المسابقة الرابعة عشر للبحث العلمي للمنظمة العربية للأجهزة العليا للرقابة المالية والمحاسبية

حول موضـوع:

الرقابة على نظم المعلومات السبيراني

– دراسة حالة رقابة نظم المعلومات السبيراني للمؤسسة الوطنية للكهرباء والغاز

من اعداد الســـيد:

محمودي امحمد

مدير دراسات

مجلس المحاسبة

-2024-

ملخص البحث:

تعد الرقابة على نظم المعلومات والأمن السيبراني من المواضيع الحيوية والمعاصرة في مجال تدقيق تكنولوجيا المعلومات، حيث تتزايد أهميتها مع التهديدات السيبرانية المتنامية والاعتماد المتزايد على التكنولوجيا في القطاع العام. تهدف هذه الدراسة إلى تسليط الضوء على دور الأجهزة العليا للرقابة المالية والمحاسبة في تقييم نظم المعلومات والأمن السيبراني، مع التركيز على تحديات التدقيق وأهميته في تعزيز الحوكمة والشفافية، بالإضافة إلى المعايير والممارسات الفضلى والمنهجية الرقابية.

تم اعتماد المنهج التحليلي الاستقرائي في هذه الدراسة، حيث تم تقديم إطار نظري لتقييم نظم المعلومات والأمن السيبراني، مع استعراض التحديات التي تواجه الأجهزة الرقابية في هذا المجال. وفي الجانب التطبيقي، تم التركيز على تقييم نظم المعلومات والأمن لشركة سونلغاز للتوزيع، حيث تم تحديد الأهداف والنطاق والمنهجية المعتمدة، واستخدام أسلوب التقييم المعتمد على المخاطر، وجمع الأدلة، وتنفيذ التدقيق وتحليل النتائج. وتمت مراجعة النتائج مع المنظمة المدققة ووضع التقرير الرقابي تحت تصرف الفريق الرقابي والغرفة المعنية.

أسفرت الدراسة عن نتائج مهمة، منها:

أهمية فهم شامل للمفاهيم الأساسية لرقابة نظم المعلومات والأمن السيبراني وتحديد الأهداف الرئيسية لتدقيق تكنولوجيا المعلومات. كما تم تسليط الضوء على جهود الجزائر في تعزيز الحوكمة السيبرانية وتطوير استراتيجيات الأمن السيبراني. دور تدقيق تكنولوجيا المعلومات في الحماية من التهديدات السيبرانية المعقدة والمتزايدة، وضمان الامتثال التنظيمي وتقليل مخاطر الهجمات السيبرانية. دور الأجهزة العليا للرقابة المالية والمحاسبة في تعزيز الرقابة على نظم المعلومات في ظل التحول الرقمي، وضرورة التعاون الدولي، وإنشاء وحدات متخصصة وتدريب الكوادر واعتماد أفضل الممارسات والمعايير الدولية.

باختصار، يعد تأمين نظم المعلومات وضمان أمنها عملية معقدة تتطلب تعاوناً وثيقاً بين مختلف الهيئات العليا للرقابة والمؤسسات الحكومية والقطاع الخاص. يجب أن يكون هناك تنسيق فعال بين هذه الجهات لضمان تنفيذ أفضل الممارسات والسياسات الأمنية وتطوير استراتيجيات متكاملة لمواجهة التهديدات السيبرانية. إن تعزيز الرقابة على نظم المعلومات والأمن السيبراني لا يسهم فقط في تحقيق الشفافية والكفاءة، بل أيضاً في تعزيز الثقة بين الجمهور والمؤسسات، وضمان استمرارية الأعمال وحماية البيانات الحساسة من الهجمات السيبرانية. من خلال هذا التعاون، يمكن بناء نظام

حكومي واقتصادي قوي قائم على البيانات، يدعم الابتكار ويعزز النمو الاقتصادي، مما يؤدي إلى تحسين الخدمات المقدمة للمجتمع وتحقيق المصلحة العامة بفعالية وكفاءة عالية.

الكلمات المفتاحية: الرقابة على نظم المعلومات، الأمن السيبراني، الأجهزة العليا للرقابة المالية والمحاسبة، النهج القائم على المخاطر، شركة سونلغاز للتوزيع.

