موافقة الهيئة لتباشر هذه الأنشطة باستخدام بعض مجالات التكنولوجيا المالية بنفسها ، أو من خلال إحدى جهات التعهيد تحت مظلة القانون رقم ٥ لسنة ٢٠٢٢
- الشركات الراغبة فى تقديم خدمات التعهيد فى مجالات التكنولوجيا المالية التى يمكن استخدامها فى مزاولة الأنشطة المالية غير المصرفية تحت مظلة القانون رقم ٥ لسنة ٢٠٢٢

ثانيًا – التجهيزات والبنية التكنولوجية وأنظمة المعلومات ووسائل الحماية والتأمين :

١- تلتزم الشركات والجهات المخاطبة بأحكام هذا القرار بتوفير التجهيزات التى تحددها الهيئة واللازمة للربط الآلى معها .

٢- تلتزم الشركات والجهات المخاطبة بأحكام هذا القرار بتوفير أجهزة الخوادم الأساسية التالية كحد أدنى لمتطلبات البنية التكنولوجية وأنظمة المعلومات :

- حاسبات تعمل كخوادم لقواعد البيانات Database Servers .
- حاسبات تعمل كخوادم للتطبيقات Application Servers .
- حاسبات تعمل كخوادم للويب Web Server .

على أن يتم مراعاة التالى :

- توفير نظم تشغيل حديثة ومرخصة .
- توفير الأنظمة والتطبيقات والبرمجيات – المُرخصة – اللازمة لتشغيل الخدمات المختلفة .
- الإتاحة الدائمة للخدمات دون توقف (High Availability) .

٣- تلتزم الشركات والجهات المخاطبة بأحكام هذا القرار بضوابط أمن المعلومات التالية كحد أدنى :

- نظام جدار نارى (Next Generation Firewall) لتأمين الشبكات والمعلومات .
- نظام حماية لأنظمة الويب (Web Application Firewall) .
- نظم أمن المعلومات لكافة الأصول .
- نظام رصد ومراقبة كافة الأحداث المرتبطة بالأصول بما يتيح الرصد اللحظى وإصدار التقارير المجمعة للأحداث المرتبطة .
- استخدام خاصية تشفير البيانات بما يتوافق مع المعايير العالمية فى تشفير قواعد البيانات .
- إجراء الصيانة الدورية للأجهزة والأنظمة وتأمين الشبكات والمعلومات مع مراعاة قواعد الضبط المناسبة لها وتحديثها بصفة مستمرة .

- تزويد جميع أجهزة الحاسب المتصلة بشبكة الشركة (حاسبات مكتبية ، محمولة ، خوادم) ببرامج محدثة ومرخصة لمكافحة الفيروسات والبرمجيات الضارة مثل نظام (Antivirus) ونظام (Endpoint Detection & Response) .
- عمل التحديث الدورى لأنظمة التشغيل والتطبيقات والبرمجيات المختلفة .
- الفصل المؤمن (Security Isolation) بين أنظمة الخدمات المختلفة وفقًا للمستوى الأمنى لها .
- عمل اختبارات معتمدة (Penetration Test) لقياس مدى تأمين الشبكات والتطبيقات والبرمجيات مرة واحدة سنويًا على الأقل وتسليم نسخة من هذه الاختبارات للهيئة ، ويجوز للهيئة طلب إعادة الاختبارات إذا تبين وجود نقاط ضعف تستدعى ذلك .
- إبلاغ الهيئة عند حدوث اختراقات لأمن المعلومات (Security Incidents) التى تحدث على مستوى البنية الأساسية للمعلومات والأنظمة العاملة عليها .
- تأمين الموقع الإلكترونى بشهادة تأمين إلكترونية سارية مخصصة للتعريف وتشفير البيانات (SSL Certificate) ، بحيث تظهر للعملاء عند تصفحهم الموقع الالكترونى بشهادة تأمين الكترونية .
- إصدار رقم فريد (Unique Session ID) ، مضافًا إليه ختم التوقيت (Time Stamp) لكل اتصال حال فتح الاتصال عند التحقق من الدخول .
- تسجيل الأنشطة (Logging Activities) التى تحدث على جميع الأجهزة والأنظمة مثل (System Logs, Security Logs, Application Logs) وما تعتمد عليه من أجهزة مساعدة مثل (الحاسبات ، وأجهزة شبكات ، وأجهزة تأمين معلومات) لمدة لا تقل عن خمس سنوات من تاريخ حدوث النشاط .
- الاحتفاظ بسجلات التعاملات على الحساب كاملة (Transactions Logs) بما فى ذلك جميع عمليات تسجيل الدخول والخروج وغيرها لمده لا تقل عن خمس سنوات .

٤- تلتزم الشركات والجهات المخاطبة بأحكام هذا القرار بالضوابط التالية :

- أن تكون قاعدة بيانات عملاء الشركة داخل الحدود الجغرافية لجمهورية مصر العربية .
- إبلاغ الهيئة فى حالة اتخاذ أى إجراءات لنقل مقرها أو مركز بياناتها (Data Center) بمدة لا تزيد على ٣٠ يومًا من تاريخ البدء فى اتخاذ الإجراءات .
- توفير مركز لخدمة العملاء يعمل لمدة ٢٤ ساعة يوميا للرد على استفسارات العملاء وحل المشاكل محل الاستفسار فور حدوثها .
- توقيع اتفاقية مستوى الخدمات (Service Level Agreement) بين كل من الشركة وعملائها .

٥- تعتبر الأطر العامة (إطار عمل حوكمة تكنولوجيا المعلومات وإطار عمل إدارة مخاطر التكنولوجيا وإطار عمل إدارة الأمن السيبراني) الواردة بالملاحق المرفقة أدلة استرشادية للممارسات الصحيحة ، وتحدد الهيئة الحد الأدنى اللازم اتباعه منها فى كل حالة على حدة .

ملحق (١) : إطار عمل حوكمة تكنولوجيا المعلومات

(ITG-F : Information Technology Governance Framework)

يقصد بالمصطلحات التالية المعنى المبين قرين كل منها :

إطار عمل حوكمة تكنولوجيا المعلومات : هو عنصر أساسى ومتمم لحوكمة المؤسسات ، وما يستتبعه من حوكمة لإدارة خدمات تكنولوجيا المعلومات (ITSM : Information Technology Service Management) . ويتكون إطار العمل من العمليات الاستراتيجية على المستوى الاستراتيجى ، والعمليات التخطيطية على المستوى التنفيذى ، والإجراءات التطبيقية على المستوى التشغيلى ، ويتبنى هذا العرض لإطار عمل "حوكمة تكنولوجيا المعلومات" منهجية التوجه الخدمى لتقديم خدمات تكنولوجيا المعلومات (ITSM) لكل من التجهيزات ، والبنية التكنولوجية ، وأنظمة معلومات ، ووسائل الحماية والتأمين ، ويجوز استخدام أفضل الممارسات وأطر العمل العالمية الأخرى ، أو تبنى إطار عمل بديل بعد العرض والموافقة من الهيئة .

ويجب على مجلس إدارة الشركة وضع واعتماد "استراتيجية تكنولوجيا المعلومات" ويكون ذلك من خلال "إطار عمل حوكمة تكنولوجيا المعلومات" والذى يكون معتمدًا من مجلس الإدارة وحاكمًا للإدارة التنفيذية وللإدارة التشغيلية . كما يجب على مجلس الإدارة أيضًا مراجعته بشكل دورى ، مرة واحدة على الأقل كل ثلاث سنوات ، ويكون لمجلس الإدارة تشكيل لجنة تسمى "لجنة حوكمة تكنولوجيا المعلومات" التابعة لمجلس الإدارة وتكون مسئولة عن الإشراف على تنفيذ إطار عمل حوكمة خدمات تكنولوجيا المعلومات والتأكد من ملائمة دورة العمل والمسئولين عن تنفيذها ، والتأكد من الالتزام بالإجراءات المطلوب اتباعها .

ويشمل إطار عمل تكنولوجيا المعلومات خمس عمليات استراتيجية أساسية لدورة الحياة (LP) ، تتضمن ٤٠ عملية تخطيطية على المستوى التنفيذى ، بالإضافة إلى ١٢ عملية استراتيجية مساندة لدورة الحياة (SP) ، تتضمن ٦٢ عملية تخطيطية على المستوى التنفيذى ، بإجمالى ١٧ عملية استراتيجية و١٠٢ عملية تخطيطية .

١- **العمليات الاستراتيجية :** هى العمليات التى تهدف إلى تحويل موارد مُقدِم خدمات تكنولوجيا المعلومات إلى خدمات ذات قيمة للعملاء ، ويجب توفير هذه الخدمات بمستويات متفق عليها من الجودة والتكلفة والمخاطر ، وتنقسم إلى :

أولاً - العمليات الاستراتيجية الأساسية لدورة الحياة ، وتشمل :

١- تحديد الاتجاه الاستراتيجى : ويقصد به اتخاذ قرارات استراتيجية لخدمة العملاء باستخدام تكنولوجيا المعلومات ، بدءًا من تقييم احتياجات العملاء وبيئة الأعمال ، وتشمل تحديد الخدمات التى يجب أن تقدم والقدرات المطلوبة لتقديمها .

٢- تصميم الخدمات الجديدة أو المعدلة : ويقصد به تحديد النتائج المتوقعة والخصائص المطلوبة لخدمة جديدة أو معدلة ، وتحديد البنية التحتية والقدرات الأخرى اللازمة لتقديم الخدمة ، وتطوير نهج تنفيذها .

٣- بناء الخدمات الجديدة أو المعدلة : ويقصد به بناء ونشر خدمات جديدة أو معدلة ، ويشمل تنسيق تطوير واقتناء واختبار جميع مكونات الخدمة المطلوبة .

٤- تشغيل الخدمات : ويقصد به ضمان تقديم الخدمات بفعالية وكفاءة ، بما يتماشى مع الالتزامات التعاقدية ، ويشمل تلبية طلبات الخدمة ، وحل الحوادث والمشكلات ، وكذلك تنفيذ المهام التشغيلية الروتينية .

٥- تحسين الخدمات : ويقصد به التحقق باستمرار مما إذا كانت الخدمات تقدم النتائج المطلوبة ، وتحديد إمكانات التحسين فى طريقة إنتاج الخدمات .

ثانيًا - العمليات الاستراتيجية المساندة لدورة الحياة ، وتشمل :

١- **إعداد وصيانة نظام إدارة الخدمة :** ويقصد به إنشاء نظام إدارة الخدمة وتشغيله وتحسينه باستمرار ، وتكون هذه العملية مسئولة عن إدارة سياسات وعمليات إدارة الخدمة كمكونات رئيسية فى نظام إدارة الخدمة .

٢- **الحفاظ على محفظة الخدمات :** ويقصد به ضمان احتواء محفظة الخدمات على معلومات متسقة ومحدثة حول الخدمات التى يديرها مقدم الخدمة ، ويتحقق ذلك من خلال التحكم فى التغييرات فى محفظة الخدمات وتعريفات الخدمة ، بالإضافة إلى إجراء مراجعات منتظمة لمحفظة الخدمات .

٣- إدارة علاقات العملاء : وتكون هذه العملية مسئولة عن الحفاظ على علاقة إيجابية مع العملاء ، وتحديد العملاء الجدد المحتملين ، وضمان الحصول على تعليقات منتظمة من العملاء الحاليين من خلال اجتماعات العملاء واستطلاعات الرأى ، وتوقيع اتفاقيات خدمة العملاء مع عملاء مقدم الخدمة .

