FINANCIAL REGULATORY AUTHORITY
الهيئة العامة للرقابة المالية

عرض توضيحي لاطار تنظيم بعض قرارات قانون التكنولوجيا المالية غير المصرفية

Illustrative Presentation for Organizational Framework for some Decrees of Non-Banking Financial Services Technologies Law

Tarek.Ibrahim@fra.gov.eg

Building Bridges not Walls
نبنى الجسور لا الحواجز

قرارات مجلس إدارة الهيئة بشأن ...

قرار 139 لسنة 2023

- ضوابط التجهيزات والبنية التكنولوجية وأنظمة المعلومات ووسائل الحماية والتأمين والوظائف التكنولوجية الرئيسية ..
  - المذكورة في:
    - المواد 4، 5 من القانون رقم 5 لسنة 2022
    - المواد 6، 7 من قرار مجلس إدارة الهيئة 58 لسنة 2022

قرار 140 لسنة 2023

- الضوابط التكنولوجية للهوية الرقمية والعقود الرقمية والسجلات الرقمية ((أصول رقمية))
  - المذكورة في:
    - المادة 11 من القانون رقم 5 لسنة 2022
- ومجالات التكنولوجيا المالية وخدمات التعهيد المرتبطين ((عمليات إلكترونية))
  - المذكورة في:
    - المواد 6، 8 من القانون رقم 5 لسنة 2022
- وقواعد وضوابط ومتطلبات الامتثال
  - المذكورة في:
    - المادة 7 من القانون رقم 5 لسنة 2022

قرار 141 لسنة 2023

- ضوابط القيد والشطب في سجل الجهات الراغبة في تقديم خدمات التعهيد
  - المذكورة في:
    - المادة 6 من القانون رقم 5 لسنة 2022

قرار ###4 لسنة 2023

- شروط وضوابط وإجراءات الترخيص المؤقت
  - المذكورة في:
    - الفقرة الثانية من المادة 9 من القانون رقم 5 لسنة 2022

الجهات المخاطبة بالقرارات ...

1. الشركات الراغبة في الحصول على ترخيص لمزاولة الأنشطة المالية غير المصرفية من خلال تقنيات التكنولوجيا المالية تحت مظلة القانون 5 لسنة 2022
(NBFSTI: Non-Banking Financial Services Technology Institution)

2. الشركات والجهات الحاصلة على ترخيص من الهيئة بمزاولة أي من الأنشطة المالية غير المصرفية تحت مظلة قوانين أخرى والراغبة في الحصول على موافقة الهيئة مباشرتها لهذه الأنشطة باستخدام بعض مجالات التكنولوجيا المالية، من خلال مصادرها الداخلية أو من خلال إحدى جهات التعهيد تحت مظلة القانون 5 لسنة 2022
(NBFSI-NBFST-IS or NBFSI-NBFST-OS: Non-Banking Financial Services Institution with NBFS Technology In-Sourcing or with NBFS Technology Out-Sourcing)

3. الجهات الراغبة في تقديم خدمات التعهيد في مجالات التكنولوجيا المالية التي يمكن استخدامها في مزاولة الأنشطة المالية غير المصرفية تحت مظلة القانون 5 لسنة 2022
(NBFSTOI: Non-Banking Financial Services Technology Out-Sourcee Institution)

قرار 139
لسنة 2023

مصطلحات تعريفية ...

- تعريف **التجهيزات** هي: البنية التحتية من مرافق وتجهيزات لازمة لمراكز المعلومات (الأساسية والبديلة) والتي تشمل التجهيزات اللازمة للوصول للمرافق العامة من الكهرباء والاتصالات والمياه والصرف، والأنظمة الداخلية للكهرباء والتهوية والتبريد وكابلات الشبكات واكتشاف ومكافحة الحريق والأمن المادي والتحكم في الدخول والمراقبة من خلال الدوائر التليفزيونية المغلقة. (**Facilities Infrastructure**)
- تعريف **البنية التكنولوجية** هي: البنية التحتية من أجهزة ونظم لازمة لمراكز المعلومات (الأساسية والبديلة) والتي تشمل أجهزة الشبكات ونقل البيانات، وأجهزة الحاسبات ووسائل التخزين والأجهزة الطرفية المخصصة، وأنظمة البنية التحتية للتطبيقات، وأنظمة البنية التحتية لقواعد البيانات. (**Technology Infrastructure**)
- تعريف **أنظمة المعلومات** هي: الأنظمة المكونة من تطبيقات (Applications) وقواعد بيانات (Databases) يتم تطويرها لتؤدي مهام محددة دعما لعمليات ودورات العمل المستهدفة، وتساهم في التنسيق بين المستخدمين الداخليين أو الخارجيين، وقد تشمل تطبيقات "ذكاء اصطناعي" (Artificial Intelligence) لتوفير درجات أعلى من الأتمتة والدقة والسرعة في أداء المهام. (**Information System**)
- تعريف **وسائل الحماية والتأمين** هي: الآليات والمنهجيات المستخدمة لتوفير (1) القدرة على منع وقوع المخاطر التكنولوجية (Technology Risk Prevention) التي من شأنها فقد الخصوصية والسرية (Confidentiality)، أو السلامة والتكامل (Integrity)، أو التوافر والاتاحة (Availability)، للبنية التحتية للتجهيزات أو للبنية التحتية للبنية التكنولوجية أو لأنظمة المعلومات شاملة التطبيقات والبيانات، بالإضافة إلى توفير (2) القدرة على التحمل والمرونة للتعافي واستعادة الإمكانيات والوظائف والبيانات بعد وقوع المخاطر(After-Risk Recovery & Resiliency) (**Protection & Security Mechanisms**)

مصطلحات تعريفية ... بقية

قرار 139
لسنة 2023

- مصطلح **العمليات الاستراتيجية هي**: مجموعة 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 يكون 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 الاستراتيجي لإطار العمل المستهدف (Intended Framework). (**Strategy Processes**)
- مصطلح **العمليات التخطيطية هي**: مجموعة العمليات (Processes) المحققة لخطط مستهدفة تنفيذاً لاستراتيجية معينة، وتكون لكل عملية مجموعة من المدخلات (Inputs) ومجموعة من المخرجات (Outputs)، وعلى أن يكون 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 التنفيذي لإطار العمل المستهدف (Intended Framework). (**Planning Processes**)
- مصطلح **الإجراءات التطبيقية هي**: مجموعة الإجراءات (Procedures) المطبقة لعمليات تخطيطية معينة، ويكون لكل إجراء "حادث مشغل" (trigger events) كما يكون له "حالات ناتجة" (resulting state) والتي قد تكون "مشغِلة" لإجراء آخر (أو لإجراءات أخريات)، وعلى أن يتحقق من مجموعة الإجراءات التطبيقية "الأغراض والقيم المضافة" للعمليات التخطيطية المعينة. وتمثل الإجراءات التطبيقية "المستوى التشغيلي" لإطار العمل المستهدف (Intended Framework). (**Applied Procedures**)
- مصطلح **مجموعات العمل هي**: الموارد البشرية اللازمة لتنفيذ العمليات والإجراءات ويكون لكل منهم دور محدد (Role) ومسئولية محددة (Responsibility) ومساءلة محددة (Accountability)، تمكنهم من أداء عملهم والذي قد يتطلب أدوات وآليات وأنظمة (– Products Tools) تمكنهم من أداء عملهم بكفاءة. (People – Work Force)

قرار 139
لسنة 2023

مصطلحات تعريفية ... بقية

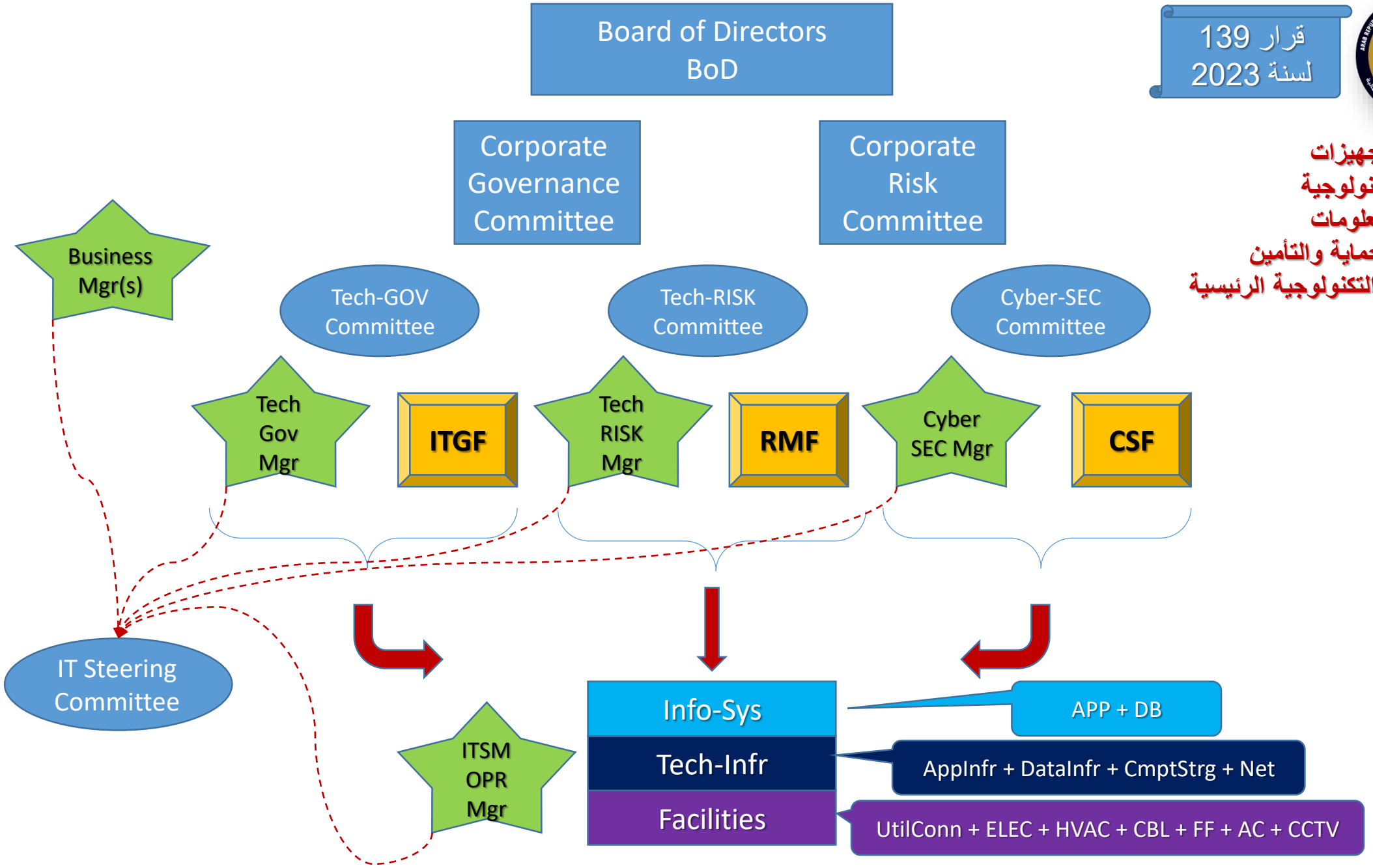
- مصطلح **إطار عمل حوكمة تكنولوجيا المعلومات** هو: إطار العمل المنظم لحوكمة تكنولوجيا المعلومات (ITG: Information Technology Governance) كعنصر أساسي ومتمم لحوكمة المؤسسات (CG: Corporate Governance)، وما يستتبعه من حوكمة لإدارة خدمات تكنولوجيا المعلومات (ITSM: Information Technology Service Management). ويتكون إطار العمل من العمليات الاستراتيجية على المستوى الاستراتيجي، والعمليات التخطيطية على المستوى التنفيذي، والإجراءات التطبيقية على المستوى التشغيلي. (**ITG-Framework**)

- مصطلح **إطار عمل إدارة مخاطر التكنولوجيا** هو: إطار العمل المنظم لإدارة مخاطر التكنولوجيا (TRM: Technology Risk Management) كعنصر أساسي ومتمم لإدارة مخاطر المؤسسات (ERM: Enterprise Risk Management). ويتكون إطار العمل من العمليات الاستراتيجية على المستوى الاستراتيجي، والعمليات التخطيطية على المستوى التنفيذي، والإجراءات التطبيقية على المستوى التشغيلي. (**TRM-Framework**)

- مصطلح **إطار عمل إدارة الأمن السيبراني** هو: إطار العمل المنظم لإدارة الأمن السيبراني (CSM: Cyber Security Management) كعنصر أساسي ومتمم لإدارة أمن المؤسسات (ESM: Enterprise Security Management). ويتكون إطار العمل من العمليات الاستراتيجية على المستوى الاستراتيجي، والعمليات التخطيطية على المستوى التنفيذي، والإجراءات التطبيقية على المستوى التشغيلي. (**CSM-Framework**)

قرار 139
لسنة 2023

ضوابط التجهيزات
والبنية التكنولوجية
وأنظمة المعلومات
ووسائل الحماية والتأمين
والوظائف التكنولوجية الرئيسية