خطة البحث

المقدمة:

في ظل تصاعد وتيرة التحول الرقمي على مستوى العالم، تواجه بنى تكنولوجيا المعلومات تحديات أمنية متزايدة، مما يجعل الأمن السيبراني ضرورة ملحة لضمان سلامة وخصوصية البيانات. في هذا السياق، تبرز الحاجة الماسة لتعزيز رقابة نظم المعلومات، ليس فقط كإجراء دفاعي، بل كجزء من استراتيجية شاملة للأمن في المؤسسات والهيئات الحكومية.

الأجهزة العليا للرقابة المالية والمحاسبة تلعب دورًا محوريًا في هذه العملية، حيث تقدم الإشراف الضروري والتوجيه لتحسين الإجراءات الأمنية وضمان الامتثال للمعايير الدولية وأفضل الممارسات في مجال الأمن السيبراني. هذه الأجهزة لا تقتصر مهمتها على تقييم السياسات والإجراءات القائمة فقط، بل تساهم أيضًا في تطوير استراتيجيات فعالة تعزز من الكشف المبكر عن التهديدات ومواجهتها.

التدقيق الأمني السيبراني يمثل إحدى الأدوات الأساسية التي تستعين بها هذه الأجهزة لتحقيق أهداف الأمن. من خلال تقييم دقيق ومستمر للأنظمة والضوابط، يتم التحقق من فعالية الإجراءات الأمنية المطبقة ومدى امتثالها للمعايير. يتضمن هذا التقييم تحليل الثغرات الأمنية وتقديم توصيات لتعزيز الأمن وتقليل المخاطر. تتطلب تعزيز أمن المعلومات نهجًا متكاملًا يشمل تحديث السياسات، تطوير الكفاءات البشرية، وتسهيل مبادرات التدقيق المنهجي للمخاطر. يسعى هذا البحث إلى استكشاف كيفية مساهمة الرقابة المعززة على نظم المعلومات في تحقيق مستوى أعلى من الأمن السيبراني، مما يعزز قدرة المؤسسات على مواجهة التحديات الأمنية المعاصرة بكفاءة وفعالية.

في الجزائر، تقوم الهيئات المختصة في تكنولوجيا المعلومات والأمن السيبراني بدور رئيسي في دعم هذه الجهود، حيث تعمل على تطوير أدوات ووسائل متنوعة، وتقييم الأثر الذي يمكن أن تحدثه هذه الأدوات في تحقيق مستوى أعلى من الأمن السيبراني. يسعى مجلس المحاسبة الجزائري، كأحد الأجهزة العليا، إلى تنفيذ مبادرات تستجيب للسياسة الوطنية المتكاملة الرامية إلى تعزيز قدرات الرقابة على نظم المعلومات والتصدي للتحديات الأمنية بكفاءة وفعالية.

1. إشكالية البحث:

في ظل التحول الرقمي العالمي، تبرز تحديات أمنية متزايدة تواجه بنى تكنولوجيا المعلومات، مما يجعل الأمن السيبراني ضرورة ملحة لضمان سلامة وخصوصية البيانات. الأجهزة العليا للرقابة المالية والمحاسبة تلعب دورًا محوريًا في هذا السياق، من خلال تقييم ومراقبة الإجراءات الأمنية القائمة ومدى توافقها مع المعايير الدولية لأمن المعلومات والتنظيمات المحلية. على الرغم من أهمية التدقيق الأمني السيبراني كأداة

رئيسية لتحقيق الأمان، تواجه الهيئات العمومية تحديات كبيرة بسبب التعقيدات التقنية والتطورات المستمرة في المجال السيبراني، ومن هذا تم طرح الاشكالية التالية:

- ❖ هل يمكن للأجهزة العليا للرقابة المالية والمحاسبة تعزيز كفاءتها في التدقيق الأمني السيبراني لمواجهة التحديات المستمرة في بيئة تكنولوجيا المعلومات المعاصرة والمساهمة في تنفيذ استراتيجية الدولة لأمن المعلومات والأمن السيبراني؟

2. أسئلة فرعية:

- ما هي المفاهيم الأساسية للرقابة على نظم المعلومات والأمن السيبراني، وما أهميتها في مواجهة التحديات الحالية؟
- ما هي التحديات التي تواجه الأجهزة العليا للرقابة المالية والمحاسبة في تدقيق نظم المعلومات والأمن السيبـراني، وما دورها المحتمل في مواجهة هذه التحديات؟
- ما هي الخطوات الرئيسية والمنهجية العملية التي يمكن اتباعها في تقييم نظم المعلومات وأمن السيبراني؟

3. أهمية البحث

تتصدر الرقابة على نظم المعلومات والأمن السيبراني أهمية كبيرة في العصر الرقمي الحالي، إذ تمثل الأساس الذي يضمن سلامة البيانات والمعلومات الحساسة في المؤسسات والهيئات العامة. يهدف هذا البحث إلى تعزيز الفهم العلمي لمفاهيم الرقابة على نظم المعلومات والأمن السيبراني، وتقديم إرشادات عملية لتحسين أداء الرقابة والتدقيق في هذا المجال. ويسعى البحث أيضًا إلى فهم كيفية تعزيز الهيئات الرقابية العليا لأمن المعلومات والبيانات، وضمان إمكانية استخدام الأدوات والتقنيات الحديثة التي تساهم في تحقيق نتائج رقابية فعّالة.

بالإضافة إلى ذلك، يسلط البحث الضوء على ضرورة الالتزام بالمعايير الدولية وأفضل الممارسات في مجال الرقابة على نظم المعلومات والأمن السيبراني. وبذلك، يساهم البحث في بناء الثقة في استخدام التكنولوجيا الرقمية وتحقيق أهداف الرقابة على نظم المعلومات والأمن السيبراني بكفاءة وفعالية.

4. أهداف البحث

يسعى هذا البحث إلى تحقيق الأهداف التالية:

- تقديم إطار نظري شامل يشرح مفاهيم الرقابة على نظم المعلومات والأمن السيبراني وتطبيقاتها العملية.
- تحليل أسس وأهداف الرقابة على نظم المعلومات والأمن السيبراني في العصر الرقمي الحالي.

- تحليل التحديات والمعوقات التي تواجه الرقابة على نظم المعلومات والأمن السيبراني في العصر الرقمي.
- دراسة تحليلية لجهود الهيئات الرقابية العليا في تعزيز أمن المعلومات والبيانات.
- تقديم توصيات عملية لتحسين أداء الرقابة والتدقيق في مجال الأمن السيبراني.
- توضيح أهمية الالتزام بالمعايير الدولية وأفضل الممارسات في مجال الرقابة على نظم المعلومات والأمن السيبراني.
- دراسة حالة أو تحليل لنتائج تطبيق أدوات وتقنيات حديثة لتعزيز الرقابة والأمن السيبراني.

5. **فرضيات البحث :**

بناء على اشكالية وأهداف البحث يمكن صياغة مجموعة من الفرضيات على النحو التالي:

- **الفرضية الرئيسية:**
- تبني الهيئات الرقابية لأساليب وأدوات الرقابة على نظم المعلومات والأمن السيبراني يؤدي إلى المساهمة في تعزيز الأمن السيبراني.

- **الفرضيات الفرعية:**

- **الفرضية الفرعية الأولى:** إذا قامت الأجهزة العليا للرقابة المالية والمحاسبة بفهم وتطبيق المفاهيم الأساسية للرقابة على نظم المعلومات والأمن السيبراني، فإنها ستكون أكثر قدرة على مواجهة التحديات الحالية بفعالية.
- **الفرضية الفرعية الثانية:** إذا تبنت الأجهزة العليا للرقابة المالية والمحاسبة خطوات رئيسية ومنهجية عملية فعالة في تقييم نظم المعلومات والأمن السيبراني، فإن ذلك سيؤدي إلى تعزيز كفاءة عمليات التدقيق وتحقيق الأهداف الرقابية بكل فعالية ونجاعة.
- **الفرضية الفرعية الثالثة:** إذا عملت الأجهزة العليا للرقابة المالية والمحاسبة على تحسين الإجراءات والسياسات المتعلقة بتدقيق نظم المعلومات والأمن السيبراني، فإنها ستساهم في بناء نظام حكومي آمن وموثوق يتماشى مع المعايير الدولية ويعزز الأمن السيبراني الوطني.
- **الفرضية الفرعية الرابعة:** إذا تم تعزيز التنسيق والتعاون بين الهيئات الرقابية المختلفة، فإن ذلك سيعزز قدرتها على مكافحة التهديدات السيبرانية بشكل أكثر فعالية.