٤- إدارة معلومات مكونات التهيئة : ويقصد بها الاحتفاظ بمعلومات حول عناصر مكونات التهيئة المطلوبة لتقديم الخدمات ، بما فى ذلك العلاقات بينهم .

٥- تقييم التغييرات والتنسيق لها : ويقصد به التحكم فى دورة حياة جميع التغييرات ويكون غرضها الرئيسى هو التمكين من إجراء تغييرات مفيدة ، مع الحد الأدنى من تعطيل الخدمات .

٦- إدارة المشاريع : ويقصد به تخطيط وتنسيق الموارد لإكمال مشروع فى الوقت والتكلفة والنطاق المستهدفين .

٧- ضمان الأمن : ويقصد به ضمان أمن مجموعة خدمات مقدم الخدمة ، ومواءمة الاحتياجات الأمنية لمقدم الخدمة مع احتياجات عملائه ، وضمان حماية الأنظمة والبيانات من التطفل ، وألا يتم الوصول إليها إلا من قبل الأطراف المصرح لها .

٨- الاستعداد لأحداث الكوارث : ويقصد به التأكد من أن مقدم الخدمة يمكنه توفير الحد الأدنى من مستويات الخدمة المتفق عليها فى حالة الأحداث التى تعتبر كوارث ، ويتم تحقيق ذلك فى المقام الأول من خلال تنفيذ آليات لمنع حدوث الكوارث ، ومن خلال وضع خطط وترتيبات الاستمرارية لاستعادة الخدمات بمجرد وقوع كارثة .

٩- ضمان الامتثال : ويقصد به ضمان امتثال الخدمات والعمليات والأنظمة للمتطلبات القانونية ذات الصلة والمعايير وسياسات المؤسسة .

١٠- إدارة الموارد البشرية : ويقصد به توفير المهارات ومستويات الموظفين المطلوبة من قبل مقدم الخدمة لتحقيق أهدافه .

١١- إدارة الموردين : ويقصد به التأكد من أن جميع الاتفاقيات مع الموردين تدعم احتياجات العمل ، وأن جميع الموردين يفون بالتزاماتهم التعاقدية .

١٢- إدارة الشئون المالية للخدمة : ويقصد به إدارة متطلبات الميزانية والمحاسبة والرسوم الخاصة بمقدم الخدمة .

٢- العمليات التخطيطية ، وتشمل :

أولاً - العمليات التخطيطية الأساسية لدورة الحياة ، وتشمل :

١- تحديد الاتجاه الاستراتيجى :

- تقييم الوضع الاستراتيجى الحالى : ويقصد به تقييم الوضع القائم لمقدم خدمات تكنولوجيا المعلومات والقدرات اللازمة لأدائها ، واحتياجات عملائها ، والبدائل المتاحة لتلك الخدمات ومكوناتها .
- تحديد توجيهات الاستخدام الاستراتيجى للتكنولوجيا : ويقصد به الموائمة مع الأهداف الاستراتيجية للأعمال .
- تحديد المبادرات الاستراتيجية : ويقصد به دراسة وتحديد المبادرات وأنسب الطرق لتنفيذها .
- البدء فى مشروعات تطوير الخدمات : ويقصد به تحديد مسئول الخدمة وتحديد وضمان الموازنة اللازمة ، وتحديد جدول زمنى .
- مراقبة المبادرات الاستراتيجية : ويقصد به التحقق من سيرها وفقًا للمخطط ، واتخاذ تدابير تصحيحية عند الضرورة .

٢- تصميم الخدمات الجديدة أو المعدلة :

- تحديد خصائص الخدمة المطلوبة : ويقصد به تحديد النتيجة المتوقعة والخصائص المطلوبة لخدمة جديدة أو معدلة ، ويتضمن ذلك تحديد خصائص أى خدمات داعمة يجب إعدادها أو تعديلها حتى تتمكن من تقديم الخدمة الجديدة .
- تصميم البنية التحتية المطلوبة : ويقصد به تحديد البنية التحتية المطلوبة والإمكانيات الأخرى التى يجب إنشاؤها قبل تقديم خدمة جديدة أو معدلة .
- تحديد منهجية التنفيذ : ويقصد به وصف كيفية إنشاء البنية التحتية والقدرات الأخرى المطلوبة لتقديم خدمة جديدة أو معدلة .
- الإعداد لتنفيذ الخدمة : ويقصد به تقديم مستندات تصميم الخدمة للمراجعة النهائية وتحديد ما إذا كانت الخدمة جاهزة للتنفيذ .

٣- بناءً الخدمات الجديدة أو المعدلة :

- التنسيق بين عمليات التطوير والشراء : ويقصد به بدء وتنسيق الأنشطة لتطوير أو شراء مكونات البنية التحتية والقدرات الأخرى المطلوبة لخدمة جديدة أو متغيرة .
- تطوير التطبيقات والأنظمة : ويقصد به تطوير أو تهيئة مكونات التطبيقات والأنظمة التى توفر الوظائف المطلوبة للخدمات ، وتتضمن هذه العملية تطوير تطبيقات وأنظمة مخصصة بالإضافة إلى تخصيص وتهيئة مكونات المنتجات التى تم شرائها .
- قبول تسليم مكونات الخدمة : ويقصد به تلقى مكونات الخدمة المطلوبة وتقديمها للتقييم الأولى ، وتضمن هذه العملية أن المكونات التى تفى بمعايير الجودة الصارمة فقط هى التى يُسمح لها بالدخول إلى مرحلة اختبار الخدمة الرئيسية .
- إنشاء أو تحديث الوثائق التشغيلية : ويقصد به تقديم إرشادات لتشغيل الخدمة الجديدة .
- اختبار مكونات الخدمة : ويقصد به اختبار جميع مكونات الخدمة وكذلك جميع الأدوات والآليات المطلوبة للنشر ، وتضمن هذه العملية نشر المكونات التى تلبى معايير الجودة الصارمة فقط فى البيئة الإنتاجية الحية .
- نشر مكونات الخدمة فى البيئة الإنتاجية : ويقصد به نشر مكونات الخدمة فى بيئة الإنتاج الحية .
- الإعداد لتفعيل الخدمة : ويقصد به تقييم ما إذا كانت جميع مكونات البنية التحتية والقدرات الأخرى موجودة قبل السماح بتفعيل الخدمات الجديدة .

٤- تشغيل الخدمات :

- دعم عملية تشغيل الخدمة : ويقصد به تقديم الدعم لعملية الخدمة ، من خلال ضمان توفر الموارد المطلوبة لتشغيل الخدمات ، وعن طريق تكوين وصيانة أنظمة الدعم التشغيلى ، وغيرها .
- تنظيم عملية الخدمة : ويقصد به تقديم إرشادات للإجراءات التى سيتم تنفيذها بواسطة طاقم التشغيل .
- مراقبة الخدمات : ويقصد به التأكد من مراقبة البنية التحتية للخدمة واستخدام الخدمة باستمرار ، ولتحديد الاستجابات المناسبة إذا تم اكتشاف أى مخالفات .

- إصدار تقارير جودة الخدمة : ويقصد به قياس جودة الخدمة المحققة على أساس منتظم وتحديد المجالات التى يجب تحسين جودة الخدمة فيها .
- أداء المهام التشغيلية الروتينية : ويقصد به تنفيذ المهام التشغيلية الروتينية المطلوبة لتقديم جودة الخدمة المتفق عليها على أساس مستدام .
- حل الحوادث وطلبات الخدمة : ويقصد بحل حوادث وطلبات الخدمة هو إعادة الخدمة إلى المستخدمين فى أسرع وقت ممكن .
- دعم حل الحوادث وطلبات الخدمة : ويقصد به تقديم الدعم لحل الحوادث وطلبات الخدمة ، على سبيل المثال عن طريق تكوين الأنظمة لإدارة الحوادث وطلبات الخدمة ، وعن طريق الحفاظ على مجموعة من نماذج طلب الخدمة والحوادث .
- تسجيل الحوادث وطلبات الخدمة : ويقصد به تسجيل جميع التفاصيل ذات الصلة بالحوادث وطلبات الخدمة ، والتحقق من إعطاء جميع التراخيص المطلوبة ، وتحديد أولويات الحوادث أو الطلبات .
- تلبية طلبات الخدمة : وتكون عادة إما طلبات للحصول على معلومات أو طلبات لتنفيذ تغييرات طفيفة (قياسية) مثل إعادة تعيين كلمة المرور .
- إبلاغ المستخدمين والعملاء بشكل استباقى : ويقصد به إبلاغ المستخدمين بإخفاقات الخدمة الفعلية أو الوشيكة بمجرد أن تصبح معروفة لدعم المستوى الأول ، بحيث يكون المستخدمون والعملاء فى وضع يمكنهم من التكيف مع الانقطاعات ، وتكون هذه العملية مسؤولة أيضًا عن توزيع معلومات مهمة أخرى ، مثل تنبيهات الأمان الحالية .
- حل الحوادث الكبرى : ويقصد به حل حادث كبير يتسبب فى انقطاعات خطيرة فى الأنشطة التجارية ويجب حلها على وجه السرعة ، بهدف استرداد سريع للخدمة ، ربما عن طريق حل بديل .

- حل الحوادث فى دعم المستوى الأول : ويقصد به حل حادث (انقطاع الخدمة) ضمن الإطار الزمنى المتفق عليه ، ويهدف إلى الاسترداد السريع للخدمة ، ربما من خلال تطبيق حل بديل ، وبمجرد أن يتضح أن دعم المستوى الأول غير قادر على حل الحادث نفسه أو عندما يتم تجاوز الأوقات المستهدفة لحل المستوى الأول ، يتم نقل الحادث إلى دعم المستوى الثانى .
- حل الحوادث فى المستوى الثانى : ويقصد به لحل حادث (انقطاع الخدمة) ضمن الإطار الزمنى المتفق عليه ، ويهدف إلى استرداد سريع للخدمة ، ربما عن طريق حل بديل ، وإذا لزم الأمر ، قد تشارك مجموعات دعم متخصصة فى هذا الشأن .
- مراقبة الحوادث وطلبات الخدمة : ويقصد به المراقبة المستمرة لحالة معالجة الحوادث المعلقة وطلبات الخدمة ، بحيث يمكن التصعيد واتخاذ التدابير المضادة إذا كان من المحتمل انتهاك أوقات الحل المتفق عليها .
- إغلاق الحوادث وطلبات الخدمة : ويقصد به تقديم سجلات طلب الخدمة والحادث إلى رقابة الجودة النهائية قبل الإغلاق الرسمى . ويهدف إلى التأكد من أن تاريخ حل الحادث أو طلب الخدمة موصوف بتفاصيل كافية ، ويجب تسجيل النتائج المستخلصة من حل الحوادث لاستخدامها فى المستقبل .
- حل المشكلات : ويقصد به إدارة دورة حياة جميع المشكلات ، حيث تكون المشكلة هى السبب الكامن وراء واحد أو عدة حوادث (محتملة) . وتهدف هذه العملية إلى منع وقوع حوادث الخدمة ، وتقليل تأثير الحوادث التى لا يمكن منعها .
- تحديد المشكلات بشكل استباقى : ويقصد به تحسين التوافر العام للخدمات من خلال تحديد المشكلات بشكل استباقى ، وتهدف هذه العملية إلى تحديد المشكلات وحلها أو توفير حلول بديلة مناسبة قبل حدوث مزيد من حوادث الخدمة .
- تصنيف المشكلات وترتيبها حسب الأولوية : ويقصد به تسجيل المشاكل وترتيبها حسب الأولوية مع العناية المناسبة ، من أجل تسهيل حل سريع وفعال .