	إطار عمل حوكمة تكنولوجيا المعلومات ITG-F: IT Governance) (Framework	إطار عمل إدارة مخاطر التكنولوجيا TRM-F: Technology Risk) (Management Framework	إطار عمل إدارة الأمن السيبراني CSM-F: Cyber Security) (Management Framework
النموذج المرجعي للاطار framework) (reference model	**النسخة الرابعة من "مكتبة البنية التحتية لتكنولوجيا المعلومات" من "آكسيلوس" (Axelos: ITILv4) و"إطار عمل إدارة الخادمات الممكنة بواسطة تكنولوجيا المعلومات" IT-enabled Services) .(Framework**	**النسخة الثانية من "نيست: إطار عمل إدارة المخاطر" NIST: RMF – Risk Management) (Framework 2.0 ومنهجية "دورة الحياة للأمن والخصوصية" من المعهد الوطني للمعايير والتكنولوجيا بالولايات المتحدة "نيست" NIST: National Institute for) (Standards & Technology**	**النسخة الثانية من "نيست: إطار عمل الأمن السيبراني" NIST: CSF – Cyber Security) (Framework 1.1 ومنهجية "دورة الحياة لتحسين الأمن السيبراني" من المعهد الوطني للمعايير والتكنولوجيا بالولايات المتحدة "نيست" NIST: National Institute for) (Standards & Technology**
العمليات الاستراتيجية (Strategy Process)	**17** (منهم 5 أساسيين لدورة الحياة و12 داعمين لدورة الحياة)	**11** (منهم 4 لدورة حياة مخاطر التكنولوجيا و7 لدورة حياة الأنظمة وآليات التحكم)	**23** (لدورة حياة الأمن السيبراني)
العمليات التخطيطية (Planning Process)	**102** (منهم 40 أساسيين لدورة الحياة، و62 داعمين لدورة الحياة)	**59** (منهم 12 لدورة حياة مخاطر التكنولوجيا و47 لدورة حياة الأنظمة وآليات التحكم)	**108** (لدورة حياة الأمن السيبراني)

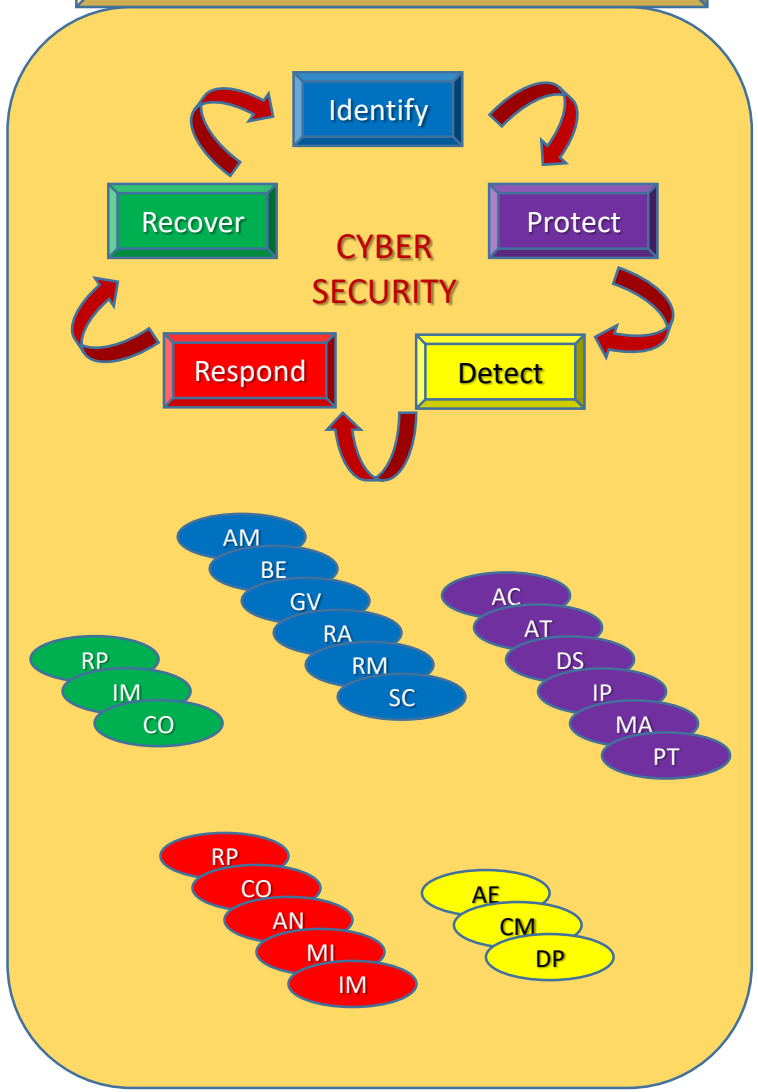
- ISO/IEC 38500-2015: **CG-IT** & ISO/IEC 20000: **ITSM**
- ISACA: **COBIT**

- ISO/IEC 27005-2022: InfoSec, CybrSec & PrvcyPtrctn - **InfoSec RISKS**

- ISO/IEC 27001: InfoSec MgtSys - **ISMS** & ISO/IEC 27002: InfoSec, CybrSec & PrvcyPtrctn - **InfoSec CNTRLS**

CYBER-SEC (CSM)

NIST – CSF 1.1

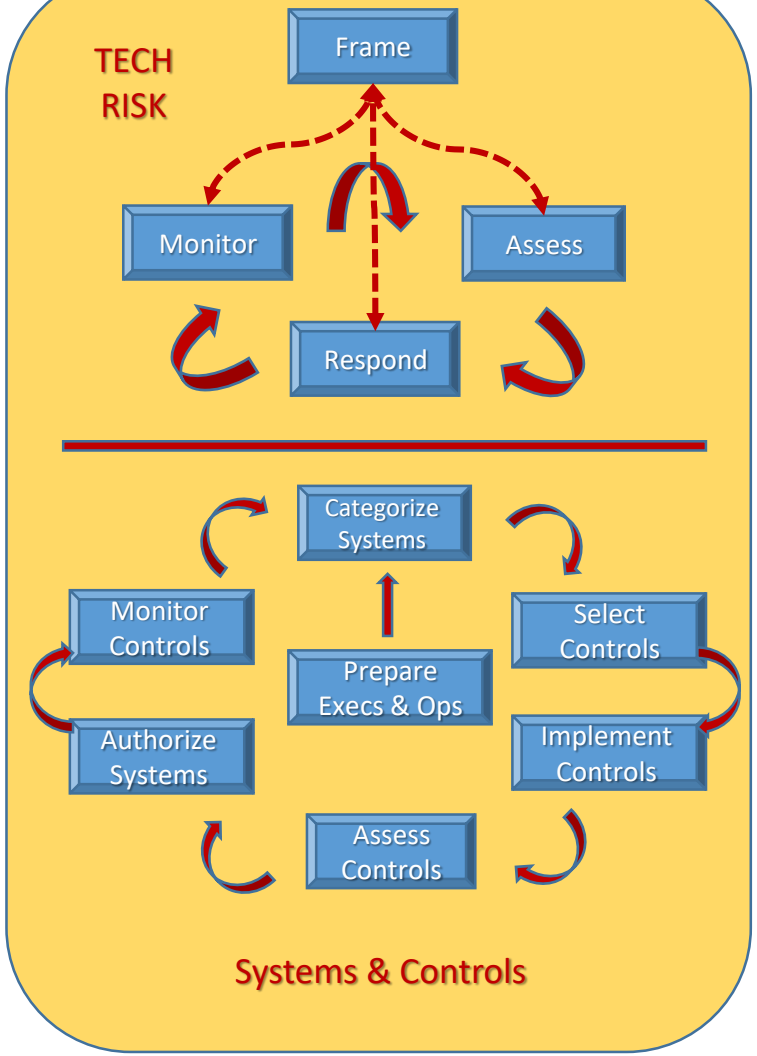


6 + 6 + 3 + 5 + 3 = 23 Strategy CSM Process

108 Planning CSM Process

TECH-RISK (TRM)

NIST – RMF 2.0

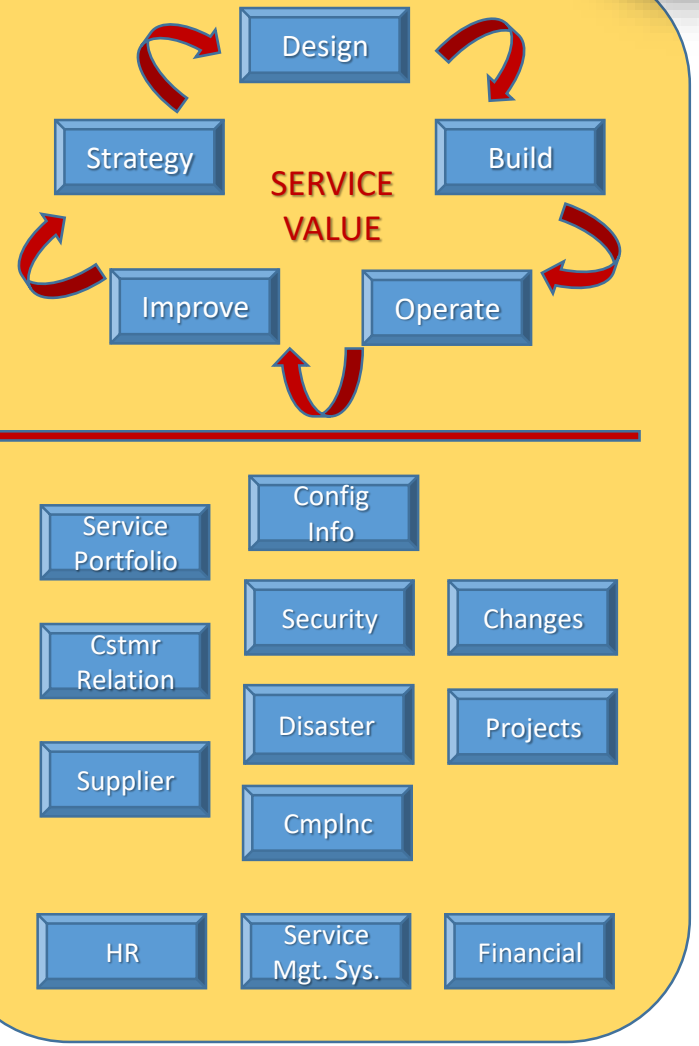


4 + 7 = 11 Strategy TRM Process

12 + 47 = 59 Planning TRM Process

IT-GOV (ITSM)

ITILv4 based on YASM



5 + 12 = 17 Strategy SVM Process

40 + 62 = 102 Planning SVM Process

مصطلحات تعريفية ...

قرار 140
لسنة 2023

- تعريف **الأصول الرقمية غير الملموسة في مزاولة الأنشطة المالية غير المصرفية** هي: أصل غير ملموس (Virtual Asset) تكون طبيعته رقمية (Digital)، ويمثل قيمة مضافة لمالكه وللمستفيد منه، ويتم إنشاءه وإدارة دورة حياته من خلال عمليات مخصصة لهذا الغرض، ويكون لهذه العمليات أنظمة داعمة تمكن المصدر والمالك والمستفيد من التعامل معه ومن خلاله في مزاولة الأنشطة المالية غير المصرفية، وتعتبر "الهوية الرقمية"، و"العقود الرقمية"، و"الحسابات الرقمية" و"السجلات الرقمية"، و"المعاملات الرقمية" في مزاولة الأنشطة المالية غير المصرفية أصول رقمية غير ملموسة. (**NBFS-DigAsset**: Non-Banking Financial Services – Digital Asset)

Digital Assets

- تعريف **عمليات إدارة دورة حياة الأصول الرقمية غير الملموسة في مزاولة الأنشطة المالية غير المصرفية** هي: عمليات دورة العمل (Work Flow Process) التي يتم من خلالها إدارة دورة حياة الأصل غير الملموس والمتضمن مراحل إنشاءه وتعديله وتحديثه وتجديده وإلغاءه ويكون ذلك في مزاولة الأنشطة المالية غير المصرفية، وتعتبر "عمليات التحديد والتحقق والمصادقة على الهوية إلكترونياً"، و"عمليات التعرف على العميل إلكترونيا"، وعمليات إبرام عقود منتجات مالية غير مصرفية إلكترونياً" في مزاولة الأنشطة المالية غير المصرفية من عمليات إدارة دورة حياة الأصول الرقمية غير الملموسة. (**NBFS-DALC-Process**: Non-Banking Financial Services – Digital Asset Life-Cycle Process)

DALC
eProcess

مصطلحات تعريفية (أصول رقمية) ...