6. **منهجية الدراسة**

اعتمدت الدراسة على المنهج التحليلي الاستقرائي لتلائمه مع طبيعة البحث. يشمل البحث إطارًا نظريًا لتقييم نظم المعلومات وتقييم الأمن السيبراني، مع استعراض للتحديات التي تواجه الأجهزة

الرقابية في هذا المجال وأدوارها المحورية. كما تم تناول مفهوم الأمن السيبراني وحوكمة الأمن السيبراني، واستعراض جهود الجزائر في هذا المجال.

في الجانب التطبيقي، ركزت الدراسة على تقييم نظم معلومات وأمن شركة سونلغاز للتوزيع، حيث تم تحديد الأهداف والنطاق والمنهجية المعتمدة في العملية الرقابية، مع شرح خطوات بدءًا من مرحلة التخطيط والتحضير للعملية الرقابية، استخدام أسلوب التقييم المبني على المخاطر، جمع الأدلة، وتنفيذ التدقيق وتحديد النتائج. تمت مراجعة النتائج مع المنظمة المدققة، ووضع الملف الرقابي تحت تصرف الفريق الرقابي والغرفة المعنية بالعملية الرقابية.

7. تقسيمات الدراسة

بغرض تحقيق الهدف من الدراسة، وعلى ضوء ما سبق تم تقسيم الدراسة إلى الجانب النظري والجانب التطبيقي على النحو التالي:

8. الجانب النظري:

-الفصل الأول: الإطار العام والنظري لتقييم أنظمة المعلومات وتقييم الأمن السيبراني.

- المبحث الأول: الرقابة على نظم المعلومات.
- المبحث الثاني: الأمن السيبراني.
- المبحث الثالث: تدقيق الأمن السيبراني.

9. الجانب التطبيقي:

- الجانب العملي والتحليلي للهمة الرقابية تقييم نظم معلومات شركة سونلغاز للتوزيع وامنها السيبراني.

الفصل الأول: الإطار النظري لتقييم أنظمة المعلومات وتقييم الامن السيبراني من طرف الأجهزة العليا للرقابة المالية والمحاسبة

تمهيـد

في العصر الرقمي الحديث، تعتمد المنظمات بشكل متزايد على التكنولوجيا، مما يعرضها لمخاطر سيبرانية متزايدة. هذا الاعتماد يؤدي إلى عواقب وخيمة ماليًا ومعنويًا بسبب الثغرات الأمنية. الاتصالات والمعلومات الميسرة تزيد من هذه المخاطر، وتفوق القدرة على التحكم بها بالأساليب التقليدية. مفهوم الأمن السيبراني يتضمن تقنيات وممارسات لحماية الأصول المعلوماتية من الوصول غير المصرح به. مع تزايد الهجمات السيبرانية، أصبحت إدارة مخاطر الأمن السيبراني ضرورية لحماية البيانات واستقرار المنظمات.

يهدف هذا الفصل إلى توفير إطار نظري لفهم أهمية تقييم أنظمة المعلومات والأمن السيبراني من قبل الأجهزة العليا للرقابة المالية والمحاسبة. سيتم تناول مفاهيم الرقابة على نظم المعلومات وأهداف تدقيق تكنولوجيا المعلومات وأهميتها، بالإضافة إلى التحديات التي تواجه هذه الأجهزة في تعزيز الأمن المعلوماتي. سيتم تسليط الضوء على معايير حوكمة الأمن السيبراني وخطوات الوصول إلى النضج السيبراني، وجهود الجزائر في هذا المجال، وأهمية ومنهجية تدقيق الأمن السيبراني وكيفية تنفيذه بفعالية.