- تحليل المشكلات وحلها : ويقصد به تحديد الأسباب الكامنة وراء المشكلات وتحديد أنسب حل للمشكلات وتوفير حل مؤقت إذا لم يتوفر حل كامل .
- مراقبة المشكلات المعلقة : ويقصد به المراقبة المستمرة للمشكلات المعلقة فيما يتعلق بحالة المعالجة الخاصة بها ، واتخاذ الإجراءات التصحيحية كما هو مطلوب .
- إغلاق المشاكل : ويقصد به التأكد من أن حل المشكلة كان ناجحًا وأن جميع المعلومات ذات الصلة محدثة .

٥- تحسين الخدمات :

- أداء مراجعات الخدمة : ويقصد به تحديد إمكانيات تحسين الخدمة ، يتضمن ذلك تقييم ما إذا كانت جودة الخدمة المقدمة تتماشى مع الالتزامات التعاقدية ، وكذلك اكتشاف نقاط الضعف فى طريقة تقديم الخدمة .
- تحديد تحسينات الخدمة : ويقصد به تحديد أهداف مبادرات تحسين الخدمة ونهج تنفيذها ، وهذا يشمل إعداد دراسات الجدوى للمبادرات .
- بدء مبادرات تحسين الخدمة : ويقصد به إطلاق مبادرات تحسين الخدمة ، ويتضمن ذلك الحصول على إذن من خلال طلب ميزانية وتقديم طلب للتغيير .
- تنفيذ تحسينات الخدمة : ويقصد به تنفيذ واختبار ونشر تحسينات الخدمة ، ويتضمن ذلك تحديث تعريفات واتفاقيات الخدمة ذات الصلة .
- مراقبة مبادرات تحسين الخدمة : ويقصد به تقييم ما إذا كانت مبادرات تحسين الخدمة تسير وفقًا للخطة ، وإدخال تدابير تصحيحية عند الضرورة .

ثانيًا – العمليات التخطيطية المساندة لدورة الحياة ، وتشمل :

١- إعداد وصيانة نظام إدارة الخدمة :

- تحديد تحسينات العملية : ويقصد به تحديد أهداف مبادرات تحسين العملية والنهج المتبع فى تنفيذها ، ويشمل إعداد دراسات الجدوى للمبادرات .
- بدء مبادرات تحسين العملية : ويقصد به إطلاق مبادرات تحسين العملية ، ويتضمن ذلك الحصول على إذن من خلال طلب ميزانية وتقديم طلب للتغيير .

- عمليات التصميم والسياسات : ويقصد به إنتاج تصميمات جديدة أو محدثة لعمليات إدارة الخدمة ، والتى يتم تنفيذها عادةً من خلال مبادرات تحسين العملية أو كجزء من مشاريع تطوير الخدمة .
- تنفيذ تحسينات العملية : ويقصد به تنفيذ واختبار ونشر عمليات إدارة خدمة جديدة أو تحسينات على العمليات الحالية ، وهذا يشمل تحديث وثائق العملية ذات الصلة .
- مراقبة مبادرات تحسين العملية : ويقصد به تقييم ما إذا كانت مبادرات تحسين العملية تسير وفقًا للخطة ، وإدخال تدابير تصحيحية عند الضرورة .
- تشغيل العمليات : ويقصد به ضمان تشغيل العمليات بفعالية وكفاءة ، بما يتماشى مع أهداف مقدم الخدمة ، ويتضمن ذلك إدارة الموارد اللازمة لتشغيل العملية ، بالإضافة إلى إعداد التقارير عن أداء العملية .
- أداء مراجعات العملية : ويقصد به تقديم عمليات إدارة الخدمة إلى مراجعات أو عمليات تدقيق منتظمة ، وتحديد إمكانيات التحسين التى يجب معالجتها من خلال مبادرات تحسين العملية .

٢- الحفاظ على محفظة الخدمات :

- إضافة خدمات جديدة أو متغيرة إلى محفظة الخدمات : ويقصد به إضافة معلومات حول (مخطط) الخدمات الجديدة أو التى تم تغييرها بشكل ملحوظ إلى مجموعة الخدمات .
- تحديث محفظة الخدمات : ويقصد به تحديث المعلومات فى محفظة الخدمات .
- تنشيط الخدمات الجديدة أو المتغيرة : ويقصد به التحقق من أن الخدمات الجديدة أو التى تم تغييرها بشكل كبير جاهزة للتشغيل ، وللحصول على موافقة رسمية لتنشيط الخدمة .
- مراجعة محفظة الخدمات : ويقصد به إرسال محفظة الخدمات إلى المراجعات المنتظمة ، من أجل اكتشاف الأخطاء فى محفظة الخدمة أو التناقضات بين تعريفات الخدمة أو اتفاقيات الخدمة .

٣- إدارة علاقات العملاء :

- البحث عن عملاء جدد : ويقصد به تحديد العملاء الجدد المحتملين وتقديم عروض مقدم الخدمة إلى هؤلاء العملاء الجدد المحتملين .
- توقيع اتفاقيات خدمة العملاء أو إنهائها : ويقصد به توقيع اتفاقيات خدمة العملاء مع العملاء الذين يرغبون فى استخدام خدمات مقدم الخدمة ، وتكون هذه العملية مسؤولة أيضًا عن إنهاء اتفاقيات خدمة العملاء التى لم تعد مطلوبة .
- معالجة شكاوى العملاء : ويقصد به تسجيل شكاوى العملاء وتقييم ما إذا كانت الشكاوى مبررة وتحديد الخطوات المطلوبة للتعامل مع الشكاوى .
- مراقبة شكاوى العملاء : ويقصد به المراقبة المستمرة لحالة معالجة شكاوى العملاء المعلقة واتخاذ الإجراءات التصحيحية إذا لزم الأمر .
- عقد اجتماعات العملاء : ويقصد به التواصل مع العملاء بشكل منتظم للتعرف على احتياجاتهم وخططهم المستقبلية .
- إجراء استطلاعات رضا العملاء : ويقصد به تخطيط وتنفيذ وتقييم استطلاعات رضا العملاء المنتظمة ، ويكون الهدف الرئيسى من هذه العملية هو التعرف على المجالات التى لا يتم فيها تلبية توقعات العملاء قبل فقدان العملاء لمقدمى الخدمات البديلة .

٤- إدارة معلومات مكونات التهيئة :

- دعم إدارة معلومات مكونات التهيئة : ويقصد به إعداد وصيانة الأدوات اللازمة لإدارة فعالة لعناصر مكونات التهيئة (Configuration Items) ومعلومات مكونات التهيئة ذات الصلة .
- الحفاظ على نموذج مكونات التهيئة : ويقصد به تحديد الهيكل الأساسى لنموذج مكونات التهيئة (Configuration Model Structure) والحفاظ عليه ، بحيث يكون قادرًا على الاحتفاظ بجميع المعلومات حول عناصر مكونات التهيئة ، ويتضمن ذلك تحديد سمات أنواعها ومكوناتها الفرعية ، بالإضافة إلى أنواع العلاقات المطلوبة بينها .

- التحكم فى عناصر مكونات التهيئة : ويقصد به التأكد من عدم إضافة عناصر مكونات التهيئة أو تعديلها بدون التفويض المطلوب ، وأن هذه التعديلات مسجلة بشكل كافٍ فى نظام إدارة مكونات التهيئة .
- مراجعة التحكم فى عناصر مكونات التهيئة : ويقصد به إجراء فحوصات منتظمة ، والتأكد من أن المعلومات الواردة فى نظام إدارة مكونات التهيئة هى تمثيل دقيق لمعلومات عناصر مكونات التهيئة المثبتة بالفعل فى بيئة الإنتاج الحية .

٥- تقييم التغييرات والتنسيق لها :

- دعم تقييم التغييرات : ويقصد به إعداد وصيانة الأدوات اللازمة لإدارة التغييرات بفعالية وكفاءة .
- تسجيل ومراجعة "طلبات التغيير" (Request for Changes) : ويقصد به تصفية طلبات التغيير التى لا تحتوى على جميع المعلومات المطلوبة للتقييم أو التى تعتبر غير عملية .
- تقييم التغييرات الطارئ : ويقصد به تقييم التغييرات الطارئة والتصريح بها فى أسرع وقت ممكن ، ويتم استدعاء هذه العملية إذا كان لا يمكن تطبيق إجراءات تقييم التغيير العادية .
- تقييم التغييرات (مدير التغيير) : ويقصد به تحديد مستوى التفويض المطلوب لتقييم التغيير المقترح ، ويتم تمرير تغييرات كبيرة إلى "المجلس الاستشارى للتغيير" (Change Advisory Board) للتقييم ، بينما يتم تقييم التغييرات الطفيفة على الفور والموافقة عليها من قبل مدير التغيير .
- تقييم التغييرات (المجلس الاستشارى للتغيير) : ويقصد به تقييم التغيير المقترح والتصريح به من خلال المجلس الاستشارى للتغيير . وإذا لزم الأمر ، تشارك مستويات أعلى من السلطة (مثل مجلس الإدارة) فى عملية التفويض .
- مراقبة التغييرات المفتوحة : ويقصد به مراقبة التغييرات المعلقة باستمرار فيما يتعلق بحالة تنفيذها واتخاذ الإجراءات التصحيحية حسب الاقتضاء .

- مراجعة وإغلاق التغييرات : ويقصد به تقييم مسار تنفيذ التغيير والنتائج المحققة ، من أجل التحقق من وجود تاريخ كامل للأنشطة للرجوع إليها فى المستقبل ، وللتأكد من تحليل أى أخطاء والدروس المستفادة .

٦- إدارة المشاريع :

- بدء المشاريع : ويقصد به تحديد أصحاب المصلحة والمسؤوليات والموارد المتاحة للمشروع ، وتحديد المخاطر والقيود والافتراضات التى تؤثر على المشروع ، وينتج عن هذه العملية ميثاق مشروع معتمد .
- تخطيط المشاريع : ويقصد به إنشاء خطة المشروع وتحديثها .
- مراقبة المشاريع : ويقصد به رصد التقدم المحرز فى المشروع واستهلاك الموارد والإبلاغ عنه ، وبدء الإجراءات التصحيحية إذا لزم الأمر .
- مراجعة المشاريع وإغلاقها : ويقصد به تقييم مسار المشروع والنتائج المحققة ، للتأكد من تحليل أى أخطاء والدروس المستفادة .

٧- ضمان الأمن :

- تقييم المخاطر الأمنية : ويقصد به تحديد المخاطر الأمنية التى يجب إدارتها من قبل مقدم الخدمة ، وتحديد الاستجابات المناسبة للمخاطر .
- تحديد التحسينات الأمنية : ويقصد به تحديد أهداف مبادرات تحسين الأمن ونهج تنفيذها ، ويشمل إعداد دراسات الجدوى للمبادرات .
- بدء مبادرات تحسين الأمان : ويقصد به إطلاق مبادرات تحسين الأمان ، ويتضمن ذلك الحصول على إذن من خلال طلب ميزانية وتقديم طلب للتغيير .
- تنفيذ آليات التحكم والضوابط الأمنية : ويقصد به تنفيذ واختبار ونشر آليات تحكم وضوابط أمنية جديدة أو محسنة .