قرار 140 لسنة 2023

- تعريف **المنصة الرقمية المستخدمة في مزاولة الأنشطة المالية غير المصرفية** هي: نموذج أعمال قائم على استخدام الوسائل التكنولوجية في مزاولة الأنشطة المالية غير المصرفية وفي عرض المنتجات والخدمات المرتبطة بها على الأشخاص الراغبين في الحصول عليها، ويسمح بتبادل البيانات والمعلومات اللازمة لإتمام هذه التعاملات والمرتبطة بالأنشطة المالية غير المصرفية. (**NBFS-DigPlatform**: Non-Banking Financial Services – Digital Platform)

DIG PLATFORM

- تعريف **السجل الرقمي المستخدم في مزاولة الأنشطة المالية غير المصرفية** هو: أي سجل رقمي يتضمن البيانات المتعلقة بالمعاملات التي يجريها الأشخاص الطبيعيون أو الاعتباريون، وعلى أن يتم تسجيل هذه المعاملات وتفاصيلها وتوقيتاتها رقمياً، وبما يسمح بالرجوع إلى هذه التفاصيل عند الحاجة بغرض الإثبات أو المراجعة، وبتتبع هذه البيانات من خلال شبكة آمنة مصممة للحفظ المركزي أو للحفظ الموزع، ومن خلال المنصات الرقمية والمرتبطة بالأنشطة المالية غير المصرفية. (**NBFS-DigRegistry**: Non-Banking Financial Services – Digital Registry)

DIG REGISTRY

مصطلحات تعريفية (أصول رقمية)... بقية

قرار 140 لسنة 2023

- تعريف **الهوية الرقمية المستخدمة في مزاولة الأنشطة المالية غير المصرفية هي**: أي بيانات معالجة تقنيًا تتعلق بشخص طبيعي أو اعتباري محدد أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخري كالاسم، أو الصوت، أو الصورة، أو رقم تعريفي، أو محدد للهوية عبر شبكة الاتصالات العالمية (الإنترنت)، على أن تسمح هذه البيانات بالتقييم والمصادقة على المعاملات التي تتم من خلال المنصات الرقمية والمرتبطة بالأنشطة المالية غير المصرفية. (**NBFS-DigID**: Non-Banking Financial Services – Digital Identity)

DIG ID

- تعريف **العقد الرقمي المستخدم في مزاولة الأنشطة المالية غير المصرفية** هو: أي عقد يتضمن حقوق والتزامات المتعاقدين بشكل رقمي، ويمكن تسجيله في سجل رقمي. كما يجوز أن يكون العقد الرقمي «عقدًا ذكيًا» من خلال برنامج يهدف إلى تنفيذ أحكام العقد والتحكم فيها أو توثيقها تلقائيًا، ويتم إبرامه من خلال المنصات الرقمية والمرتبطة بالأنشطة المالية غير المصرفية. (**NBFS-DigContract**: Non-Banking Financial Services – Digital Contract)

NBFS-DIGID NBFP-ACCOUNT

(NBFP) DIG CONTRACT

- تعريف **المعاملة الرقمية المستخدمة في مزاولة الأنشطة المالية غير المصرفية هي**: أي معاملة رقمية تتم بين متعامل له هوية رقمية محددة (NBFS-DigID) وبين مقدم خدمات ومنتجات مالية غير مصرفية، وعلى أن يتم تسجيل هذه المعاملات وتفاصيلها وتوقيتاتها في سجل رقمي (NBFS-DigRegistry)، ويكون لهذه المعاملات أسباب محددة مثل العرض والطلب والاخطار، وتحقق لأطرافها أغراض محددة، وتشمل على سبيل المثال "إنشاء/تعديل/تحديث/تجديد/إلغاء هوية رقمية"، "إنشاء/تعديل/تحديث/تجديد/إلغاء حساب للمتعامل"، "إنشاء/تعديل/تحديث/تجديد/إلغاء حساب لمنتج مالي غير مصرفي مرتبط بحساب المتعامل"، "إنشاء/تعديل/تحديث/تجديد/إلغاء طلبات مرتبطة بطبيعة المنتج المالي غير المصرفي مثل الشراء والبيع وسداد قسط وطلب تعويض"، وتتم هذه المعاملات الالكترونية من خلال المنصات الرقمية والمرتبطة بالأنشطة المالية غير المصرفية. (**NBFS-DigTransaction**: Non-Banking Financial Services – Digital Transaction)

NBFS-DIGID NBFP-TRNSC-ACCOUNT

(NBFP-TRNSC) DIG Statement

DALC eProcess

مصطلحات تعريفية (عمليات إدارة دورة الحياة)

قرار 140 لسنة 2023

- تعريف **عمليات التسجيل والحفظ في والاسترجاع من السجلات الرقمية إلكترونياً في مزاولة الأنشطة المالية غير المصرفية هي**: عمليات التسجيل والحفظ والاسترجاع للمحررات الرقمية وللمعاملات الرقمية والمتضمنة الهوية الرقمية والعقود الرقمية وأي معاملات رقمية في سجلات رقمية، بغرض إنشاء سجلات للمعاملات المالية غير المصرفية تمكن من تتبع تفاصيل البيانات وتوقيتات الأحداث المرتبطة بها بطريقة آمنة ومؤمنة، وتكون "أساسية" لعمليات التحديد والتحقق والمصادقة على الهوية إلكترونياً ولعمليات التعرف على العميل إلكترونياً ولعمليات التعاقد مع العميل إلكترونياً ولأي عمليات لتنفيذ المعاملات الرقمية إلكترونيا في مزاولة الأنشطة المالية غير المصرفية. (**NBFS-eRegistry**: Non-Banking Financial Product – electronic Registry)

NBFS-eRegistry

- تعريف **عمليات التحديد والتحقق والمصادقة على الهوية إلكترونياً في مزاولة الأنشطة المالية غير المصرفية هي**: عمليات التحديد والتحقق والمصادقة على الهوية المادية بغرض إنشاء هوية رقمية (NBFS-DigID)، وعمليات التحديد والتحقق والمصادقة على الهوية المادية والرقمية بغرض المصادقة على المعاملات (NBFS-DigTransactions) التي تتم من خلال المنصات الرقمية والمرتبطة بالأنشطة المالية غير المصرفية. (**NBFS-eIDiva**: Non-Banking Financial Services – electronic ID identification verification & authentication)

NBFS-eIDiva

- تعريف **عمليات التعرف على العميل إلكترونياً في مزاولة الأنشطة المالية غير المصرفية هي**: عمليات التعرف على المعلومات الأساسية ومتطلبات واحتياجات العميل لتحليل وتحديد مدى ملائمة المنتجات والخدمات المالية غير المصرفية المطروحة، ويكون ذلك بغرض إنشاء حساب عميل يمكنه من استعراض وطلب خدمات ومنتجات مالية غير مصرفية، من خلال المنصات الرقمية والمرتبطة بالأنشطة المالية غير المصرفية. (**NBFS-eKYC**: Non-Banking Financial Services – electronic Know-Your-Customer)

NBFS-eKYC

DALC eProcess

مصطلحات تعريفية (عمليات إدارة دورة الحياة) ... بقية

قرار 140 لسنة 2023

- تعريف **عمليات التعاقد مع العميل إلكترونياً في مزاولة الأنشطة المالية غير المصرفية هي**: عمليات التعاقد مع العميل على منتج مالي غير مصرفي بغرض إنشاء حساب للمنتج المالي غير المصرفي مرتبط بحساب العميل وتتضمن تسجيل بيانات العقد الرقمي في سجلات رقمية للحفظ ويكون ذلك بطريقة مؤمنة تضمن الحجية القانونية للإثبات، من خلال المنصات الرقمية والمرتبطة بالأنشطة المالية غير المصرفية. (**NBFS-eContract**: Non-Banking Financial Product – electronic Contract)

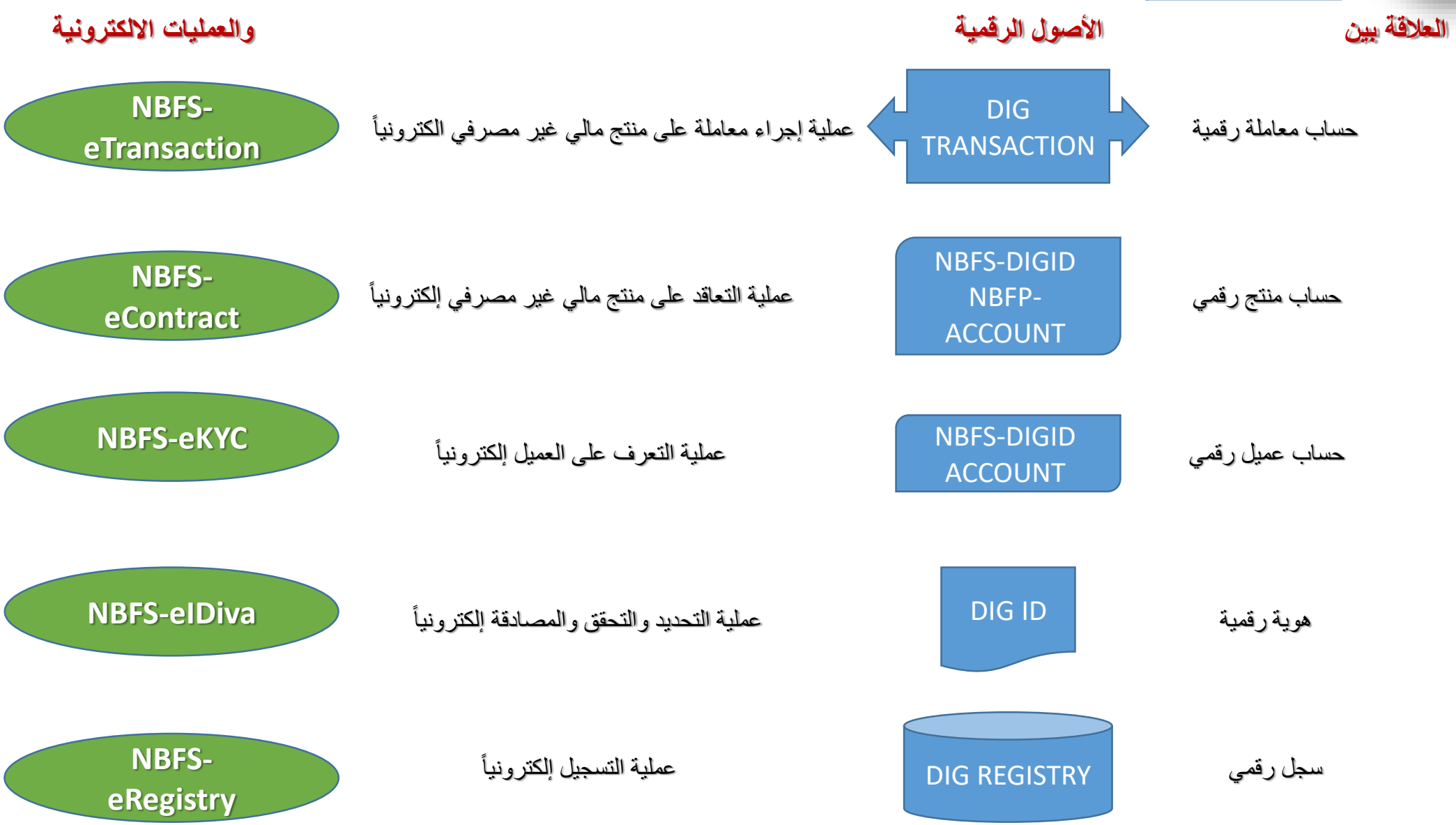
NBFS-eContract

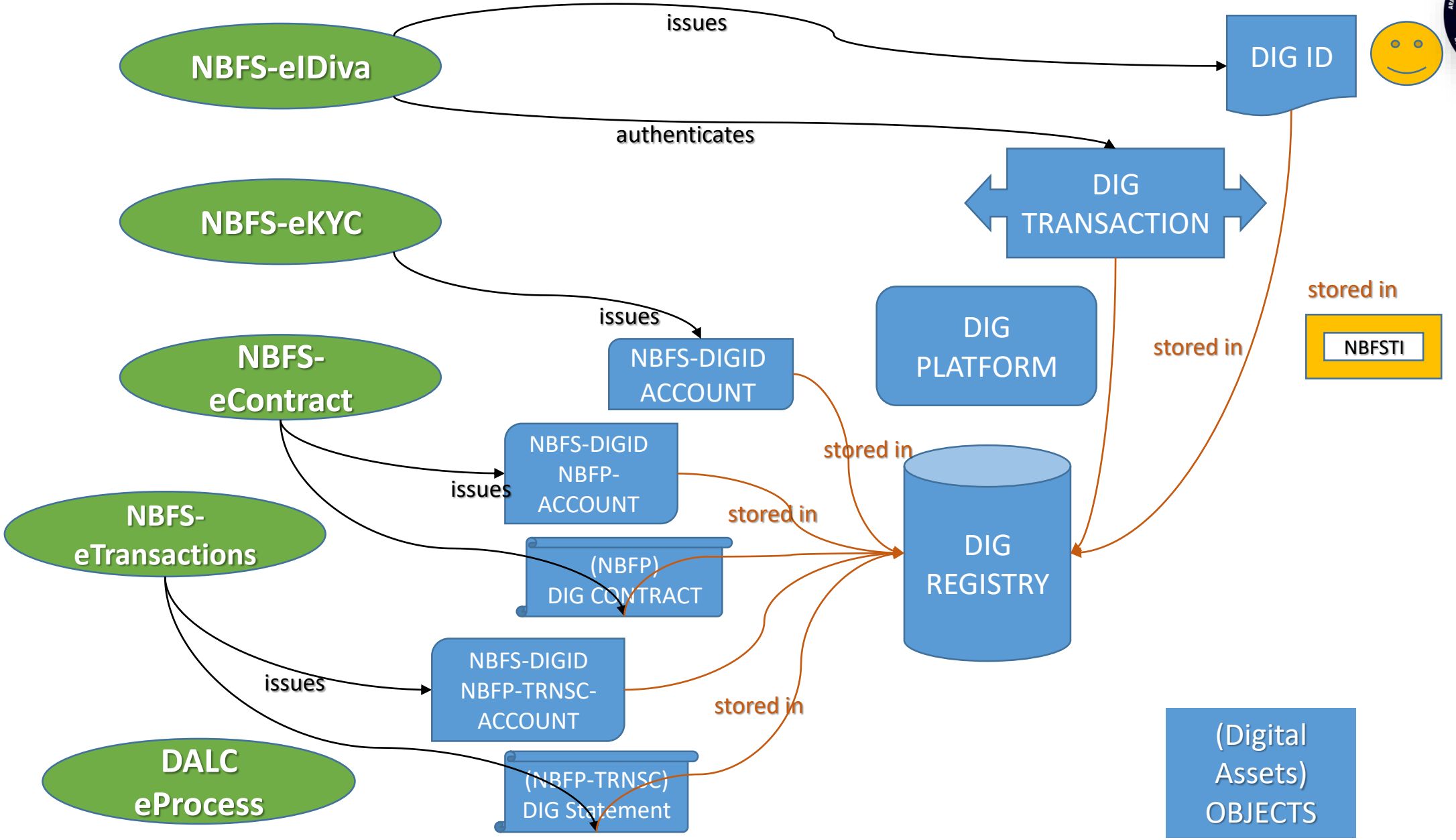
- تعريف **عمليات إجراء المعاملات إلكترونياً في مزاولة الأنشطة المالية غير المصرفية هي**: عمليات إدارة المعاملات المرتبطة بمنتج مالي غير مصرفي بغرض إنشاء حساب للمعاملات المرتبطة بالمنتج المالي غير المصرفي والذي يكون مرتبط بحساب العميل وقد تكون هذه المعاملات في مرحلة «قبل البيع» أو مرحلة «بعد البيع» (Pre-Sales or Post-Sales Transactions) وتتضمن تسجيل بيانات المعاملات الرقمية في سجلات رقمية للحفظ ويكون ذلك بطريقة مؤمنة تضمن الحجية القانونية للإثبات، من خلال المنصات الرقمية والمرتبطة بالأنشطة المالية غير المصرفية. (**NBFS-eTransaction**: Non-Banking Financial Services– electronic Transaction)