المبحث الأول: الرقابة على نظم المعلومات:

في ظل النمو الهائل في المشهد الرقمي، أصبحت دمج التقنيات المتقدمة في البنية التشغيلية للقطاع العام ضرورة استراتيجية لضمان التكيف مع البيئة السريعة التغير وشديدة التنافسية. هذا التحول الرقمي يضع المؤسسات الحكومية أمام تحديات جديدة تتعلق بأنظمة تكنولوجيا المعلومات المعقدة. ولضمان فعالية وكفاءة هذه الأنظمة، يجب إعادة النظر في الآليات التي تعزز من أدائها. تلعب الرقابة على نظم المعلومات دورًا حاسمًا في حماية البيانات الحساسة وضمان استمرارية العمليات الحكومية بفعالية، مما يساهم في تحقيق الشفافية والمساءلة وتحسين الأداء في القطاع العام.

I. المفاهيم الأساسية حول الرقابة على نظم المعلومات وأهميتها.

1. تعريف تدقيق ورقابة نظم المعلومات:

عمليات تدقيق تكنولوجيا المعلومات هي فحص لجوانب استخدام المنظمة لتكنولوجيا المعلومات، بما في ذلك البنية التحتية لتكنولوجيا المعلومات والسياسات والإجراءات والتطبيقات واستخدام البيانات. تتضمن عمليات تدقيق تكنولوجيا المعلومات بانتظام تحليل الأنظمة والضوابط للتأكد من أنها تلبي احتياجات أعمال المنظمة دون المساس بالأمن والخصوصية، التكلفة، وعناصر العمل الهامة الأخرى. غالبًا ما تتضمن عمليات تدقيق تكنولوجيا المعلومات أيضًا استخلاص تأكيدات بشأن ما إذا كانت إن تطوير وتنفيذ وصيانة

أنظمة تكنولوجيا المعلومات يلبي أهداف العمل والضمانات أصول المعلومات، ويحافظ على سلامة البيانات. غالبًا ما تتضمن عمليات تدقيق تكنولوجيا المعلومات تحديد حالات الانحراف عن المعايير، والتي تم تحديدها بدورها بناءً على نوع مهمة المراجعة (على سبيل المثال، الأداء أو التدقيق المالي أو الامتثال).[1]

يمكن تعريف الرقابة على تقنية المعلومات بأنها مجموعة من الإجراءات الرقابية المحددة التي تهدف إلى التأكد من صحة تشغيل البيانات والتقرير عنها، بحيث يمكن الاعتماد على هذه البيانات[2].

وقد عُرِّفَت أيضًا بأنها السياسات والإجراءات والممارسات والهياكل التنظيمية التي تصمم لتزويد تأكيد معقول بأن أهداف المنظمة سوف تتحقق وأن الأهداف غير المرغوب بها سوف تُمنع أو تُكشف ومن ثم تُصحح[3].

كما تعرف الرقابة على تقنية المعلومات بأنها طرق التأكد من أن البيانات الكاملة والصحيحة والمصادق عليها فقط أدخلت وحدثت في النظام الإلكتروني، وأن عملية المعالجة قد تمت بالطريقة الصحيحة وأن نتائج المعالجة متفقة مع ما هو متوقع، وأن البيانات قد تمت المصادقة عليها .[4]

وقد عُرِّفَت رقابة تقنية المعلومات أيضًا بأنها عملية جمع أدلة وتحليلها في بيئة تقنية المعلومات لكي يتم التوصل إلى استنتاج نهائي مقابل أهداف رقابة محددة سابقًا[5].

بالإضافة إلى ذلك، فقد عُرِّفَت بأنها عملية جمع أدلة وتحليلها في بيئة تقنية المعلومات لكي يتم التوصل إلى استنتاج نهائي مقابل أهداف رقابة محددة مسبقًا[6].

يُعرفه المراقب المالي والمراجع العام للهند (CAG) بأنه "عملية جمع وتقييم الأدلة لتحديد ما إذا كان نظام الكمبيوتر يحمي الأصول، ويحافظ على سلامة البيانات، ويسمح بتحقيق أهداف المنظمة بفعالية ويستخدم الموارد بكفاءة".

يشمل تدقيق تكنولوجيا المعلومات مجموعة واسعة من الأنواع المختلفة من التدقيقات مثل التدقيقات المالية (لتقييم صحة البيانات المالية للمنظمة)، والتدقيقات التشغيلية (لتقييم هيكل الرقابة الداخلية)، وتدقيق نظم المعلومات (بما في ذلك تدقيق الأداء)، والتدقيقات المتخصصة (لتقييم الخدمات المقدمة من طرف ثالث

[1] WGITA – IDI handbook on it audit for supreme audit institutions intosai development initiative, 2022 , P 07

[2] خضير، مصطفى .مراجعة المفاهيم والمعايير والإجراءات .جامعة الملك سعود، الرياض، 1991، ص 279.