- تشغيل آليات التحكم والضوابط الأمنية : ويقصد به ترتيب تدريب أمنى مناسب لموظفى وعملاء مقدم الخدمة ، ولضمان الصيانة والاختبار المنتظمين لآليات التحكم والضوابط الأمنية .
- مراجعة آليات التحكم والضوابط الأمنية : ويقصد به تقديم آليات التحكم والضوابط الأمنية إلى المراجعات المنتظمة ، من أجل تحديد إمكانيات التحسين التى يجب معالجتها من خلال مبادرات تحسين الأمن .

٨- الاستعداد لأحداث الكوارث :

- تقييم المخاطر المرتبطة بأحداث الكوارث : ويقصد به تحديد أحداث الكوارث التى يجب أن يديرها مقدم الخدمة ، وتحديد ترتيبات وآليات الاستمرارية المناسبة .
- تحديد تحسينات الاستمرارية : ويقصد به تحديد أهداف المبادرات لتحسين استمرارية الخدمة ونهج تنفيذها ، ويشمل إنشاء دراسات الجدوى للمبادرات .
- بدء مبادرات تحسين الاستمرارية : ويقصد به إطلاق مبادرات تهدف إلى ضمان أو تحسين استمرارية الخدمة ، ويتضمن ذلك الحصول على إذن من خلال طلب ميزانية وتقديم طلب للتغيير .
- تنفيذ ترتيبات الاستمرارية : ويقصد به تنفيذ واختبار ونشر ترتيبات وآليات استمرارية جديدة أو محسنة .
- تشغيل ترتيبات الاستمرارية : ويقصد به توفير وعى كافٍ لموظفى وعملاء مقدم الخدمة لأحداث الكوارث ، ولضمان الصيانة والاختبار المنتظمين لترتيبات وآليات الاستمرارية .
- مراجعة ترتيبات الاستمرارية : ويقصد به تقديم ترتيبات وآليات الاستمرارية للمراجعات المنتظمة ، من أجل تحديد إمكانيات التحسين التى يجب معالجتها من خلال مبادرات تحسين الاستمرارية .

٩- ضمان الامتثال :

- تحديد متطلبات الامتثال : ويقصد به تحديد متطلبات الامتثال التى يتعين على مزود الخدمة الوفاء بها .
- تحديد ضوابط الامتثال : ويقصد به تحديد الأهداف وتحديد تفاصيل الضوابط والآليات التى يجب وضعها للوفاء بمتطلبات الامتثال .
- أداء مراجعات الامتثال : ويقصد به تقديم ضوابط وآليات الامتثال للمراجعات المنتظمة ، وتحديد المجالات التى يجب تحسين الامتثال فيها .

١٠- إدارة الموارد البشرية :

- تحديد المهارات المطلوبة : ويقصد به تحديد المهارات التى تحتاج إلى تطوير ، بناءً على تقييم المجموعة الحالية من المهارات والاحتياجات المستقبلية .
- تطوير المهارات المطلوبة : ويقصد به تحديد وتنظيم ومراقبة تدابير التدريب والتعليم .
- تعيين موظفين جدد : ويقصد به اختيار موظفين جدد وتعيينهم بما يتماشى مع متطلبات مهارات مقدم الخدمة .

١١- إدارة الموردين :

- إعداد خدمات الدعم الخارجية : ويقصد به إعداد خدمات الدعم الخارجية ، ويتم استدعاء هذه العملية عادةً أثناء تنفيذ الخدمة إذا كانت هناك حاجة إلى خدمات دعم خارجية جديدة أو متغيرة لخدمة جديدة .
- شراء عناصر البنية التحتية : ويتم استدعاء هذه العملية أثناء تنفيذ الخدمة إذا كانت هناك حاجة إلى بنية تحتية تقنية جديدة لخدمة جديدة ، أو أثناء تشغيل الخدمة إذا كان سيتم شراء قطع الغيار .
- عقد اجتماعات الموردين : ويقصد به التواصل مع الموردين على أساس منتظم من أجل مناقشة أى قضايا تتعلق بأدائهم ، لتحديد إمكانيات تحسين التعاون والتعرف على خطط الموردين للمستقبل .

- مراجعة أداء الموردين : ويقصد به مراقبة أداء الموردين ، ولا سيما الجهات الراغبة فى تقديم خدمات التعهيد الذين يقدمون أو يقومون بتشغيل الخدمات أو العمليات . ويشمل ذلك التحقق مما إذا كانت أهداف الخدمة والالتزامات التعاقدية الأخرى قد تم الوفاء بها ، وكذلك تحديد أسباب عدم المطابقة وفرص التحسين .
- تجديد أو إنهاء اتفاقيات الموردين : ويقصد به التقييم على أساس منتظم ما إذا كانت الاتفاقيات مع الموردين لا تزال ذات صلة قبل تجديد تلك الاتفاقيات ، وإنهاء الاتفاقيات التى لم تعد هناك حاجة إليها .
- فحص فواتير الموردين : ويقصد به فحص فواتير الموردين الواردة للتأكد من صحتها قبل إرسالها إلى الإدارة المالية للتسوية .
- التعامل مع نزاعات الموردين : ويقصد به تسجيل نزاعات الموردين ، وتقييم النزاعات والحجج الأساسية الخاصة بهم ، وتحديد الخطوات المطلوبة لحل النزاعات .
- مراقبة نزاعات الموردين : ويقصد به المراقبة المستمرة لحالة معالجة نزاعات الموردين المعلقة واتخاذ الإجراءات التصحيحية إذا لزم الأمر .

١٢- إدارة الشئون المالية للخدمة :

- الحفاظ على إطار الإدارة المالية : ويقصد به تحديد الأطر اللازمة لإدارة بيانات التخطيط المالى وتكاليفه ، وتخصيص التكاليف على الخدمات وعمليات إدارة الخدمة .
- أداء التخطيط المالى : ويقصد به تحديد الموارد المالية المطلوبة خلال فترة التخطيط التالية ، وتخصيص تلك الموارد لتحقيق أفضل الفوائد .
- إعداد التقارير المالية : ويقصد به تحليل هيكل تكاليف توفير الخدمة وتقييم ربحية الخدمات ، وتعد التقارير المالية الناتجة مدخلاً هامًا لتحسين نطاق خدمات مزود الخدمة .
- إصدار فواتير العميل : ويقصد به إصدار فواتير مقابل الخدمات للعملاء .

ملحق (٢) : إطار عمل إدارة مخاطر التكنولوجيا

(TRM-F : Technology Risk Management Framework)

وهو إطار العمل المنظم لإدارة مخاطر التكنولوجيا (TRM : Technology Risk Management) كعنصر أساسى ومتمم لإدارة مخاطر المؤسسات (ERM : Enterprise Risk Management) . ويتكون إطار العمل من العمليات الاستراتيجية على المستوى الاستراتيجى ، والعمليات التخطيطية على المستوى التنفيذى ، والإجراءات التطبيقية على المستوى التشغيلى ، ويتبنى هذا العرض لإطار عمل "إدارة مخاطر التكنولوجيا" مبدأ الرقابة على أساس المخاطر التى تتبناه الهيئة العامة للرقابة المالية ، بما يتوافق مع المعايير الدولية لأطر عمل إدارة المخاطر من المعهد الوطنى للمعايير والتكنولوجيا (NIST) لكل من التجهيزات ، والبنية التكنولوجية ، وأنظمة المعلومات ، ووسائل الحماية والتأمين . ويجوز استخدام أفضل الممارسات وأطر العمل العالمية الأخرى ، أو تبنى ممارسات بديلة بعد العرض على الهيئة لإثبات فعاليتها فى معالجة ما قد تتعرض له الشركات والجهات المالية غير المصرفية من مخاطر التكنولوجيا ، وأخذ موافقة الهيئة على هذه الممارسات البديلة ، ويشمل الضوابط الحاكمة لتوافر التجهيزات والبنية التكنولوجية وأنظمة المعلومات ووسائل الحماية والتأمين من منظور "إدارة مخاطر التكنولوجيا" :

وتنشأ المخاطر الناشئة عن استخدام التكنولوجيا من فشل أو خروقات أنظمة تكنولوجيا المعلومات أو التطبيقات أو المنصات أو البنية التحتية ، مما قد يؤدى إلى خسارة مالية أو اضطرابات فى الخدمات أو العمليات المالية غير المصرفية أو الإضرار بسمعة الشركات والجهات المالية غير المصرفية .

وتعزيز قدرتها على الصمود التكنولوجى ضد الاضطرابات التشغيلية للحفاظ على الثقة فى النظام المالى غير المصرفى ، ويتطلب التطور المتزايد للتهديدات السيبرانية أيضًا زيادة اليقظة والقدرة على الاستجابة للتهديدات الناشئة . ويجب أن يكون ضمان هذا التوافر المستمر للخدمات الأساسية للعملاء والحماية الكافية لبيانات العملاء ، من الأولويات الحرجة للشركات وللجهات المالية غير المصرفية .

ويجب على مجلس الإدارة وضع واعتماد "استراتيجية إدارة مخاطر التكنولوجيا" والتى تكون مرتبطة ومتماشية مع "استراتيجية تكنولوجيا المعلومات" ومع البنية الهيكلية لأعمال الأنشطة المالية غير المصرفية ، ويكون ذلك من خلال "إطار عمل إدارة مخاطر التكنولوجيا" والذى يكون معتمدًا من مجلس الإدارة وحاكمًا للإدارة التنفيذية وللإدارة التشغيلية . كما يجب على مجلس الإدارة أيضًا مراجعته بشكل دورى ، مرة واحدة على الأقل كل ثلاث سنوات . ويكون لمجلس الإدارة تشكيل "لجنة إدارة مخاطر التكنولوجيا" التابعة لمجلس الإدارة تكون مسئولة عن الإشراف على تنفيذ إطار عمل إدارة المخاطر والتأكد من ملائمة دورة العمل والمسئولين عن تنفيذها ، والتأكد من الالتزام بالإجراءات المطلوب اتباعها .

يشمل إطار العمل هذا على : ٤ عمليات استراتيجية لدورة الحياة للمخاطر (LRP : Life-cycle Risk Process) ، تشمل "الهيكلة" (Frame) و"التقييم" (Assess) و"المجابهة" (Response) و"المراقبة" (Monitor) للمخاطر ، والتى تتكامل مع ٧ عمليات استراتيجية لدورة الحياة للأنظمة وآليات التحكم (SCP : Systems & Controls Process) ، تشمل "التحضير" (Prepare) والتصنيف" (Categorize) و"الاختيار" (Select) و"التنفيذ" (Implement) و"التقييم" (Assess) و"السماح" .

(Authorize) و"المراقبة" (Monitor) للأنظمة وآليات التحكم ، وتتضمن الأربع عمليات الاستراتيجية لدورة الحياة للمخاطر ١٢ عملية تخطيطية على المستوى التنفيذى ، وتتضمن السبع عمليات الاستراتيجية لدورة الحياة للأنظمة وآليات التحكم ٤٧ عملية تخطيطية على المستوى التنفيذى . وعلى هذا يكون إجمالى العمليات على المستوى الاستراتيجى ١١ عملية استراتيجية ، كما يكون إجمالى العمليات على المستوى التنفيذى ٥٩ عملية تخطيطية .