NBFS-eTransaction

الضوابط التكنولوجية للهوية الرقمية والعقود الرقمية والسجلات الرقمية ((أصول رقمية))
ومجالات التكنولوجيا المالية وخدمات التعهيد المرتبطين ((عمليات إلكترونية))

قرار 140 لسنة 2023




NBFS-eIDiva
issues
DIG ID
authenticates
DIG TRANSACTION
NBFS-eKYC
issues
NBFS-DIGID ACCOUNT
DIG PLATFORM
stored in
NBFSTI
stored in
NBFS-eContract
NBFS-DIGID NBFP-ACCOUNT
issues
stored in
DIG REGISTRY
NBFS-eTransactions
stored in
(NBFP) DIG CONTRACT
issues
NBFS-DIGID NBFP-TRNSC-ACCOUNT
stored in
DALC eProcess
(NBFP-TRNSC) DIG Statement
(Digital Assets) OBJECTS

سجل اضطلاع على حدث سجل إضافة حدث

Log Entry (LE)
Encrypted LE (ELE)
Log Chain (LC)
Accumulator Entry (AE)
Proof of Past Log (PPL)

Insertion ProofLog. DigRegistry

Retreival ProofLog. DigRegistry

عمليات السجل الإلكتروني «أساسية» و «داعمة» :

سجل أحداث أرشيف ملفات

NBFS-eRegistry

NBFS-eIDiva

DIG ID

هوية رقمية

EventLog. DigRegistry

eDocArchive. DigRegistry

لعمليات التحديد والتحقق والمصادقة الكترونيا

NBFS-eKYC

NBFS-DIGID ACCOUNT

حساب عميل رقمي

EventLog. DigRegistry

eDocArchive. DigRegistry

ولعمليات التعرف على العميل الكترونيا

NBFS-eContract

NBFS-DIGID NBFP-ACCOUNT

حساب منتج رقمي

EventLog. DigRegistry

eDocArchive. DigRegistry

ولعمليات التعاقد على منتجات مالية غير مصرفية الكترونياً

NBFS-eTransaction

DIG TRANSACTION

قيد معاملة رقمي

EventLog. DigRegistry

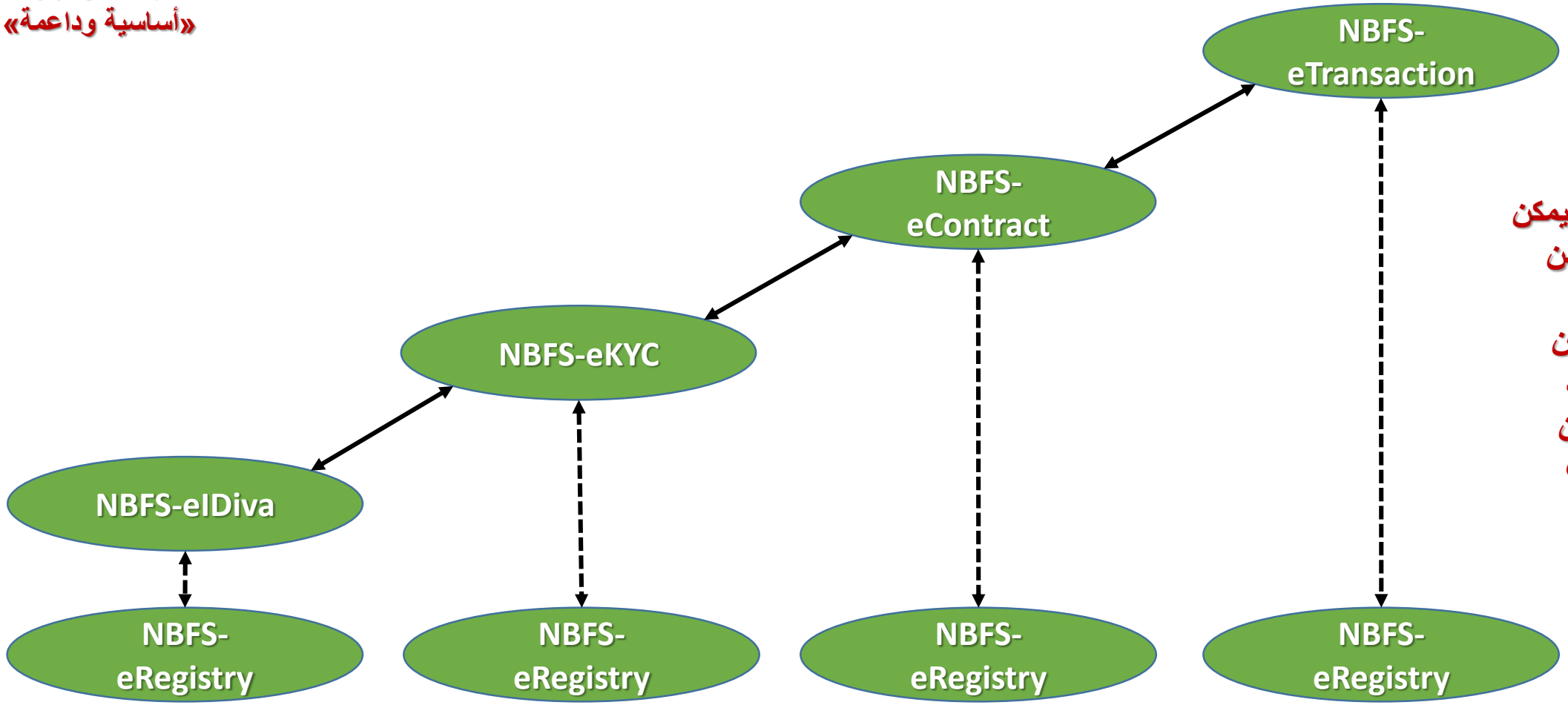
eDocArchive. DigRegistry

ولعمليات المعاملات الرقمية المرتبطة بمنتجات مالية غير مصرفية

NBFinTech Domains

تعريف **مجالات التكنولوجيا المالية غير المصرفية** هي: المجالات التكنولوجية المستخدمة في تنفيذ عمليات البنية الهيكلية لأعمال الجهات الخاضعة لرقابة الهيئة، والتي تحددها الهيئة، وتكون هذه العمليات "عامة وظيفياً" وداعمة لأكثر من نشاط مالي غير مصرفي، أو "مخصصة وظيفياً" لطبيعة منتجات أو خدمات مالية غير مصرفية محددة. (**NBFinTech-Domain**: Non-Banking Financial Technology Domain)

مجالات وظيفية
«أساسية وداعمة»



مجالات التكنولوجيا المالية التي يمكن استخدامها من خلال أنظمة وتطبيقات عن طريق موارد داخلية أو من خلال خدمات التعهيد

Illustration based on Micro-Services Architectural Concepts

مجالات وظيفية
«أساسية وداعمة»

مجالات التكنولوجيا المالية التي يمكن استخدامها من خلال أنظمة وتطبيقات عن طريق موارد داخلية أو من خلال خدمات التعهيد

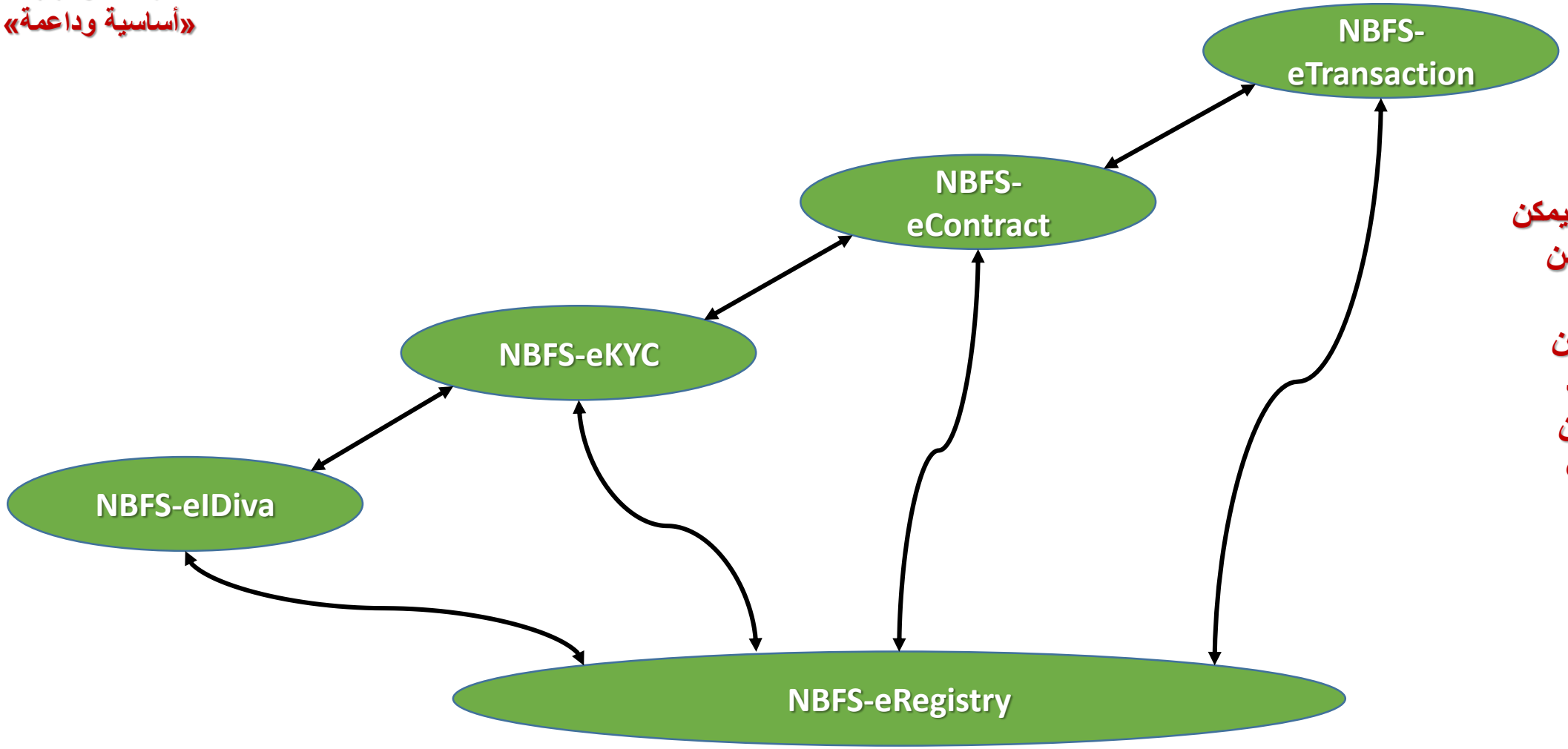


Illustration based on Micro-Services Architectural Concepts

مجالات وظيفية
«أساسية وداعمة»

مجالات التكنولوجيا المالية التي يمكن استخدامها من خلال أنظمة وتطبيقات عن طريق موارد داخلية أو من خلال خدمات التعهيد