[3] دهمش، نعيم وأبو زر، عفاف إسحق. الضوابط الرقابية والتدقيق الداخلي في بيئة تكنولوجيا المعلومات. المؤتمر العلمي الدولي السنوي الخامس لكلية الإدارة والاقتصاد والعلوم الإدارية، جامعة الزيتونة الأردنية، تحت شعار "اقتصاد المعرفة والتنمية الاقتصادية"، عمان، الأردن، 2005، ص 12.

[4] مصلح، ناصر عبد العزيز. أثر استخدام الحاسوب على أنظمة الرقابة الداخلية في المصارف العاملة في قطاع غزة. رسالة ماجستير، الجامعة الإسلامية، كلية التجارة، غزة، 2007، ص 71.

[5] الحميري، بشير، القوي، محمد، الشمري، عبد القادر. استخدام تقنية المعلومات والرقابة على البيانات باستخدام .COBITالجهاز المركزي للرقابة والمحاسبة، اليمن، 2011، ص 6.

[6] سعيد، هويدا النور. الرقابة على تقنية المعلومات. ديوان المراجعة القومي، السودان، 2011، ص 5.

مثل الاستعانة بمصادر خارجية، إلخ)، والتدقيقات الجنائية. ومع ذلك، فإن العنصر المشترك بين هذه التدقيقات هو تقديم تقييم حول مدى الثقة التي يمكن منحها لنظم تكنولوجيا المعلومات في المؤسسة المدققة. تشمل التدقيقات لأنظمة تكنولوجيا المعلومات أيضًا التدقيقات التي تعتمد على تكنولوجيا المعلومات (باستخدام أدوات تحليل البيانات بمساعدة الكمبيوتر)[7].

تعرفه المنظمة الافريقية للأجهزة العليا للرقابة المالية (الافروساي) على انه عملية الحصول على تأكيد ما إذا كان تطوير وتنفيذ ودعم وصيانة أنظمة المعلومات يلبي أهداف العمل، ويحمي أصول المعلومات ويحافظ على سلامة البيانات. بعبارة أخرى، التدقيق التقني هو فحص تنفيذ أنظمة تكنولوجيا المعلومات وضوابطها لضمان أن تلبي الأنظمة احتياجات العمل دون المساس بالأمان والخصوصية والتكلفة وعناصر العمل الحرجة الأخرى.[8]

وعليه، يمكن تلخيص تدقيق تكنولوجيا المعلومات على أنه عملية تقييم العمليات والمعلومات التقنية لمؤسسة ما للتحقق من أنها تستخدم بشكل فعال وآمن لتحقيق أهداف العمل. تشمل هذه العملية فحص تطوير وتنفيذ وصيانة أنظمة تكنولوجيا المعلومات، وضمان توافقها مع احتياجات العمل بدون المساس بالأمن والخصوصية والتكلفة وغيرها من عناصر العمل الأساسية.

II. أهمية تدقيق تكنولوجيا المعلومات

تعد سلامة وأمان بيئة تكنولوجيا المعلومات في المنظمة أمرًا ذا أولوية قصوى. تساعد عمليات تدقيق تكنولوجيا المعلومات في تحديد الثغرات ووضع استراتيجيات تصحيحية مناسبة. تضمن هذه العمليات الامتثال للمعايير واللوائح الصناعية، وتساهم في تجنب العقوبات والغرامات الناتجة عن عدم الامتثال[9].

. علاوة على ذلك، يمكن أن يكشف التدقيق الشامل لتكنولوجيا المعلومات عن الكفاءات في العمليات والأنظمة التكنولوجية، مما يؤدي إلى تحسين الأداء وتوفير التكاليف. بالنسبة للشركات المتداولة علنًا، يعد إجراء التدقيق أيضًا متطلبًا قانونيًا للحفاظ على الشفافية والثقة بين المستثمرين وأصحاب المصلحة الآخرين. بشكل عام، تعتبر عمليات تدقيق تكنولوجيا المعلومات ضرورية لضمان الامتثال، وتعزيز الأمان، وتحفيز التحسينات التشغيلية[10].