١- العمليات الاستراتيجية :

أولاً - العمليات الاستراتيجية لدورة الحياة للمخاطر ، وتشمل :

١- الهيكلة للمخاطر (Framing Risk) : ويقصد به إصدار استراتيجية إدارة المخاطر التى تتناول كيفية تقييم المخاطر ، والاستجابة لها ومراقبتها ، وتوضح استراتيجية إدارة المخاطر الافتراضات المحددة والقيود ودرجات تحمل المخاطر والأولويات المستخدمين لاتخاذ قرارات الاستثمار والعمليات . وتتضمن استراتيجية إدارة المخاطر أيضًا أى قرارات واعتبارات على المستوى الاستراتيجى حول كيفية إدارة المخاطر التى تتعرض لها العمليات والأصول التنظيمية والأفراد .

٢- التقييم للمخاطر (Assessing Risk) : ويقصد به تحديد أولويات وتقدير المخاطر على العمليات التنظيمية للأعمال (متضمنة الرسالة والوظائف والانطباع والسمعة) ، والأصول التنظيمية للأعمال ، والأفراد ، الناتجة عن تشغيل واستخدام أنظمة المعلومات .

وتتضمن عملية تقييم المخاطر تحديد التهديدات وأوجه الضعف التى يمكن استغلالها ، من حيث احتمالية الحدوث والتأثير السلبى المحتمل (أى حجم الضرر) .

٣- المجابهة للمخاطر (Responding to Risk) : ويقصد به تحديد كيفية مجابهة المخاطر ، عن طريق تقييم ، وتقرير ، وتنفيذ مسارات العمل المناسبة لقبول ، أو تجنب ، أو تخفيف ، أو مشاركة ، أو نقل المخاطر على العمليات والأصول التنظيمية ، والأفراد ، والناتجة عن تشغيل واستخدام أنظمة المعلومات .

٤- المراقبة للمخاطر (Monitoring of Risk) : ويقصد به : (١) التحقق من الامتثال ، (٢) تحديد الفعالية المستمرة لتدابير الاستجابة للمخاطر ، (٣) تحديد التغييرات المؤثرة على المخاطر فى أنظمة المعلومات التنظيمية وبيئات التشغيل .

ويعطى تحليل نتائج المراقبة القدرة على الحفاظ على الوعى بالمخاطر التى يتم تكبدها ، وتسليط الضوء على الحاجة إلى إعادة النظر فى الخطوات الأخرى فى عملية إدارة المخاطر ، وبدء أنشطة تحسين العملية حسب الحاجة .

ثانيًا – العمليات الاستراتيجية لدورة الحياة للأنظمة وآليات التحكم (Systems & Controls Process) ، وتشمل :

١- التحضير على المستوى التنفيذى والتشغيلى للأنظمة : ويقصد به تنفيذ عمليات إدارة المخاطر بفعالية وكفاءة ، من حيث الجودة والتكلفة ، من خلال :

(١) تسهيل التواصل بين مجلس الإدارة والإدارة التنفيذية والإدارة التشغيلية ، (٢) تعزيز تحديد الضوابط المشتركة والحدود الدنيا الأساسية لها لتقليل العبء على الإدارة التنفيذية والإدارة التشغيلية وتكلفة تطوير الأنظمة وحمايتها ، (٣) تقليل تعقيد البنية التحتية لتكنولوجيا المعلومات من خلال تجميع وتوحيد وتحسين الأنظمة والتطبيقات من خلال نمذجة وهيكلة بنية الأعمال ، (٤) تحديد وترتيب الأولويات ، وتركيز الموارد على الأصول الأعلى قيمة ، والتى تتطلب مستويات متزايدة من الحماية .

٢- التصنيف للأنظمة (Categorize Systems) : ويقصد به إبلاغ عمليات ومهام إدارة المخاطر التنظيمية من خلال تحديد التأثير السلبى على العمليات والأصول التنظيمية والأفراد فيما يتعلق بفقدان السرية والنزاهة وتوافر الأنظمة والمعلومات التى تتم معالجتها وتخزينها ونقلها بواسطة تلك الأنظمة .

٣- الاختيار لآليات التحكم (Select Controls) : ويقصد به تحديد الضوابط اللازمة لآليات التحكم وتخصيصها وتوثيقها لحماية نظام المعلومات والبنية الهيكلية للأعمال ، وبما يتناسب مع المخاطر التى تتعرض لها العمليات والأصول التنظيمية والأفراد .

٤- التنفيذ لآليات التحكم (Implement Controls) : ويقصد به تنفيذ آليات التحكم فى خطط الأمن والخصوصية للنظام وللبنية الهيكلية للأعمال وللتوثيق فى ملف إعدادات التهيئة المرجعى .

٥- التقييم لآليات التحكم (Assess Controls) : ويقصد به تحديد ما إذا كانت آليات التحكم والضوابط المختارة للتنفيذ قد تم تنفيذها بشكل صحيح ، وتعمل على النحو المنشود ، وتنتج النتيجة المرجوة فيما يتعلق بتلبية متطلبات الأمن والخصوصية للنظام وللبنية الهيكلية للأعمال .

٦- السماح للأنظمة (Authorize Systems) : ويقصد به توفير المساءلة التنظيمية من خلال مطالبة مسؤول الإدارة العليا بتحديد ما إذا كانت مخاطر الأمن والخصوصية (بما فى ذلك مخاطر سلسلة التوريد) للعمليات والأصول التنظيمية أو الأفراد بناءً على تشغيل نظام أو استخدام ضوابط مشتركة ، أمر مقبول .

٧- المراقبة للأنظمة ولآليات التحكم (Monitor Controls) : ويقصد به الحفاظ على الوعى المستمر بالحالة حول الوضع الأمنى والخصوصية لنظام المعلومات والمنظمة لدعم قرارات إدارة المخاطر .

٢- العمليات التخطيطية :

أولاً - العمليات التخطيطية لدورة الحياة المخاطر ، وتشمل :

١- تحديد الإطار الحاكم للمخاطر (Risk Framing) :

- افتراضات المخاطر : ويقصد به تحديد الافتراضات التى تؤثر على كيفية تقييم المخاطر والاستجابة لها ومراقبتها ، متضمنة مصادر التهديد ، ونقاط الضعف ، والعواقب ، والاحتمالات .
- محددات المخاطر : ويقصد به تحديد القيود المفروضة على إجراء تقييم المخاطر والاستجابة للمخاطر وأنشطة مراقبة المخاطر .
- تحمل المخاطر : ويقصد به تحديد مستوى تحمل المخاطر على مستوى البنية الهيكلية للأعمال .
- الأولويات والمفاضلات : ويقصد به تحديد الأولويات والمفاضلات بين البدائل فى إدارة المخاطر .

٢- تقييم المخاطر (Risk Assessment) :

- تحديد التهديدات وأوجه الضعف : ويقصد به تحديد التهديدات ونقاط الضعف فى أنظمة المعلومات التنظيمية والبيئات التى تعمل فيها الأنظمة .
- تحديد المخاطر : ويقصد به تحديد المخاطر على العمليات والأصول التنظيمية والأفراد إذا ما تمكنت التهديدات المحددة من استغلال نقاط الضعف المحددة .

٣- المجابهة للمخاطر (Responding to Risk) :

- تحديد المجابهة للمخاطر : ويقصد به تحديد مسارات العمل البديلة للاستجابة للمخاطر المحددة أثناء تقييم المخاطر ، والتى قد تتضمن قبول المخاطر ، وتجنب المخاطر ، والتخفيف من حدة المخاطر ، وتقاسم المخاطر أو تحويلها .
- تقييم البدائل : ويقصد به تقييم مسارات العمل البديلة للاستجابة للمخاطر .
- اتخاذ قرار الاستجابة للمخاطر : ويقصد به تحديد مسار العمل المناسب للاستجابة للمخاطر .
- تنفيذ الاستجابة للمخاطر : ويقصد به تنفيذ مسار العمل المختار للاستجابة للمخاطر .

٤- المراقبة للمخاطر (Monitoring Risk) :

- استراتيجية مراقبة المخاطر : ويقصد به تطوير استراتيجية مراقبة المخاطر والتى تتضمن الغرض من أنشطة المراقبة وأنواعها وتوقيتات تكرارها .
- مراقبة المخاطر : ويقصد به مراقبة أنظمة المعلومات التنظيمية وبيئات التشغيل على أساس مستمر للتحقق من الامتثال ، وتحديد فعالية تدابير الاستجابة للمخاطر ، وتحديد التغييرات .

ثانيًا – العمليات التخطيطية لدورة الحياة للأنظمة وآليات التحكم :

١- التحضير على المستوى التنفيذى والتشغيلى للأنظمة (Prepare Executive & Operational Levels) .

التحضير على المستوى التنفيذى للأنظمة :

- أدوار إدارة المخاطر : ويقصد به تحديد الأفراد وتعيين أدوار رئيسية لتنفيذ إطار عمل إدارة المخاطر .
- استراتيجية إدارة المخاطر : ويقصد به وضع استراتيجية لإدارة المخاطر تتضمن تحديدًا وتعبيرًا عن تحمل المخاطر التنظيمية .
- تقييم المخاطر التنظيمية للأعمال : ويقصد به اكتمال تقييم المخاطر على المستوى التنظيمى للأعمال أو تحديث تقييم المخاطر الحالى .

- الحدود الدنيا الأساسية لآليات التحكم : ويقصد بـه تحديـد وإتاحـة الحـدود الدنيا الأساسية لآليات التحكم ، والتى تكون مخصصة ومتناسقة مع إطار عمل الأمن السيبرانى .
- تحديد آليات التحكم المشتركة : ويقصد به تحديد وتوثيق ونشر آليات الـتحكم المشتركة المتاحة لأنظمة المعلومات المختلفة .
- تحديد أولويات مستوى التأثير : ويقصد به أن يـتم تحديـد أولويـات أنظمـة المعلومات من حيث مستوى التأثير .
- استراتيجية المراقبة المستمرة على المستوى التنفيذى : ويقـصد بـه تطـوير وتنفيذ استراتيجية لمراقبة فعالية الرقابة على المستوى التنفيذى للأنظمة .

التحضير على المستوى التشغيلى للأنظمة :

- التركيز على الرسالة والغرض ووظائف الأعمال : ويقصد به تحديد الرسـالة والغرض ووظائف الأعمال المهمة التى يهدف النظام إلى دعمها .
- أصحاب المصلحة فى النظام : ويقصد به تحديد أصحاب المصلحة الذين لهـم مصلحة فى النظام .
- تحديد الأصول : ويقصد به تحديد وترتيب أهمية الأصول لأصحاب المصلحة .
- حدود الحصول على الصلاحية : ويقصد به تحديد الحدود التى يلزم الحـصول على صلاحية للدخول من خلالها على النظام .
- أنواع المعلومات : ويقصد به تحديد أنواع المعلومـات التـى تـتم معالجتهـا وتخزينها ونقلها بواسطة النظام .
- دورة حياة المعلومات : ويقصد به تحديد وفهـم جميـع مراحـل دورة حيـاة المعلومات لكل نوع من أنواع المعلومات التى تـتم معالجتهـا أو تخزينهـا أو نقلها بواسطة النظام .
- تقييم المخاطر على المستوى التشغيلى للنظام : ويقـصد بـه اكتمـال تقيـيم المخاطر على مستوى النظام أو تحديث تقييم المخاطر الحالى .