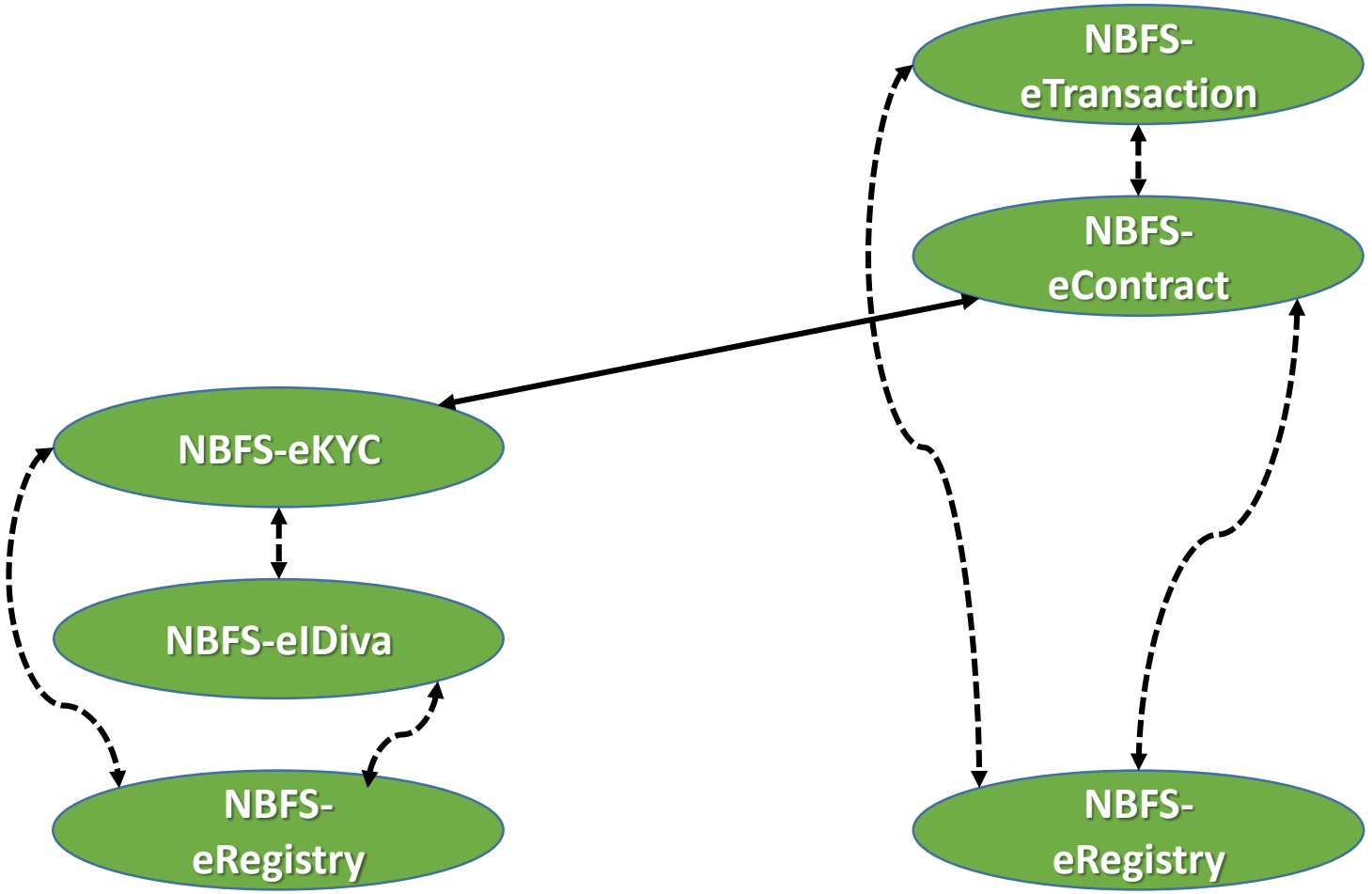


Illustration based on Micro-Services Architectural Concepts

NBFS-eIDiva

DIG ID

الهوية الرقمية ... وعمليات التحديد والتحقق والمصادقة

- تتضمن عملية "التحقق من الهوية التي تتم من خلال منصات رقمية" ثلاث عمليات فرعية وهي:
  1. عملية التحديد
  2. وعملية التحقق
  3. وعملية المصادقة.
- يجب أن تعتمد العمليات على أكثر من مجموعة نوعية من عوامل التحديد والتحقق والمصادقة، وتشمل كل مجموعة على أكثر من عنصر:
  1. مجموعة عامل المعرفة (something you KNOW)
     وتشمل عدة عناصر ومنها على سبيل المثال: اسم المستخدم، كلمة مرور، إجابات على أسئلة شخصية
  2. مجموعة عامل الحيازة (something you HAVE)
     وتشمل عدة عناصر ومنها على سبيل المثال: مستند اثبات الشخصية، صندوق بريد الإلكتروني، رقم التليفون المحمول، رقم الجهاز المستخدم و/أو رقم الشريحة المرتبطين برقم التليفون المحمول، حساب دفع غير نقدي، توقيع الكتروني معتمد
  3. مجموعة عامل الكيان أو الوجود والحيوية (something you ARE)
     وتشمل عدة عناصر ومنها على سبيل المثال: الخصائص البيومترية لبصمة الوجه ولبصمة الصوت ولبصمة الأصابع ولهندسة الكف ولبصمة العين، وحيوية رد الفعل، محددات الموقع الجغرافي، بالإضافة إلى محددات الموقع السيبراني، ومحددات وقت المعاملة

تكون العمليات المعتمدة على أكثر من عنصر لأكثر من مجموعة من المجموعات النوعية الثلاث، أكثر أمناً وصعوبة في الاختراق.

NBFS-eIDiva

DIG ID

الهوية الرقمية ... وعمليات التحديد والتحقق والمصادقة

2+3+3+4 = 12 عنصر بحد أدني

- يراعى في عمليات التحديد والتحقق والمصادقة للمرة الأولى بغرض إنشاء هوية رقمية للخدمات المالية غير المصرفية، (أو عند التجديد أو تحديث البيانات):
  - استخدام أربعة عناصر على الأقل من مجموعة عامل الحيازة مستند اثبات الشخصية، صندوق بريد الإلكتروني، رقم التليفون المحمول، رقم الجهاز المستخدم) بالإضافة إلى ثلاث عناصر على الأقل من مجموعة عامل الكيان (الوجود والحيوية) (الخصائص البيومترية لبصمة الوجه، وحيوية رد الفعل، ومحددات الموقع الجغرافي)،
  - كما يتم تحديد الموقع السيبراني ووقت المعاملة بغرض التسجيل والمراجعة،
  - ويتم إنشاء (تحديث) ثلاث عناصر من مجموعة عامل المعرفة (اسم المستخدم، كلمة المرور، إجابات على الأسئلة الشخصية).
  - ويجب (في حال تواجدها) الربط مع "منظومة الهوية الرقمية الموحدة للخدمات المالية غير المصرفية بالهيئة" من خلال "واجهة تطبيقات قابلة للبرمجة" (FRA-NBFS-DigID-API) لإصدار أو الحصول على (أو تجديد صلاحية) رقم مرجعي فريد للأشخاص الطبيعية (FRA.IFP code) لكل متعامل في الأسواق المالية غير المصرفية

2+1+1+2 = 6 عنصر بحد أدنى

- يراعى في عمليات التحديد والتحقق والمصادقة للعمليات اللاحقة:
  - استخدام عنصران من عناصر عامل المعرفة (اسم المستخدم، كلمة المرور)، بالإضافة إلى عنصر على الأقل من عناصر عامل الحيازة (رقم الجهاز المستخدم، و/او رقم التليفون المحمول، و/أو صندوق البريد الإلكتروني)، بالإضافة إلى عنصر على الأقل من عناصر عامل الكيان (الوجود والحيوية) (الخصائص البيومترية وحيوية رد الفعل لبصمة الوجه، و/أو محددات الموقع الجغرافي)،
  - كما يتم تحديد الموقع السيبراني ووقت المعاملة بغرض التسجيل والمراجعة.
  - ويراعى متابعة ومراجعة التغيرات على أياَ من العناصر من خلال سجلات التسجيل والمراجعة، واتخاذ الإجراءات المناسبة في حال تغير العناصر، والتي تتضمن الربط مع "منظومة الهوية الرقمية الموحدة للخدمات المالية غير المصرفية بالهيئة" من خلال "واجهة تطبيقات قابلة للبرمجة" (FRA-NBFS-DigID-API) لتحديث بيانات الرقم المرجعي الفريد للأشخاص الطبيعية (FRA.IFP code) لكل متعامل في الأسواق المالية غير المصرفية.

NBFS-eIDiva

DIG ID

الهوية الرقمية ... وعمليات التحديد والتحقق والمصادقة

- يراعى في عمليات التحديد والتحقق والمصادقة للخدمات المالية غير المصرفية الترتيب والضوابط التالية:

1. في مرحلة تحديد الخصائص البيومترية يجب الاعتماد على خصائص الوجه لانتشار الأجهزة المحمولة المدعومة بالكاميرات اللازمة لالتقاط الصور أو مقاطع فيديو مرئية ومسموعة، ويجب أن يتم التأكد من أن الصورة والفيديو يتم التقاطهم مباشرة، كما يجب أن يتم مقارنة الخصائص الملتقطة بالمرات السابقة
2. ولتحديد الحيوية يجب التأكد أن حيوية ورد فعل العميل تلقائية وليست ميكانيكية وأنه ليس منتحلًا للشخصية (مثل استخدام الصور ومقاطع الفيديو وأقنعة الوجه) من خلال الاستجابة لطلبات عشوائية
3. في مرحلة تحديد مستند الهوية يجب التأكد من أن يتم التقاط صورة حية للمستند، (وجه وظهر في حالة بطاقة الرقم القومي)، كما يجب أن يتم تحويل البيانات من الملتقطة إلى بيانات رقمية من خلال تقنية التعرف على الحروف والأرقام. كما يجب أن يتم التقاط الصورة الشخصية لمقارنتها بالصورة الملتقطة في مرحلة تحديد الخصائص البيومترية، كما يجب أن يتم التحقق من أن البطاقة غير مزيفة من خلال مراجعة خصائص البطاقة أو من خلال الربط مع الأحوال المدنية أو من خلال "واجهة التطبيقات القابلة للبرمجة لمنظومة الهوية الرقمية الموحدة للخدمات المالية غير المصرفية بالهيئة" (FRA-NBFS-DigID-API). ويكون الرقم القومي أساسي للمصريين، ويمكن إضافة مستندات هوية أخرى (جواز سفر، رخصة قيادة، بطاقة إقامة لغير المصريين)
4. في مرحلة تحديد البريد الالكتروني يجب التحقق من الحيازة عن طريق إرسال رسالة والتأكد من الرد في إطار زمني محدد لينا سب الغرض من إثبات الحيازة (email Check). ويكون البريد الإلكتروني الأساسي هو الحد الأدنى، ويمكن إضافة بريد إلكتروني آخر ثانوي.
5. في مرحلة تحديد رقم التليفون المحمول يجب التحقق من الحيازة عن طريق إرسال رسالة نصية قصيرة والتأكد من الرد في إطار زمني محدد (Mobile # Check)، كما يجب التحقق من أن رقم التليفون المحمول المصدر من أحد مقدمي خدمات الاتصالات المصرح لهم بتقديم خدمات الاتصالات من الجهاز القومي لتنظيم الاتصالات، مرتبط بنفس الرقم القومي الذي تم تحديده في مرحلة تحديد مستند الهوية من خلال الربط مع الجهاز القومي لتنظيم الاتصالات أو من خلال "واجهة التطبيقات القابلة للبرمجة لمنظومة الهوية الرقمية الموحدة للخدمات المالية غير المصرفية بالهيئة" (FRA-NBFS-DigID-API) ويكون رقم التليفون المحمول الأساسي هو الحد الأدنى، ويمكن إضافة رقم تليفون محمول آخر ثانوي.
6. في مرحلة تحديد رقم الجهاز المستخدم و/أو رقم الشريحة من خلال الحصول على الهوية الدولية للجهاز المحمول (International Mobile Equipment Identity - IMEI) أو ما يكافئها، كما يجب التحقق من صحة الرقم (IEMI Check). ويكون الجهاز الأساسي هو الحد الأدنى، ويمكن إضافة أجهزة ثانوية أخرى.
7. في مرحلة تحديد الموقع الجغرافي من خلال الجهاز المحمول (Location services). يجب التحقق من القرب الجغرافي بالمقارنة مع العنوان البريدي الذي تم تحديده في مرحلة تحديد الهوية، أو العنوان البريدي المختار للمراسلة (Address Check).
8. في مرحلة تحديد الموقع السيبراني من خلال الجهاز المحمول يجب التحقق من القرب السيبراني بالمقارنة مع العنوان البريدي الذي تم تحديده في مرحلة تحديد الهوية، أو العنوان البريدي المختار للمراسلة (IP Address Check)
9. في مرحلة تحديد وقت المعاملة من الجهاز المحمول يجب التحقق من القرب الزمني بالمقارنة مع مصدر مستقل لتحديد الوقت الزمني (Time Check).
10. في حال / مرحلة تحديد حساب دفع غير نقدي من أحد البنوك أو مقدمي أو ميسري الدفع الالكتروني، والخاضعين لرقابة البنك المركزي، يجب التأكد من حيازة حساب الدفع الالكتروني عن طريق تحويل صغير والتأكد من إتمامه بنجاح، كما يجب التأكد من استخدام نفس رقم التليفون المحمول الذي تم تحديده في مرحلة تحديد رقم تليفون المحمول، مما يساهم في استيفاء متطلبات الوحدة المركزية لمكافحة غسل الأموال وتمويل الإرهاب.
11. في حال / مرحلة تحديد التوقيع الإلكتروني المعتمد يجب التحقق من الحيازة عن طريق طلب استخدام التوقيع الالكتروني والمتضمن الحصول على المفتاح الشفري العام والبصمة الإلكترونية الزمنية وشهادة التصديق الإلكتروني لتحديد بيانات إنشاء التوقيع الإلكتروني، كما يجب التحقق من أن التوقيع الالكتروني المصدر من أحد مقدمي خدمات التصديق على التوقيع الإلكتروني المصرح لهم من هيئة تنمية صناعة تكنولوجيا المعلومات، مرتبط بنفس الرقم القومي الذي تم تحديده في مرحلة تحديد مستند الهوية، مما يساهم في رفع درجة الثقة للمعاملات المرتبطة.

NBFS-eIDiva

DIG ID

الهوية الرقمية ... وعمليات التحديد والتحقق والمصادقة

- تعتمد الهيئة ثلاث درجات من الثقة للهوية الرقمية الموحدة للخدمات المالية غير المصرفية (NBFS-DigID Levels-of-Trust) ، وهي:

1. درجة الثقة الأساسية (Basic-Level-of-Trust) والمتضمنة بحد أدنى عنصران من مجموعة عوامل المعرفة، بالإضافة إلى ثلاث عناصر من مجموعة عوامل الكيان والحيوية بالإضافة إلى أربع عناصر من مجموعة عوامل الحيازة
2. درجة الثقة العامة (General-Level-of-Trust) والمتضمنة بحد أدنى العوامل والعناصر في درجة الثقة الأساسية بالإضافة إلى (حيازة حساب الدفع الالكتروني)
3. درجة الثقة العالية (High-Level-of-Trust) والمتضمنة بحد أدنى العوامل والعناصر في درجة الثقة العامة بالإضافة إلى (حيازة توقيع إلكتروني معتمد)

على أن يتم استخدام درجة الثقة المناسبة لدرجة الخطر المرتبطة بطبيعة المعاملة، وتكون درجة الثقة الأساسية هي الحد الأدنى لإنشاء الهوية الرقمية الموحدة للخدمات المالية غير المصرفية، ولتنفيذ عمليات التعرف على العميل عن بعد (NBFS-eKYC) بغرض إنشاء حساب عميل، وتكون درجة الثقة العامة هي الحد الأدنى لتنفيذ عمليات التعاقد على منتج مالي غير مصرفي عن بعد (NBFSP-eContract) وتنفيذ المعاملات المرتبطة ذات درجة المخاطر المحدودة عن بعد (Limited-Risk-NBFSP-eTransactions)، وتكون درجة الثقة العالية هي اللازمة لتنفيذ المعاملات المرتبطة ذات درجة المخاطر العالية عن بعد (High-Risk-NBFSP-eTransactions)، وبخلاف ما تقدم يترك أمر تحديد نوع المعاملة من حيث الخطورة لمقدمي الخدمات.

NBFS-eKYC

NBFS-DIGID ACCOUNT

الحساب الرقمي المرتبط بالهوية الرقمية ... وعمليات التعرف على العميل

- إقرار "عمليات التعرف على العميل إلكترونياً في مزاولة الأنشطة المالية غير المصرفية" (NBFS-eKYC) كأحد مجالات التكنولوجيا المالية التي يمكن استخدامها لمزاولة الأنشطة المالية غير المصرفية، واعتماد الأنظمة المرتبطة بها من التطبيقات الإلكترونية "الداعمة" لمجالات التكنولوجيا المالية التي يمكن استخدامها في مزاولة الأنشطة المالية غير المصرفية من خلال خدمات التعهيد، أو بدونها.
- إقرار خدمات "عمليات التعرف على العميل إلكترونياً في مزاولة الأنشطة المالية غير المصرفية" (NBFS-eKYC) كأحد خدمات التعهيد في مجالات التكنولوجيا المالية التي يمكن استخدامها لمزاولة الأنشطة المالية غير المصرفية من خلال الجهات الراغبة في تقديم هذه الخدمات.
- كما يمكن أن يتم التخصص لكل من الأسواق المالية غير المصرفية:
  1. " التعرف على العميل – لأنشطة الاستثمار"
  2. " التعرف على العميل – لأنشطة الاقتراض"
  3. " التعرف على العميل – لأنشطة التأمين"

NBFS-
eContract

(NBFP)
DIG CONTRACT

العقود الرقمية ... وعمليات ابرام التعاقدات على منتج مالي غير مصرفي إلكترونياً

- تتضمن عملية "إبرام العقود الرقمية التي تتم من خلال منصات رقمية" خمسة عمليات فرعية على الأقل وهي:
  1. عملية التحقق من هوية أطراف التعاقد
  2. عملية التحقق من الشروط العامة لإبرام التعاقد والمتضمنة القبول والإيجاب والأهلية والرضاء،
  3. عملية الكتابة الالكترونية لموضوع التعاقد (محل وسبب الالتزام)، وإجراء التوقيع والحفظ في وقت يحقق الحضور الزماني للأطراف المتعاقدة،
  4. عملية التحقق من سلامة العقد وبنوده، من ناحية أنه لم يجر عليه أية تعديلات بعد إجراء التوقيع، ويكون ذلك من خلال السجل الرقمي،
  5. عملية التحقق من وقوع الحدث المرتبط بانتهاء صلاحية حق العدول (على حسب الحالة)، وتوثيقها في السجل الرقمي (معاملة مرتبطة بنوع من التدفقات نقدية).

- يراعى أن يتم الالتزام بضوابط الهوية الرقمية الأطراف التعاقد الرقمي في مزاولة الأنشطة غير المصرفية، وعلى أن يتم تضمين الرقم المرجعي الفريد للشخص الطبيعي (FRA.IFP code)، فقط في حال تمثيله لنفسه، أو أن يكون مقرون بالرقم المرجعي الفريد للشخص الاعتباري (FRA.IFC code) في حال التمثيل القانوني لشخص اعتباري، أو أن يكون مقرون بالرقم المرجعي الفريد لشخص طبيعي آخر أو أشخاص طبيعيين آخرين (FRA.IFP code) في حال التمثيل القانوني للشخص الطبيعي الآخر أو للأشخاص الطبيعيين الآخرين (الوكالة)، ويكون ذلك لجميع أطراف التعاقد من متعاملين ومقدمي خدمات في الأسواق المالية غير المصرفية. ويراعى أن يتم توضيح ذلك في برامج التوعية للمتعاملين.

NBFS-
eContract

(NBFP)
DIG CONTRACT

العقود الرقمية ... وعمليات ابرام التعاقدات على منتج مالي غير مصرفي إلكترونياً

- استناداً إلى تعريف "الكتابة الإلكترونية" في قانون التوقيع الإلكتروني رقم 15 لسنة 2004 وتبني مفهوما موسعا للكتابة ومنح الكتابة الإلكترونية نفس الحجية القانونية المقررة للكتابة التقليدية للإثبات، على أنها تقوم بنفس الدور الذي تقوم به الكتابة التقليدية طالما أنه يمكن قراءتها وتدل بوضوح على مضمون التصرف القانوني وطالما كانت مدونة على دعامة إلكترونية تضمن لها الاستمرارية وتخول للأطراف الرجوع إليها عند الضرورة، بالإضافة إلى كونها تضمن عدم التعديل في بياناتها على نحو يوفر للمتعاملين الأمان والثقة. وينطبق ذلك التعريف على "المحررات الرقمية" المذكورة بصفة عامة في هذا القرار، كما يتم تحقيق هذه المقاصد في حال "العقود الرقمية للمنتجات المالية غير المصرفية" من خلال:

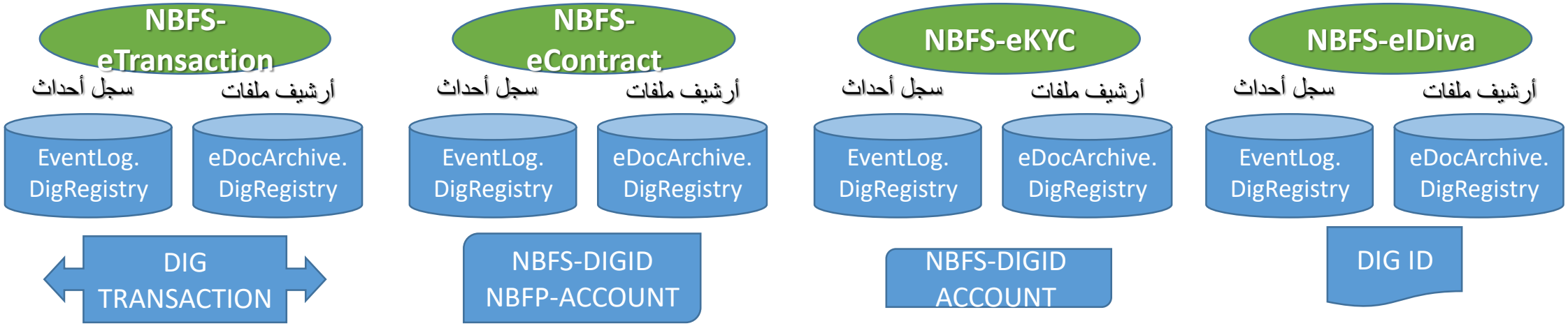
1. إثبات الايجاب: عرض العقد الرقمي من المنصة الرقمية على شاشة الجهاز الطرفي المحمول للمتعاقد،
2. إثبات القبول: التوقيع عليه باستخدام الآلية المناسبة ويكون ذلك مقروناً باستخدام نفس الجهاز الطرفي المحمول،
3. إثبات الأهلية: توثيق أهلية المعاملة وقدرة المتعامل للتمييز من خلال الكاميرا المرتبطة بالجهاز الطرفي المحمول،
4. حفظ العقد الرقمي الموقع الكترونياً مع التوقيتات التي تمت فيها مراحل الإيجاب والقبول والأهلية، في السجل الرقمي باستخدام تقنية التشفير والتي تمكن من اكتشاف أي تعديل في البيانات الإلكترونية كما تمكن من تحديد بدقة البيانات المعدلة وتاريخ تعديلها. وتتضمن تقنية التشفير تركيز وضغط محتوى المعاملة التي يتم التوقيع عليها، ويكون ذلك باستخدام مفاتيح سرية وطرق حسابية معقدة ومعادلات رياضية (لوغاريتمات) تتحول بواسطتها المعاملة من رسالة ذات كتابة عادية مقروءة ومفهومة إلى معادلة رياضية أو رسالة رقمية غير مقروءة وغير مفهومة، ما لم يتم فك تشفيرها ممن يملك مفتاح فك الشفرة وهو المعادلة الخاصة بذلك.

- في حال التعاقدات الرقمية المرتبطة بتنفيذ معاملات ذات درجة المخاطر المحدودة، يتم استخدام تقنية التشفير المناسبة مع تضمين بيانات حساب الدفع الالكتروني التي تم التحقق من حيازتها، ويتضمن العقد الرقمي في هذه الحالة موافقة المتعاقد على استخدام الحساب لإتمام المعاملات المرتبطة بالتدفقات النقدية المتوافق عليها من خلال مقدمي وميسري خدمات الدفع الالكتروني المعتمدين من البنك المركزي.
- في حال التعاقدات الرقمية المرتبطة بتنفيذ معاملات ذات درجة المخاطر العالية، يتم استخدام تقنية التوقيع الالكتروني المقرون بشفرة المفتاحين العام والخاص (المعروفة باسم تقنية شفرة المفتاح العام)، من أحد مقدمي خدمات التصديق على التوقيع الإلكتروني المصرح لهم من هيئة تنمية صناعة تكنولوجيا المعلومات.
- ويترك أمر تحديد درجة خطورة المعاملة لمقدمي الخدمات، وفي كل حال تكون عملية إنشاء الهوية الرقمية، والتعرف على العميل عن بعد بغرض إنشاء حساب من العمليات ذات المخاطر المنخفضة، وتكون عملية التعاقد على منتج مالي غير مصرفي عن بعد من العمليات ذات المخاطر المتوسطة.

السجلات الرقمية ... وعمليات تسجيل قيد أو ملف في السجل الرقمي إلكترونياً

- معايير الإنشاء:

1. يكون "السجل الرقمي" قابل للتجزئة لسجلات رقمية يكون كلٍ منها مخصص لنوع واحد من العمليات والمعاملات المرتبطة بخدمة من خدمات المنصة الرقمية، وعلى سبيل المثال:
    1. "السجل الرقمي" لعمليات "التحقق والإصدار والمصادقة على الهوية الرقمية" والمتضمن معاملات "إنشاء/تعديل/تحديث/تجديد/إلغاء هوية رقمية
    2. "السجل الرقمي" لعمليات "التعرف على العميل" والمتضمن معاملات "إنشاء/تعديل/تحديث/تجديد/إلغاء حساب عميل رقمي
    3. "السجل الرقمي" لعمليات "التعاقد الالكتروني على منتج مالي غير مصرفي" والمتضمن معاملات "إنشاء/تعديل/تحديث/تجديد/إلغاء حساب منتج مالي غير مصرفي رقمي
    4. "السجل الرقمي" لعمليات "المعاملات المرتبطة بالمنتج المالي غير المصرفي والمتضمن معاملات "إنشاء/تعديل/تحديث/تجديد/إلغاء معاملة على حساب منتج مالي غير مصرفي رقمي، وتكون مرتبطة بطبيعته مثل سداد قسط، طلب تعويض، طلب بيع، طلب شراء.
2. يكون "السجل الرقمي" قابل لاحتواء وحفظ واسترجاع:
    1. بيانات وتفاصيل المعاملة وتسجيل الأحداث (Event Logging) المرتبطة بالعمليات المختلفة مع بيان أطرافها وتوقيتاتها وسياقها ونتيجتها كلما تغيرت الحالة للأصل الرقمي
    2. المستندات الرقمية المرتبطة كمدخل أو مرفق أو مخرج للمعاملة وأرشفة هذه المستندات الرقمية (Document Archiving)



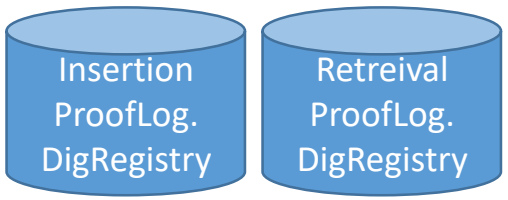
السجلات الرقمية ... وعمليات تسجيل قيد أو ملف في السجل الرقمي إلكترونياً

- معايير الإنشاء:

3. في جميع الأحوال يجب أن يتضمن السجل الرقمي الخصائص التي تمكن "التحليل الجنائي الرقمي" (Digital Forensics) للأحداث والتي قد تشمل سلوك غير سوي أو مخالفات للقوانين، وبما يسمح بإعادة عرض الأحداث على جهات قضائية بدرجة ثقة الحجية القانونية والتي تضمن عدم التلاعب أو التغيير في سجلات الأحداث، من خلال سلسلة منهجية من الأساليب والإجراءات الخاصة بجمع الأدلة، من مكونات البنية التكنولوجية والمتضمنة أجهزة الشبكات وأجهزة الحاسبات وسائل التخزين وأنظمة إدارة البيئات الافتراضية والاحتوائية وأنظمة التشغيل وأنظمة إدارة قواعد البيانات وأنظمة التحكم في السماحية والدخول، ومن مكونات نظم المعلومات والمتضمنة التطبيقات وقواعد البيانات، ويكون ذلك بطريقة متناسقة ومتسلسلة.