- تعريف المتطلبات : ويقصد به تحديد متطلبات الأمن والخصوصية وتحديد أولوياتها .
- البنية الهيكلية للأعمال : ويقصد به تحديد وضع النظام داخل البنية الهيكلية للأعمال .
- تخصيص المتطلبات : ويقصد به تخصيص متطلبات الأمن والخصوصية للنظام وللبيئة التى يعمل فيها النظام .
- تسجيل النظام : ويقصد به تسجيل النظام لأغراض الإدارة والمساءلة والتنسيق والإشراف .

٢- التصنيف للأنظمة (Categorize Systems) :

- وصف نظام : ويقصد به وصف وتوثيق خصائص النظام .
- التصنيف الأمنى : ويقصد به تحديد التصنيف الأمنى للنظام ، بما فى ذلك المعلومات التى تتم معالجتها بواسطة النظام ، وعلى أن يتم توثيق نتائج التصنيف الأمنى فى خطط الأمن والخصوصية وإدارة مخاطر سلسلة الإمدادات (Supply Chain Risk Management) ، وعلى أن تتوافق نتائج التصنيف الأمنى مع البنية الهيكلية للأعمال ، وعلى أن تعكس نتائج التصنيف الأمنى استراتيجية إدارة المخاطر المعتمدة .
- مراجعة التصنيف الأمنى والموافقة عليه : ويقصد به مراجعة نتائج التصنيف الأمنى والموافقة على قرار التصنيف من قبل الإدارة العليا .

٣- الاختيار لآليات التحكم (Select Controls) :

- اختيار آليات التحكم : ويقصد به اختيار الحدود الدنيا الأساسية لضوابط وآليات التحكم لحماية النظام بما يتناسب مع المخاطر .
- تفصيل آليات التحكم : ويقصد به تفصيل الحدود الدنيا الأساسية لآليات التحكم لحماية النظام بما يتناسب مع المخاطر .
- تخصيص آليات التحكم : ويقصد به وجود منهجية لآليات التحكم مخصصة لنظام ، أو مشتركة لمجموعة من الأنظمة ، أو مختلطة ، وعلى أن يتم تحديد عناصر آليات التحكم (أى عناصر آلية أو فيزيائية أو بشرية) .

- توثيق عمليات تنفيذ التحكم المخطط لها : ويقصد به توثيق آليات التحكم وإجراءات التخصيص المرتبطة بها فى خطط الأمن والخصوصية أو المستندات المكافئة .
- استراتيجية المراقبة المستمرة للنظام : ويقصد به تطوير استراتيجية مراقبة مستمرة للنظام تعكس استراتيجية إدارة المخاطر .
- مراجعة الخطة والموافقة عليها : ويقصد به مراجعة واعتماد خطط الأمن والخصوصية التى تعكس اختيار آليات التحكم والضوابط اللازمة لحماية النظام وبيئة التشغيل المتناسبة مع المخاطر والموافقة عليها من قبل مسئول إدارة المخاطر التكنولوجية .

٤- التنفيذ لآليات التحكم (Implement Controls) :

- تنفيذ آليات التحكم : ويقصد به تنفيذ آليات التحكم والضوابط المحددة فى خطط الأمن والخصوصية النظام .
- تحديث معلومات تنفيذ آليات التحكم : ويقصد به توثيق التغييرات على التنفيذ المخطط لآليات التحكم والضوابط ، وعلى أن يتم تحديث خطط الأمن والخصوصية بناءً على المعلومات التى تم الحصول عليها أثناء تنفيذ آليات التحكم والضوابط .

٥- التقييم لآليات التحكم (Assess Controls) :

- اختيار المقيم للمهمة : ويقصد به اختيار مقيِّم أو فريق تقييم لإجراء تقييمات آليات التحكم ، وعلى أن يتم تحقيق المستوى المناسب من الاستقلالية للمقيم أو فريق التقييم المختار .
- خطة التقييم للمهمة : ويقصد به توفير الوثائق اللازمة لإجراء التقييمات للمقيم أو فريق التقييم ، وعلى أن يتم تطوير وتوثيق خطط تقييم الأمان والخصوصية ، ويتم مراجعة واعتماد خطط تقييم الأمان والخصوصية لتحديد التوقعات لتقييم الرقابة ومستوى الجهد المطلوب .

- تقييمات آليات التحكم : ويقصد به إجراء تقييمات أليات التحكم وفقًا لخطط تقييم الأمن والخصوصية ، وعلى أن يتم النظر فى فرص إعادة استخدام نتائج التقييم من التقييمات السابقة لتحسين فعالية عملية إدارة المخاطر من حيث الوقت والتكلفة ، وعلى أن يتم تعظيم استخدام التشغيل الآلى automation لإجراء تقييمات التحكم لزيادة سرعة وفعالية وكفاءة التقييمات .
- تقارير تقييم المهام : ويقصد به إصدار تقارير تقييم الأمن والخصوصية التى توفر النتائج والتوصيات .
- إجراءات المعالجة : ويقصد به اتخاذ إجراءات تصحيحية لمعالجة أوجه القصور فى آليات التحكم والضوابط المطبقة فى نظام وبيئة التشغيل ، وعلى أن يتم تحديث خطط الأمن والخصوصية لتعكس تغييرات تنفيذ آليات التحكم التى تم إجراؤها بناءً على التقييمات وإجراءات العلاج اللاحقة .
- خطة العمل ومخرجات محددة : ويقصد به وضع خطة عمل ومخرجات محددة عن خطط العلاج المقترحة للمخاطر غير المقبولة بناء على تقارير تقييم الأمن والخصوصية .

٦- السماح للأنظمة (Authorize Systems) :

- متطلبات ومرفقات السماح : ويقصد به تحديد متطلبات والمرفقات اللازم توفيرها وتقديمها للمسئول للموافقة على السماح للنظام أو لآليات التحكم بالتشغيل فى البيئة الإنتاجية .
- تحليل المخاطر وتحديدها : ويقصد به تقديم تحديد للمخاطر من قبل المسؤول المفوض يعكس استراتيجية إدارة المخاطر بما فى ذلك تحمل المخاطر .
- الاستجابة للمخاطر : ويقصد به توفير استجابات للمخاطر ، بناءً على المخاطر المحددة .
- قرار السماح : ويقصد به اتخاذ قرار الموافقة على أو رفض طلب السماح الخاص بالنظام أو آليات التحكم العامة .
- تقرير السماح : ويقصد به الإبلاغ عن قرارات السماح ونقاط الضعف الكبيرة والمخاطر للإدارة العليا .

٧- المراقبة للأنظمة ولآليات التحكم (Monitor Controls) :

- تغييرات النظام والبيئة : ويقصد به مراقبة نظام المعلومات وبيئة التشغيل وفقاً لاستراتيجية المراقبة المستمرة .
- التقييمات الجارية : ويقصد به إجراء التقييمات المستمرة لفعالية الرقابة وفقًا لاستراتيجية المراقبة المستمرة .
- الاستجابة للمخاطر المستمرة : ويقصد به تحليل مخرجات أنشطة المراقبة المستمرة والاستجابة لها بشكل مناسب .
- تحديثات متطلبات ومرفقات السماح : ويقصد به تحديث وثائق إدارة المخاطر بناءً على أنشطة المراقبة المستمرة .
- الإبلاغ عن الأمن والخصوصية : ويقصد به إيجاد عملية للإبلاغ عن وضع الأمن والخصوصية إلى المسؤول المفوض وغيره من الإدارة العليا .
- السماح المستمر : ويقصد به قيام مسئولى الموافقة على السماح للأنظمة ولآليات التحكم باستخدام نتائج أنشطة المراقبة المستمرة والإبلاغ عن التغييرات فى تحديد المخاطر وقرارات القبول .
- التخلص من نظام : ويقصد به تطوير وتنفيذ استراتيجية للتخلص من النظام ، حسب الحاجة .

ملحق (٣) : إطار عمل إدارة الأمن السيبراني

(CSM-F : Cybersecurity Management Framework)

وهو إطار العمل المنظم لإدارة الأمن السيبرانى (Cybersecurity Management) كعنصر أساسى ومتمم لإدارة أمن المؤسسات (ESM : Enterprise Security Management) . ويتكون إطار العمل من العمليات الاستراتيجية على المستوى الاستراتيجى ، والعمليات التخطيطية على المستوى التنفيذى ، والإجراءات التطبيقية على المستوى التشغيلى ، وتتبنى الهيئة مبدأ الموائمة بين "إدارة الأمن السيبراني" ، و"إدارة المخاطر التكنولوجية" ، حيث تكون المخاطر السيبرانية أحد أنواع المخاطر التكنولوجية . وعلى هذا تكون دورة حياة إدارة المخاطر السيبرانية على المستوى الاستراتيجى مماثلة لدورة حياة إدارة المخاطر التكنولوجية ("الهيكلة" و"التقييم" و"المجابهة" و"المراقبة" للمخاطر التكنولوجية) .

ومن خلال فهم درجة تحمل المخاطر ، يمكن للشركات أو الجهات المالية غير المصرفية تحديد الأولوية لأنشطة الأمن السيبرانى ، مما يمكّن من اتخاذ قرارات مستنيرة بشأن نفقات الأمن السيبرانى . ويوفر تنفيذ مبادرات إدارة المخاطر القدرة على تحديد التعديلات والإبلاغ عنها لمبادرات الأمن السيبرانى . وقد يتم التعامل مع المخاطر بطرق مختلفة ، بما فى ذلك تخفيف المخاطر ، أو تحويل المخاطر ، أو تجنب المخاطر ، أو قبول المخاطر ، اعتمادًا على التأثير المحتمل على تقديم الخدمات الهامة .

وتعمل الضوابط المنصوص عليها كدليل للممارسات السليمة لإدارة الأمن السيبرانى والمخاطر السيبرانية .

ويتبنى هذا العرض لإطار عمل "إدارة الأمن السيبراني" ، منهجية "دورة الحياة لتحسين الأمن السيبراني" من المعهد الوطنى للمعايير والتكنولوجيا (NIST : National Institute for Standards & Technology) لكل من التجهيزات ، والبنية التكنولوجية ، وأنظمة المعلومات ، ووسائل الحماية والتأمين .

ويجب على مجلس الإدارة وضع واعتماد "استراتيجية إدارة الأمن السيبراني" والتى تكون مرتبطة ومتماشية مع "استراتيجية تكنولوجيا المعلومات" ومع البنية الهيكلية لأعمال الأنشطة المالية غير المصرفية ، ويكون ذلك من خلال "إطار عمل إدارة الأمن السيبراني" والذى يكون معتمدًا من مجلس الإدارة وحاكمًا للإدارة التنفيذية وللإدارة التشغيلية . كما يجب على مجلس الإدارة أيضًا مراجعته بشكل دورى ، مرة واحدة على الأقل كل ثلاث سنوات . ويكون لمجلس الإدارة تشكيل "لجنة إدارة الأمن السيبراني" التابعة لمجلس الإدارة تكون مسئولة عن الإشراف على تنفيذ إطار عمل إدارة الأمن السيبرانى والتأكد من ملائمة دورة العمل والمسئولين عن تنفيذها ، والتأكد من الالتزام بالإجراءات المطلوب اتباعها .