1. يجب أن تكون السجلات المرتبطة بالمكونات المختلفة في متناول مختلف أصحاب المصلحة، والذين يشملوا على سبيل المثال، مسؤول النظام، والمحقق الجنائي، والمطور. يحتاج مسؤولو النظام إلى السجل ذي الصلة لاستكشاف أخطاء النظام وإصلاحها؛ يحتاج التطوير إلى السجل المطلوب لإصلاح خطأ التطبيق؛ يحتاج محققو التحليل الجنائي إلى سجلات يمكن أن تساعد في تحقيقاتهم. ومن ثم، يجب أن يكون هناك بعض آليات التحكم في الوصول، بحيث يحصل الجميع على ما يحتاجون إليه بالضبط (need-to-know-basis)، لا أكثر، ولا أقل، وبطريقة آمنة.
2. في حال الاعتماد على نماذج عمل الحوسبة السحابية العامة أو الخاصة والتي تقدم خدمات متنوعة على نفس البيئة التكنولوجية المشتركة لأكثر من عميل، يجب التأكد من الفصل التام بين البيئة الافتراضية لكل عميل.
3. يجب أن يتضمن السجل الرقمي ما يساهم في إثبات وتوثيق التسلسل في الحيازة (chain-of-custody) على المخرجات من السجل الرقمي وبما يحافظ على:
    1. خصوصية البيانات
    2. عدم التعديل بالحذف أو بالإضافة أو بالتغيير (من مسئول المنصة الرقمية أو من مستخدم المنصة الرقمية أو من المحقق الجنائي أو من أي طرف خارجي)
    3. ما يمنع انكار محتوى السجل من مسئول المنصة الرقمية
    4. ما يمنع انكار محتوى السجل من مستخدم المنصة الرقمية
4. من تاريخ حفظ البيانات في السجل الرقمي
ومن تاريخ استخراج البيانات من السجل الرقمي في مخرجات اثبات التسجيل، تحوز تلكا البيانات حجية المحررات الرسمية في الإثبات

سجل اضطلاع على حدث سجل إضافة حدث



NBFS-
eRegistry

DIG
REGISTRY

السجلات الرقمية ... وعمليات تسجيل قيد أو ملف في السجل الرقمي إلكترونياً

- ضوابط العمل:

1. يتم استخدام تقنية التشفير المناسبة لضمان سرية وسلامة محتويات السجل الرقمي واستخدام آليات لضمان عدم تعديل المحتوى بعد حفظه وتخزينه
2. يتم توفير وسائل تخزين مناسبة ذات سعة تخزينية للحفاظ على السجلات والمستندات الرقمية لمدة 5 سنوات على الأقل من بعد انتهاء صلاحية الأصل الرقمي موضوع التسجيل بانتفاء الغرض منه وبموافقة الجهات المالكة والمستفيدة من الأصل، ويجوز أرشفة السجلات والمستندات بعد هذه المدة في وسائل تخزين خارج البيئة التشغيلية الحية، أو التخلص منها بعد إخطار الهيئة وموافقتها.
3. يتم استخدام نظم إدارة قواعد بيانات وإدارة ملفات مناسبة مع التأكد من توفيرها درجات الاعتمادية القصوى، والتأكد من تطبيق آليات إدارة حالات فشل التسجيل المناسبة والتأكد من تطبيق آليات استمرارية الأعمال والتعافي من الكوارث المناسبة.
4. يتم التأكد من وجود أليات للتحقق وللبحث وللتلخيص وإصدار التقارير عن محتوى السجلات دون المساس بمتطلبات التأمين والحماية، مع وجود آليات لتسجيل عمليات التحقق والبحث مع بيان توقيتاتها دون المساس بتوقيتات الأحداث الأصلية.
5. يفضل أن يتم الالتزام بنموذج تنسيق للتسجيل المستخدم على نطاق واسع وهو (Syslog)، المحدد في Internet Engineering Task Force (IETF) RFC 5424)، ويجوز أن يتم استخدام نموذج تنسيق بديل بعد العرض على الهيئة وأخذ موافقتها.
6. يجوز تطبيق السجل الرقمي على "تقنية مجموعة القيود الموزعة" (Distributed Ledger Technology)، أو "تقنية سلسلة الكتل" (Blockchain Technology) في إدارة سجلات الشركات أو الجهات المالية غير المصرفية، بما في ذلك سجلات الأسهم وحملة الأسهم، وسجلات شركات الإيداع والقيد المركزي، وسجلات الضمانات، وسجلات التعرف على العميل (على سبيل المثال)، ويكون ذلك بعد التقدم بطلب للهيئة والموافقة مع تخصيص "منسق عام" لكل "سجل موزع"، وهو المسؤول عن إشراك أصحاب المصلحة في المنظومة لتحديد احتياجات كل منهم والعمل بشكل قاطع على حلها والذي قد يتم تنفيذه من خلال "تقنية سلسلة الكتل" كنوع من أنواع السجلات الموزعة.

NBFS-eContract

NBFS-eKYC

NBFS-eIDiva

NBFS-eRegistry

مجالات التكنولوجيا المالية غير المصرفية – تطبيقات الأنظمة لعمليات ...

- اعتماد الأنظمة المستخدمة في:

1. عمليات التحديد والتحقق والمصادقة على الهوية إلكترونياً (NBFS-eIDiva)
2. وعمليات التعرف على العميل إلكترونياً (NBFS-eKYC) ،
3. وعمليات إبرام التعاقدات على المنتجات إلكترونياً (NBFS-eContract)،
4. وعمليات التسجيل والحفظ في والاسترجاع من السجلات الرقمية إلكترونياً (NBFS-eRegistry)،

كتطبيقات إلكترونية "داعمة" لمجالات التكنولوجيا المالية غير المصرفية

تكون مجالات التكنولوجيا المالية هذه متاحه للشركات والجهات الخاضعة لرقابة الهيئة والراغبة في الحصول على ترخيص أو موافقة بحسب الأحوال لمباشرتها أنشطتها المالية غير المصرفية باستخدامها، وتلتزم هذه الشركات باتخاذ التدابير التي من شأنها الحفاظ على صلاحيتها لأداء مهامها، كما تلتزم بتوفير النظم اللازمة لحماية البيانات الخاصة بالمتعاملين من الاختراق الإلكتروني، كما تلتزم الجهات الراغبة في الحصول على موافقة الهيئة بالشروط والإجراءات.

NBFS-eContract

NBFS-eKYC

NBFS-eIDiva

NBFS-eRegistry

مجالات التكنولوجيا المالية غير المصرفية – خدمات تعهيد لعمليات ...

- اعتماد الخدمات التعهيد المستخدمة في:

1. عمليات التحديد والتحقق والمصادقة على الهوية إلكترونياً (NBFS-eIDiva)
2. وعمليات التعرف على العميل إلكترونياً (NBFS-eKYC) ،
3. وعمليات إبرام التعاقدات على المنتجات إلكترونياً (NBFS-eContract)،
4. وعمليات التسجيل والحفظ في والاسترجاع من السجلات الرقمية إلكترونياً (NBFS-eRegistry)،

كخدمات تعهيد "داعمة" لمجالات التكنولوجيا المالية غير المصرفية

- تكون خدمات التعهيد هذه متاحه للشركات والجهات المرخص لها من الهيئة بمزاولة الأنشطة المالية غير المصرفية حال رغبتها في استخدام بعض مجالات التكنولوجيا المالية غير المصرفية من خلال شركات التعهيد، والتي تلتزم بشروط وإجراءات الحصول على موافقة الهيئة.
- كما تكون متاحة لشركات خدمات التعهيد الراغبة في تقديم هذه الخدمات، والتي تلتزم بضوابط القيد والشطب التي تضعها الهيئة للقيد بسجل خدمات التعهيد والمتضمنة:

1. الخبرة المتطلبة في الجهات الراغبة في القيد بالسجل
2. الالتزامات التي يجب أن تلتزم بها الجهات الراغبة في القيد بالسجل
3. حالات الشطب من السجل

NBFS-eIDiva

متطلبات الامتثال – لكل عملية من العمليات الوظيفية المحددة

- يجب التأكد بشكل مستمر من الالتزام التام بالمتطلبات القانونية والإجراءات التنظيمية ذات الصلة، ويعد تقرير نصف سنوي بشأن "نتائج أعمال المراجعة ونسب الخطأ "، أخذاً في الاعتبار طبيعة وحجم النشاط الذي تزاوله الجهة، ويجب موافاة الهيئة بهذا التقرير معتمداً من مجلس إدارة الجهة خلال أربعة أسابيع من تاريخ انتهاء المدة المقدم عنها التقرير، وذلك لكل من عمليات ومجالات التكنولوجيا المالية غير المصرفية التي يمكن استخدامها في مزاولة الأنشطة المالية غير المصرفية:
  - لمراقبة فعالية ودقة منظومة "تحديد وتحقق ومصادقة الهوية رقمياً"، يجب على الشركات أو الجهات الحاصلة على ترخيص أو موافقة الاحتفاظ بسجل لقياس مستوى الأداء ومن أهمها معدلات القبول الخاطئة (FAR) أو معدلات الرفض الخاطئ (FRR). مقسم على أساس شهري وفقًا للنموذج التالي:

	شهر 1	....	شهر 6	إجمالي الفترة
1. اجمالي عدد عمليات التحديد والتحقق				
2. اجمالي عدد حالات القبول				
3. إجمالي عدد الحالات التي تم مراجعتها				
4. عدد حالات القبول الصحيحة				
5. عدد حالات الرفض الصحيحة				
6. عدد حالات القبول الخاطئة				
7. عدد حالات الرفض الخاطئة				
8. معدل القبول الخاطئ = 6 / (5+6)				
9. معدل الرفض الخاطئ = 7 / (4+7)				

NBFS-eKYC

متطلبات الامتثال – لكل عملية من العمليات الوظيفية المحددة

- لمراقبة فعالية ودقة منظومة "تعرف على العميل إلكترونياً"، يجب على الشركات أو الجهات الحاصلة على ترخيص أو موافقة الاحتفاظ بسجل لقياس مستوى الأداء ومن أهمها معدلات القبول الخاطئة (FAR) أو معدلات الرفض الخاطئ (FRR). مقسم على أساس شهري وفقًا للنموذج التالي:

	شهر 1	....	شهر 6	إجمالي الفترة
1. اجمالي عدد عمليات التعرف على العميل				
2. اجمالي عدد حالات القبول				
3. إجمالي عدد الحالات التي تم مراجعتها				
4. عدد حالات القبول الصحيحة				
5. عدد حالات الرفض الصحيحة				
6. عدد حالات القبول الخاطئة				
7. عدد حالات الرفض الخاطئة				
8. معدل القبول الخاطئ = 6 / (5+6)				
9. معدل الرفض الخاطئ = 7 / (4+7)				

NBFS-
eContract

متطلبات الامتثال – لكل عملية من العمليات الوظيفية المحددة

- لمراقبة فعالية ودقة منظومة "إبرام التعاقد إلكترونياً"، يجب على الشركات أو الجهات الحاصلة على ترخيص أو موافقة الاحتفاظ بسجل لقياس مستوى الأداء ومن أهمها معدلات القبول الخاطئة (FAR) أو معدلات الرفض الخاطئ (FRR). مقسم على أساس شهري وفقًا للنموذج التالي:

	شهر 1	....	شهر 6	إجمالي الفترة
1. اجمالي عدد عمليات ابرام التعاقد الكترونياً				
2. اجمالي عدد حالات القبول				
3. إجمالي عدد الحالات التي تم مراجعتها				
4. عدد حالات القبول الصحيحة				
5. عدد حالات الرفض الصحيحة				
6. عدد حالات القبول الخاطئة				
7. عدد حالات الرفض الخاطئة				
8. معدل القبول الخاطئ = 6 / (5+6)				
9. معدل الرفض الخاطئ = 7 / (4+7)				

NBFS-
eRegistry

متطلبات الامتثال – لكل عملية من العمليات الوظيفية المحددة

- لمراقبة فعالية ودقة منظومة "إضافة قيد معاملة للسجل إلكترونياً"، يجب على الشركات أو الجهات الحاصلة على ترخيص أو موافقة الاحتفاظ بسجل لقياس مستوى الأداء ومن أهمها معدلات القبول الخاطئة (FAR) أو معدلات الرفض الخاطئ (FRR). مقسم على أساس شهري وفقًا للنموذج التالي:

	شهر 1	....	شهر 6	إجمالي الفترة
1. اجمالي عدد عمليات إضافة قيد للسجل الكترونياً				
2. اجمالي عدد حالات القبول				
3. إجمالي عدد الحالات التي تم مراجعتها				
4. عدد حالات القبول الصحيحة				
5. عدد حالات الرفض الصحيحة				
6. عدد حالات القبول الخاطئة				
7. عدد حالات الرفض الخاطئة				
8. معدل القبول الخاطئ = 6 / (5+6)				
9. معدل الرفض الخاطئ = 7 / (4+7)				

- ولمراقبة فعالية ودقة منظومة " إضافة ملف رقمي للسجل إلكترونياً " يجب على الشركات أو الجهات الحاصلة على ترخيص أو موافقة الاحتفاظ بسجل لقياس مستوى الأداء ومن أهمها معدلات القبول الخاطئة (FAR) أو معدلات الرفض الخاطئ (FRR). مقسم على أساس شهري وفقًا للنموذج التالي:

	شهر 1	....	شهر 6	إجمالي الفترة
1. اجمالي عدد عمليات إضافة ملف للسجل الكترونياً				
2. اجمالي عدد حالات القبول				
3. إجمالي عدد الحالات التي تم مراجعتها				
4. عدد حالات القبول الصحيحة				
5. عدد حالات الرفض الصحيحة				
6. عدد حالات القبول الخاطئة				
7. عدد حالات الرفض الخاطئة				
8. معدل القبول الخاطئ = 6 / (5+6)				
9. معدل الرفض الخاطئ = 7 / (4+7)				

قرار 140
لسنة 2023

ضوابط القيد والشطب في سجل الجهات الراغبة في تقديم خدمات التعهيد

- شروط القيد في سجل الجهات الراغبة في تقديم خدمات التعهيد:

1. أن تكون شركة مساهمة مصرية، أو أي شكل من الأشكال الأخرى على أن تتعهد بتحويل شكلها القانوني إلى شركة مساهمة بحد أقصى 12 شهراً من تاريخ قيدها بالسجل.
2. ألا يقل رأس مال الشركة عن الحد الأدنى الذي تحدده الهيئة.
3. أن تتوافر لديها خبرات مناسبة حسب المجال، على النحو الذي تقرره الهيئة.
4. أن يتوافر بالشركة قواعد الحوكمة اللازمة وتطبيقاتها والتي تكفل إحكام بيئة الرقابة الداخلية بالشركة.
5. أن يتوافر لديها الإمكانات التكنولوجية اللازمة لضمان أمن بيانات عملاء العاهد، وحماية خصوصية وسرية البيانات المتعلقة بالخدمة، والإجراءات التصحيحية اللازمة عند ظهور أي خلل في مستوى الآداء وتسجيل الأحداث المرتبطة.
6. التعهد بإبرام وثيقة تأمين ضد المخاطر التكنولوجية والمسئولية المهنية.
7. سداد قيمة مقابل خدمة القيد في السجل وقدره 25000 جنيه، عن كل مجال.

- يحق للهيئة شطب مقدم التعهيد من السجل حال فقده لأحد شروط القيد وعدم قدرته على توفيق أوضاعه، كما يجوز الشطب في حال عدم الامتثال بالالتزامات المحددة والتقاعس عن تصحيحها، ولا يجوز أعادة القيد إلا بعد إزالة أسباب الشطب ومرور مدة على الشطب لا تقل على سنتين.

قرار 140
لسنة 2023

ضوابط اتفاقية التعهيد

- تكون **اتفاقية التعهيد** اتفاقية ملزمة قانونا بين الجهة العاهدة (متلقي الخدمة) ومقدم خدمة التعهيد (مقدم التعهيد) وتتضمن كحد أدني:

1. المدة الزمنية للاتفاقية مثبت بها كل من تاريخ البدء، وتاريخ الانتهاء، وتاريخ التجديد.
2. تحديد نطاق أعمال مقدم التعهيد ومعاير قياس الأداء، والمخاطر التي يمكن قياسها بشكل واضح ومحدد
3. تحديد مؤشرات أداء واضحة للتقييم المستمر لمستوى جودة الخدمة
4. الضوابط والإجراءات المتبعة والخاصة بأمن البيانات ومسئولية مقدم الخدمة تجاه تلك البيانات.
5. نطاق البيانات الواجب حمايتها (البيانات الشخصية الحساسة)، واقتصار تبادل البيانات والمعلومات على ما يكون لازماً لتنفيذ نطاق الأعمال المحدد.
6. إدراج بند بشأن سرية البيانات وكذا توقيع اتفاقية عدم إفصاح لضمان امن البيانات وتحديد مدى المسئولية في حالة الخرق الأمني وتسريب المعلومات السرية.
7. الاحكام الملزمة لتعويض متلقي الخدمة عن أي خسائر او التزامات قد تنشأ نتيجة خرق أمني منسوب إلى مقدم الخدمة.
8. أساليب اخطار مقدم الخدمة لمتلقي الخدمة في حال حدوث الخرق الأمني وتسريب المعلومات السرية.

ضوابط اتفاقية التعهيد - بقية

- تكون **اتفاقية التعهيد** اتفاقية ملزمة قانونا بين الجهة العاهدة (متلقي الخدمة) ومقدم خدمة التعهيد (مقدم التعهيد) وتتضمن كحد أدني:

9. تضمين ما يضمن قيام متلقي الخدمة بدوره في الاشراف والرقابة على الأنشطة بشكل فعال، وحقه بشكل كامل ومستمر في الوصول إلى جميع البيانات والمعلومات المتبادلة لدى مقدم التعهيد.
10. ضمان احقية متلقي الخدمة في التمكن الكامل من بيانات عملائه في حال فسخ التعاقد او في حالة النزاع ما بين الطرفين.
11. التزام موظفي مقدم التعهيد، الذين يشاركون في تقديم الخدمات إلى عملاء الجهة العاهدة، بالامتثال لمعايير والمتطلبات المماثلة التي تفرضها الهيئة على الجهة العاهدة.
12. حق الهيئة بالحصول مباشرة وفوراً ودون أي شروط على أي معلومات أو مستندات متعلقة بالخدمة المقدمة أو الوصول للنظام المستخدم.
13. حق الهيئة في التفتيش والإشراف على مقدم التعهيد حالة وجوة ضرورة لذلك، وحق الهيئة في الاستعانة بأطراف خارجية للقيام بذلك.
14. حق الجهة العاهدة في إنهاء العقد حال صدور قرار من الهيئة بإنهاء خدمة التعهيد
15. إجراءات فض النزاع في حال الإهمال وعدم الالتزام.
16. الملابسات وحالات التقاعس التي قد تؤدى الى انهاء الاتفاقية.

حقوق والتزامات الجهة العاهدة

1. لا يجوز تعهيد العمليات والمهام والأعمال الرئيسية بما يترتب عليه التفريغ من هدف الترخيص للأنشطة المالية غير المصرفية، وفى جميع الأحوال يجب الحصول على موافقة الهيئة على العمليات الاعمال والمهام التي ترغب الشركة او الجهة في تعهيدها.
2. لا يؤثر التعهيد في مسؤوليات والتزامات الجهة العاهدة، وتظل الجهة العاهدة مسؤولة مسؤولية كاملة في جميع الأحوال عن أية إخفاقات في أداء المهام أو المسؤوليات أو الأعمال أو إخلال بالالتزامات، أو مخالفة للتشريعات المعمول بها.
3. في كل الأحوال تكون الجهة العاهدة هي المسئولة عن سلامة الاعمال التي يقوم مقدم التعهيد بإدائها وفي سبيل ذلك لابد ان تمتلك الجهة العاهدة الكوادر الفنية التي تمكنها من تقييم سلامة وجودة الاعمال التي ينفذها مقدم التعهيد.
4. على مجلس إدارة الجهة العاهدة اعتماد خطة تعهيد متكاملة ومفصلة للعام المالي التالي.
5. يجب الالتزام بإبرام اتفاقية تعهيد على النحو المفصل في 5.1.3 مع مقدم التعهيد.
6. بذل عناية الرجل الحريص عند اختيار مقدم التعهيد لأداء أي أعمال أو مهام.
7. يجب اخطار الهيئة عند ابرام أي اتفاقية تعهيد، او اجراء تعديل جوهري لاتفاقية التعهيد القائمة.
8. وجود سياسة تعهيد محددة وواضحة تضمن مؤشرات تقييم الأداء KPIs لمتابعة أداء مقدمي التعهيد.
9. وضع المناهج او الطرق المناسبة لضمان ان مقدم التعهيد لا يعوقها او يعارضها في الاشراف على أنشطتها وادارتها بشكل دائم وفعال، كما انه لا يعوقها في أداء مهامها.
10. ان تتوافر لدى الشركة خطة محكمة او سياسات محددة لإدارة مخاطر التعهيد (Outsourcing Risk Management Framework)، على ان يتم مراجعتها وامداد الهيئة بها بشكل سنوي.
11. مراقبة والسيطرة على كافة مراحل خدمة التعهيد بداية من تطويرها الى اختبارها الى تنفيذها ثم تشغيلها، والقيام بالإجراءات التصحيحية اللازمة عند ظهور أي خلل في مستوى أداء مقدم التعهيد.
12. الاحتفاظ بسجل مؤشرات أداء واضحة للتقييم المستمر لمستوى جودة الخدمة المقدمة من مقدم التعهيد وامداد الهيئة بها بشكل سنوي.

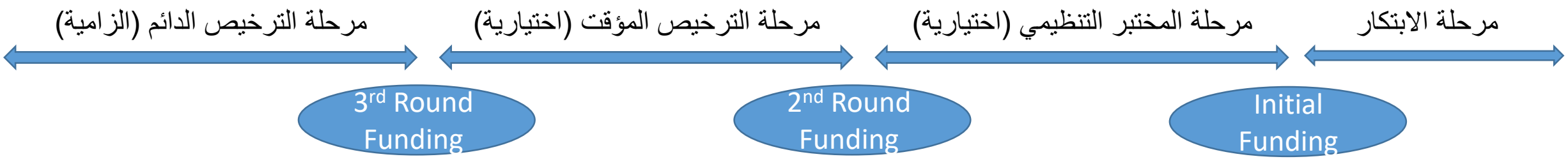
حقوق والتزامات مقدم التعهيد

1. في جميع الأحوال يجب أن يلتزم مقدم التعهيد بمساعدة الجهة العاهدة في الامتثال بالضوابط الصادرة من الهيئة والمنظمة للعمليات والمهام والأعمال موضوع التعهيد، والمتضمنة على سبيل المثال "ضوابط التجهيزات والبنية التكنولوجية وأنظمة المعلومات ووسائل الحماية والتأمين والوظائف التكنولوجية الرئيسية".
2. ضمان أمن بيانات عملاء الجهة العاهدة وكذلك عدم جواز احتفاظ مقدم التعهيد ببيانات عملاء الشركة والخدمة التي تنفذها وكذلك استخدام الوسائل المناسبة لحماية خصوصية وسرية تلك البيانات والعمل على ضمان عدم الوصول غير المسموح به له.
3. وضع إجراءات احترازية بشأن أمن البيانات وخطة استمرارية العمل.
4. القيام بالإجراءات التصحيحية اللازمة عند ظهور أي خلل في مستوى الأداء وتسجيل الأحداث المرتبطة، ومما يمكن الجهة العاهدة والهيئة من مراجعة تلك الأحداث.
5. إخطار الجهة العاهدة والهيئة في حال طلبت أي جهة رقابية تخضع لها شركة التعهيد إعمال شئونها الرقابية بالمراجعة والتفتيش، وبنتائج هذه الأعمال.

التكنولوجيا المالية المبتكرة

منتجات مبتكرة للمتعاملين الحاليين أو الجدد (حماية سنتين اعتماد المنتجات)

منتجات تقليدية لمتعاملين جدد (الشمول المالي)



Ideation	Proof-of-Concept	Product Growth	Fair Competition
Feasibility Study	Product Ready-to-Market	Portfolio Growth	“Survival of the fittest”
	Highly Controlled “Market Exposure”	Limited “Market Exposure”	Open “Market Exposure”
	Product Scale # Customers Customer Profile (Risk Tolerance) Geographic Distribution # & amount of transactions	Product Scale # Customers Customer Profile (Risk Tolerance) Geographic Distribution # & amount of transactions	

مراحل تقديم الطلبات للجنة التكنولوجيا المالية بالهيئة
(FinTech@fra.gov.eg)

الاعداد

- تتلقي اللجنة الاستفسارات على متطلبات التقديم (كيفية توثيق نموذج الأعمال، قوائم التحقق من الامتثال، أو أياَ من المستندات المطلوبة)
- تتلقى اللجنة طلبات التعليق على «مشروع الطلب» (للوقوف على مدى اكتماله)
- يتم الرد من الجنة مباشرةً أو بعد دعوة الشركة مقدمة مشروع الطلب لورشة عمل للتوضيح وللاستيفاء

التقديم

- تتلقى اللجنة الطلبات (ترخيص، موافقة، قيد).
- تقوم الهيئة بعمل فحص أولي **preliminary review** لما تم تقديمهم قبل الشركات
- يتم دعوة الشركة مقدمة الطلب لورشة عمل لعرض تقديمي لنموذج العمل وآليات التحقق من الامتثال
- تقوم الهيئة بإجراءات فحص العناية الواجبة (Due Diligence) والتدقيق (Audit).
- يتم اتخاذ القرار من قبل الهيئة والرد على الشركات.

كما تختص اللجنة بدراسة:
الشكاوى والمقترحات وطلبات الإضافة لمجالات التكنولوجيا المالية