ويشتمل هذا الإطار على : ٥ عمليات استراتيجية لدورة الحياة للأمن السيبرانى (Cybersecurity Process) ، تشمل "التحديد" (Identify) و"الحماية" (Protect) و"الرصد" (Detect) و"الاستجابة" (Respond) و"الاستعادة" (Recover) للأمن السيبرانى وما تتضمنه من ٢٣ عملية استراتيجية فرعية ، وما يرتبط بهم من ١٠٨ عملية تخطيطية على المستوى التنفيذى .

١- العمليات الاستراتيجية :

العمليات الاستراتيجية لدورة حياة الأمن السيبرانى (Cybersecurity Process) ، وتشمل :

١- التحديد (Identify) : ويقصد به تطوير الفهم التنظيمى لإدارة مخاطر الأمن السيبرانى للأنظمة والأصول والبيانات والقدرات .

- إدارة الأصول (Asset Management) : ويقصد به تحديد وإدارة البيانات والموظفين والأجهزة والأنظمة والمرافق التى تمكن الشركة أو الجهة المالية غير المصرفية من تحقيق أغراض العمل بما يتوافق مع أهميتها النسبية للأهداف التنظيمية واستراتيجية المخاطر لها .

- بيئة الأعمال (Business Environment) : ويقصد به فهم رسالة الشركة أو الجهة المالية غير المصرفية وأهدافها وأصحاب المصلحة وأنشطتها وتحديد أولوياتها؛ وتُستخدم هذه المعلومات لإبلاغ أدوار ومسؤوليات وقرارات إدارة المخاطر فى مجال الأمن السيبرانى .
- الحوكمة (Governance) : ويقصد بها فهم السياسات والإجراءات والعمليات لإدارة ومراقبة المتطلبات التنظيمية والقانونية والمتعلقة بالمخاطر البيئية والتشغيلية وإبلاغ إدارة مخاطر الأمن السيبرانى .
- تقييم المخاطر (Risk Assessment) : ويقصد به تفهم الشركة أو الجهة المالية غير المصرفية مخاطر الأمن السيبرانى للعمليات التنظيمية (بما فى ذلك الرسالة أو الوظائف أو الانطباع أو السمعة) والأصول التنظيمية والأفراد .
- استراتيجية إدارة المخاطر (Risk Management Strategy) : ويقصد به وضع أولويات الشركة أو الجهة المالية غير المصرفية والقيود وتحمل المخاطر والافتراضات واستخدامها لدعم قرارات المخاطر التشغيلية .
- إدارة مخاطر سلسلة التوريد (Supply Chain Risk Management) : ويقصد به وضع أولويات الشركة أو الجهة المالية غير المصرفية والقيود ودرجة تحمل المخاطر والافتراضات واستخدامها لدعم قرارات المخاطر المرتبطة بإدارة مخاطر سلسلة التوريد . ويتم تخطيط وتنفيذ عمليات لتحديد وتقييم وإدارة مخاطر سلسلة التوريد .

٢- الحماية (Protect) : ويقصد بها تطوير وتنفيذ الضمانات المناسبة لضمان تقديم خدمات البنية التحتية الحيوية .

- إدارة الهوية والمصادقة والتحكم فى الوصول (Authentication & Access Control) : ويقصد به الوصول إلى الأصول المادية والمنطقية والملحقات المرتبطة بها على المستخدمين المعتمدين والعمليات والأجهزة ، ويتم إدارتها بما يتفق مع المخاطر المقدرة للوصول غير المصرح به إلى الأنشطة والمعاملات المصرح بها .

- الوعى والتدريب (Awareness & Training) : ويقصد بـه تزويـد مـوظفى الشركة أو الجهة المالية غير المصرفية وشركائها بالتثقيف للتوعيـة بـالأمن السيبرانى ويتم تدريبهم على أداء واجبـاتهم ومـسؤولياتهم المتعلقـة بـالأمن السيبرانى بما يتفق مع السياسات والإجراءات والاتفاقيات ذات الصلة .
- أمن البيانات (Data Security) : ويقـصد بـه إدارة المعلومـات والـسجلات (البيانات) بما يتوافق مع استراتيجية المخـاطر لحمايـة سـرية المعلومـات وسلامتها وتوافرها .
- عمليـات وإجـراءات حمايـة المعلومـات (Information Protection Processes & Procedures) : ويقصد به الحفاظ على السياسات الأمنيـة (التـى تتنـاول الغـرض والنطاق والأدوار والمسؤوليات والتزام الإدارة والتنسيق بـين الكيانـات التنظيميـة) والعمليات والإجراءات وتستخدم لإدارة حماية أنظمة المعلومات والأصول .
- الصيانة (Maintenance) : ويقصد به إجراء عمليات الصيانة والإصـلاح لمكونـات أنظمة التحكم والمعلومات الصناعية بما يتفق مع السياسات والإجراءات .
- التكنولوجيا الوقائية (Protective Technology) : ويقصد به أن تـدار الحلـول الأمنية التكنولوجية لضمان أمن ومرونة الأنظمة والأصول ، بما يتوافـق مـع السياسات والإجراءات والاتفاقيات ذات الصلة .

٣- الرصد (Detect) : ويقصد به تطوير وتنفيذ الإجراءات المناسـبة لاكتـشاف وتحديد وقوع حدث الأمن السيبرانى .

- الأحداث غير المألوفة والنمطية (Anomalies & Events) : ويقصد به الكـشف عن الأنشطة غير المألوفة وفهم التأثير المحتمل للأحداث .
- المراقبة الأمنية المستمرة (Security Continuous Monitoring) : ويقـصد بـه مراقبة نظام المعلومات والأصول لتحديد أحداث الأمن السيبرانى والتحقق مـن فعالية تدابير الحماية .
- تحسين عمليـة الرصـد (Detection Process Improvement) : ويقـصد بـه تحديث عملية الرصد وإجراءاتها واختبارها بما يتناسب مع مـا يطـرأ مـن أحداث غير متوقعة .

٤- الاستجابة (Respond) : ويقصد به تطوير وتنفيذ الاجراءات المناسبة لاتخاذ التدابير المتعلقة بحدث الأمن السيبرانى المكتشف .

- تخطيط الاستجابة (Response Planning) : ويقصد به تنفيذ عمليات وإجراءات الاستجابة والحفاظ عليها لضمان الاستجابة لحوادث الأمن السيبرانى المكتشفة .
- التواصل بخصوص الاستجابة (Response Communications) : ويقصد به أن يتم تنسيق إجراءات الاستجابة مع أصحاب المصلحة الداخليين والخارجيين (مثل الدعم الخارجى من وكالات إنفاذ القانون) .
- التحليل (Response Analysis) : ويقصد به إجراء التحليل لضمان الاستجابة الفعالة ودعم إجراءات التعافى .
- تدابير التخفيف (Mitigation) : ويقصد به اتخاذ التدابير التى من شأنها منع تفاقم الحدث ، والتخفيف من آثاره ، وحل مسبباته .
- تحسين عملية الاستجابة (Respond Process Improvement) : ويقصد به أن يتم تحسين إجراءات الاستجابة من خلال دمج الدروس المستفادة من إجراءات الرصد أو الاستجابة الحالية والسابقة .

٥- الاستعادة (Recover) : ويقصد به تطوير وتنفيذ الإجراءات المناسبة للحفاظ على خطط المرونة واستعادة أى قدرات أو خدمات تعرضت للضرر بسبب حدث للأمن السيبرانى .

- تخطيط الاستعادة (Recovery Planning) : ويقصد به تنفيذ عمليات وإجراءات الاسترداد وصيانتها لضمان استعادة الأنظمة أو الأصول المتأثرة بحوادث الأمن السيبرانى .
- تحسين عملية الاستعادة (Recover Process Improvement) : ويقصد به تحسين تخطيط الاسترداد وعملياته من خلال دمج الدروس المستفادة فى الأنشطة المستقبلية .

- التواصل بخصوص الاستعادة (Recovery Communications) : ويقصد به تنسيق أنشطة الاستعادة مع أطراف داخلية وخارجية (مثل مراكز التنسيق بالاتحادات والهيئة ومقدمى خدمة الإنترنت ومسئولى الأنظمة مصدر الهجوم ومسئولى الأنظمة المتعرضة للهجوم وفرق مجابهة أحداث الأمن السيبرانى الأخرى مثل وزارة الاتصالات والموردين للأنظمة المصدرة والمتعرضة للهجوم) .

٢- العمليات التخطيطية :

العمليات التخطيطية لدورة الحياة للأمن السيبرانى (Cybersecurity Process) :

١- التحديد (Identify) :

إدارة الأصول (Asset Management) وتشتمل على :

- جرد الأجهزة والأنظمة المادية للشركة أو الجهة المالية غير المصرفية .
- جرد منصات البرامج والتطبيقات للشركة أو الجهة المالية غير المصرفية .
- تحديد آليات ومسارات التواصل وتدفق البيانات على المستوى التنظيمى .
- فهرسة أنظمة المعلومات الخارجية .
- تحديد أولويات الموارد (على سبيل المثال ، الأصول الملموسة ، والأجهزة ، والبيانات ، والوقت ، والموظفين ، والبرامج) بناءً على تصنيفها وأهميتها وقيمة الأعمال .
- إنشاء أدوار ومسؤوليات الأمن السيبرانى لجميع القوى العاملة وأصحاب المصلحة من الأطراف الثالثة (مثل الموردين والعملاء والشركاء) .

بيئة الأعمال (Business Environment) وتشتمل على :

- تحديد دور الشركة أو الجهة المالية غير المصرفية فى سلسلة التوريد والإفصاح عنه .
- تحديد مكان الشركة أو الجهة المالية غير المصرفية فى البنية التحتية الحيوية وقطاعها السوقى والإفصاح عنها .
- تحديد أولويات الرسالة والأهداف والأنشطة التنظيمية والإفصاح عنها .
- إنشاء التبعيات والوظائف الرئيسية لتقديم الخدمات الحيوية .
- وضع متطلبات المرونة لدعم تقديم الخدمات الحيوية لجميع حالات التشغيل (على سبيل المثال ، أثناء وقوع الخطر / الهجوم ، أثناء التعافى ، العمليات العادية) .

الحوكمة (Governance) وتشتمل على :

- وضع سياسة الأمن السيبرانى التنظيمى والإفصاح عنها .
- تنسيق أدوار ومسؤوليات الأمن السيبرانى ومواءمتها مع الأدوار الداخلية والشركاء الخارجيين .
- التحقق من أن المتطلبات القانونية والتنظيمية المتعلقة بالأمن السيبرانى ، بما فى ذلك التزامات الخصوصية والحريات المدنية ، مفهومة ومدارة .
- التحقق من أن عمليات الحوكمة وإدارة المخاطر قادرة على مجابهة مخاطر الأمن السيبرانى .

تقييم المخاطر (Risk Assessment) وتشتمل على :

- تحديد وتوثيق ثغرات الأصول .
- تلقى معلومات التهديد السيبرانى من منتديات ومصادر مشاركة المعلومات .
- تحديد وتوثيق التهديدات ، الداخلية منها والخارجية .
- تحديد التأثيرات والاحتمالات المتوقعة على الأعمال .
- استخدام التهديدات ونقاط الضعف والاحتمالات والتأثيرات لتحديد المخاطر .
- تحديد الاستجابات للمخاطر وترتيبها حسب الأولوية .

استراتيجية إدارة المخاطر (Risk Management Strategy) وتشتمل على :

- إنشاء عمليات إدارة المخاطر وإدارتها والموافقة عليها من قبل أصحاب المصلحة التنظيميين .
- تحديد درجة تحمل المخاطر التنظيمية والتعبير عنها بوضوح .
- الأخذ فى الاعتبار دور الشركة أو الجهة المالية غير المصرفية فى القطاع السوقى وفى البنية التحتية الحيوية الداعمة للقطاع السوقى ، عند تحديد درجة تحمل المخاطر .

إدارة مخاطر سلسلة التوريد (Supply Chain Risk Management) :

- تحديد عمليات إدارة مخاطر سلسلة التوريد السيبرانى وإنشاءها وتقييمها وإدارتها والموافقة عليها من قبل أصحاب المصلحة التنظيميين .

- تحديد الموردين والشركاء الخارجيين لأنظمة المعلومات والمكونات والخدمات وتحديد أولوياتها وتقييمها باستخدام عملية تقييم مخاطر سلسلة التوريد للتكنولوجيا .
- استخدم العقود المبرمة مع الموردين والشركاء الخارجيين لتنفيذ التدابير المناسبة المصممة لتلبية أهداف برنامج الأمن .
- السيبرانى للشركة أو الجهة المالية غير المصرفية وخطة إدارة مخاطر سلسلة التوريد السيبرانى .
- تقييم الموردين والشركاء الخارجيين بشكل روتينى باستخدام عمليات التدقيق أو نتائج الاختبارات أو غيرها من أشكال التقييم للتأكد من وفائهم بالتزاماتهم التعاقدية .
- إجراء تخطيط واختبار الاستجابة والاسترداد مع الموردين ومقدمي خدمات التعهيد .

٢- الحماية (Protect) :

إدارة الهوية والمصادقة والتحكم فى الوصول (Authentication & Access Control) وتشتمل على :

- إصدار الهويات وبيانات الاعتماد وإدارتها والتحقق منها وإبطالها وتدقيقها للأجهزة والمستخدمين والعمليات المصرح لهم .
- إدارة وحماية الوصول المادى إلى الأصول .
- إدارة الوصول عن بعد .
- إدارة أذونات وتصاريح الوصول ، بما فى ذلك مبادئ الحد الأدنى من الامتياز والفصل بين الواجبات .
- سلامة الشبكة محمية (على سبيل المثال ، الفصل بين الشبكات وتجزئة الشبكة) .
- إثبات الهوية الرقمية وربطها بعوامل التعريف والتأكيد عليها فى كل المعاملات طبقاً لضوابط الهيئة الصادرة فى هذا الشأن .
- المصادقة على المستخدمين والأجهزة والأصول الأخرى (على سبيل المثال ، عامل واحد ، أكثر من عامل) بما يتناسب مع مخاطر المعاملة (على سبيل المثال ، مخاطر أمن وخصوصية الأفراد والمخاطر التنظيمية الأخرى) وطبقًا لضوابط الهيئة الصادرة فى هذا الشأن .

الوعى والتدريب (Awareness & Training) وتشتمل على :

- إعلام جميع المستخدمين وتدريبهم .
- فهم المستخدمين المتميزين أدوارهم ومسؤولياتهم .
- فهم أصحاب المصلحة من الأطراف الثالثة (مثل الموردين والعملاء والشركاء) أدوارهم ومسؤولياتهم .
- فهم المديرين التنفيذيين أدوارهم ومسؤولياتهم .
- فهم موظفو الأمن المادى والأمن السيبرانى أدوارهم ومسؤولياتهم .

أمن البيانات (Data Security) وتشتمل على :

- حماية البيانات المخزنة .
- حماية البيانات المنقولة .
- تدار الأصول طبقًا للسياسات الحاكمة فى حالات الإهلاك والتحويل والتصرف .
- الحفاظ على القدرة الكافية لضمان التوافر .
- تنفيذ الحماية ضد تسرب البيانات .
- استخدام آليات قياس السلامة للتحقق من سلامة البرمجيات وأنظمة التشغيل والبرمجيات وسلامة المعلومات .
- بيئة التطوير والاختبار منفصلة عن بيئة الإنتاج .
- استخدام آليات قياس السلامة للتحقق من سلامة الأجهزة .

عمليات وإجراءات حماية المعلومات (Information Protection Processes & Procedures) وتشتمل علي :

- تطوير وصيانة الحدود الدنيا الأساسية لآليات التحكم ولضوابط تكنولوجيا المعلومات يتضمن مبادئ الأمن الأساسية (مثل مفهوم الحد الأدنى من الوظائف) .
- تنفيذ دورة حياة تطوير الأنظمة – SDLC .
- التأكد من الالتزام بعمليات التحكم فى تغيير بيانات التهيئة لعناصر المكونات .
- إجراء نسخ احتياطية للمعلومات وصيانتها واختبارها .

- استيفاء السياسة واللوائح المتعلقة ببيئة التشغيل المادية للأصول التنظيمية .
- إهلاك البيانات وفقًا للسياسة المعتمدة .
- تحسين عمليات الحماية .
- التحقق من فعالية تقنيات الحماية مشتركة .
- خطط الاستجابة (الاستجابة للحوادث واستمرارية الأعمال) وخطط التعافى (التعافى من الحوادث والتعافى من الكوارث) قيد الإدارة التنفيذية والتشغيلية .
- اختبار خطط الاستجابة والتعافى .
- تضمين الأمن السيبرانى فى ممارسات الموارد البشرية .
- تطوير وتنفيذ خطة إدارة نقاط الضعف .

الصيانة (Maintenance) وتشتمل على :

- تنفيذ عمليات الصيانة والإصلاح للأصول التنظيمية وتسجيلها باستخدام الأدوات المعتمدة والتى تم معايرتها .
- الموافقة على الصيانة عن بُعد للأصول التنظيمية وتسجيلها وتنفيذها بطريقة تمنع الوصول غير المصرح به .

التكنولوجيا الوقائية (Protective Technology) وتشتمل على :

- تحديد سجلات التدقيق أو التسجيل وتوثيقها وتنفيذها ومراجعتها وفقًا للسياسة المعتمدة وطبقًا لضوابط الهيئة الصادرة فى شأن السجلات الرقمية .
- حماية الوسائط القابلة للإزالة ويقيد استخدامها وفقًا للسياسة المعتمدة .
- استخدام مبدأ "الوظيفة الأقل لزوما" فى إعدادات التهيئة لعناصر مكونات الأنظمة لتوفير القدرات الأساسية فقط .
- التأكد من حماية شبكات الاتصالات والتحكم .
- تنفيذ آليات المرونة (على سبيل المثال ، "التشغيل الآمن فى حالة حدوث فشل" ، و"توزيع الأحمال" ، و"تبديل المكونات أثناء التشغيل الحي") لتحقيق متطلبات المرونة فى المواقف العادية والمعاكسة .

٣- الرصد (Detect) :

الأحداث غير المألوفة والنمطية (Anomalies & Events) وتشتمل على :

- تحديد السلوك النمطى لتشغيل الشبكات والتدفقات المتوقعة للبيانات المتداولة بين المستخدمين والأنظمة .
- تحليل الأحداث المكتشفة غير المألوفة بغرض فهم أهداف وأساليب الهجوم .
- جمع بيانات الأحداث وربطها من مصادر وأجهزة استشعار متعددة .
- تحديد تأثير الأحداث .
- وضع إعدادات ودراجات للتنبيه بالحوادث .

المراقبة الأمنية المستمرة (Continuous Monitoring) وتشتمل على :

- رصد الشبكة لاكتشاف أحداث الأمن السيبرانى المحتملة .
- رصد البيئة المادية لاكتشاف أحداث الأمن السيبرانى المحتملة .
- رصد نشاط الأفراد لاكتشاف أحداث الأمن السيبرانى المحتملة .
- الكشف عن البرمجيات الضارة .
- الكشف عن تحرك غير مصرح به للبرمجيات .
- رصد نشاط مقدم الخدمة الخارجى لاكتشاف أحداث الأمن السيبرانى المحتملة .
- تنفيذ مراقبة الأفراد وخطوط الربط والأجهزة والبرامج غير المصرح لهم .
- إجراء عمليات فحص الثغرات الأمنية .

تحسين عملية الرصد (Detection Process Improvement) وتشتمل على :

- أدوار ومسؤوليات الرصد محددة جيدًا لضمان المساءلة .
- تتوافق إجراءات الرصد مع جميع الضوابط المنتهجة .
- اختبار عمليات الرصد .
- إرسال معلومات الرصد عن الأحداث المكتشفة .
- تحسين عمليات الرصد باستمرار .

٤- الاستجابة (Respond) :

تخطيط الاستجابة (Response Planning) وتشتمل على :

- التحقق من تنفيذ خطة الاستجابة أثناء أو بعد وقوع حادث .

التواصل بخصوص الاستجابة (Response Communications) وتشتمل على :

- التحقق من أن يعرف الموظفون أدوارهم وترتيب العمليات عند الحاجة إلى الاستجابة .
- الإبلاغ عن الحوادث بما يتفق مع المعايير المعمول بها .
- تبادل المعلومات بما يتفق مع خطط الاستجابة .
- التنسيق مع أصحاب المصلحة بما يتفق مع خطط الاستجابة .
- المشاركة الطوعية للمعلومات مع أصحاب المصلحة الخارجيين لتحقيق وعى أوسع بحالة الأمن السيبرانى .

التحليل (Response Analysis) وتشتمل على :

- التحقيق فى الإخطارات من أنظمة الرصد .
- تحديد وفهم تأثير الحادث .
- تنفيذ التحاليل المحددة لتفاصيل ووقائع الحدث .
- تصنيف الحوادث وفقًا لخطط الاستجابة .
- تصميم وتخصيص عمليات للتلقى وللتحليل وللاستجابة لمواطن الضعف التى تم رصدها والكشف عنها من مصادر داخلية أو خارجية (مثل الاختبار الداخلي أو النشرات الأمنية أو الباحثين الأمنيين) .

تدابير التخفيف (Mitigation) وتشتمل على :

- احتواء الحوادث .
- التخفيف من حدة الحوادث .
- تصنيف وتوثيق نقاط الضعف المكتشفة حديثًا كمخاطر قابلة للتخفيف أو كمخاطر مقبولة .

تحسين عملية الاستجابة (Respond Process Improvement) وتشتمل على :

- خطط الاستجابة والدروس المستفادة .
- تحديث استراتيجيات الاستجابة .

٥- الاستعادة (Recover) :

تخطيط الاستعادة (Recovery Planning) وتشتمل على :

- تنفيذ خطة الاسترداد أثناء أو بعد حادث الأمن السيبرانى .

تحسين عملية الاستعادة (Recover Process Improvement) وتشتمل على :

- خطط التعافى والدروس المستفادة .
- تحديث استراتيجيات الاستعادة .

التواصل بخصوص الاستعادة (Recovery Communications) وتشتمل على :

- إدارة العلاقات العامة .
- إصلاح السمعة بعد وقوع حادث .
- الإبلاغ عن إجراءات الاستعادة لأصحاب المصلحة الداخليين والخارجيين بالإضافة إلى مجموعات العمل التنفيذية والإدارية .