- **دور تدقيق تكنولوجيا المعلومات في الابتكار:** يساعد تدقيق تكنولوجيا المعلومات في دعم جهود الابتكار من خلال تقييم قدرة المنظمة على إدارة المخاطر المرتبطة بالابتكار. يمكن للمدققين تقييم

[7] https://cag.gov.in/
[8] AFROSAI-E INFORMATION TECHNOLOGY AUDIT GUIDELINE – 2017, P5
[9] https://www.auditboard.com/
[10] https://thecodest.co/blog/it-audits-and-cybersecurity/

متانة عمليات إدارة المشاريع وفعالية ممارسات إدارة التغيير، مما يدعم الابتكار مع إدارة المخاطر بشكل فعال. من خلال استغلال تقنيات تحليل البيانات والتشغيل التلقائي، يمكن لتدقيق تكنولوجيا المعلومات تعزيز كفاءته وفعاليته في تقييم الأنظمة والعمليات الرقمية[11].علاوة على ذلك، يمكن لتدقيق تكنولوجيا المعلومات تقديم رؤى قيمة للإدارة من خلال تحديد المجالات التي يمكن تحسينها وتحسينها في المبادرات الرقمية [12].علاوة على ذلك، يمكن لتدقيق تكنولوجيا المعلومات أن يلعب دورًا استباقيًا في دعم رحلات التحول الرقمي للمؤسسات من خلال تقديم خدمات استشارية وتوجيه استراتيجي [13].من خلال مواكبة التقنيات الناشئة واتجاهات الصناعة، يمكن لمدققي تكنولوجيا المعلومات مساعدة المؤسسات على الاستفادة من الفرص ومواجهة التحديات المرتبطة بالتحول الرقمي .[14]

- **تكامل تدقيق تكنولوجيا المعلومات مع التخطيط لاستمرارية الأعمال:** يلعب تدقيق تكنولوجيا المعلومات دورًا حيويًا في ضمان استمرارية الأعمال من خلال تقييم مرونة أنظمة تكنولوجيا المعلومات وضمان وجود عمليات النسخ الاحتياطي والاستعادة الكافية. ويتم ذلك عبر مراجعة نتائج التمارين المكتبية والمحاكاة لتحديد فعالية الخطة في سيناريوهات العالم الحقيقي والتركيز على نقاط الضعف والمجالات التي تحتاج إلى تحسين. يجمع المدققون ملاحظات من الموظفين وأصحاب المصلحة لفهم مدى فعالية وسهولة تنفيذ الخطة، وتحديد التحديات التي تواجههم. كما يقيمون مدى توافق الخطة مع أهداف التعافي الخاصة بالمؤسسة، ويتحققون من تغطية الخطة للعمليات والنظم والموارد الأساسية بشكل كاف. إضافة إلى ذلك، يضمن المدققون مواءمة الخطة مع المتطلبات التجارية المتغيرة من خلال تحديثها لتظل فعالة في ضوء التغيرات في التكنولوجيا والعمليات واستراتيجيات العمل[15].

أيضًا، يعتبر تدقيق تكنولوجيا المعلومات أمرًا أساسيًا لتخطيط استمرارية الأعمال بالنسبة للشركات الناشئة في مجال الحوسبة السحابية. حيث يساهم هذا التدقيق في ضمان مرونة واستدامة هذه الشركات، من خلال تطوير واختبار خطط فعالة تساهم في تقليل تأثير الأحداث المدمرة على الوظائف الحيوية للأعمال والبنية التحتية لتكنولوجيا المعلومات. كما تساهم هذه الخطط في الحفاظ

[11] Deloitte A. 2021. IT audit in the era of digital transformation: How to adapt and thrive. Deloitte Insights.
[12] PwC. 2018. Digital transformation. PwC.
[13] EY, Ajak. 2020. Navigating the risk and regulatory landscape: Technology and digital transformation. EY Insights.
[14] Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. MIS Quarterly, 34(3), 487-502.
[15] https://audit.guru/disaster-recovery-and-business-continuity-in-it-audits/#:~

على ثقة العملاء والامتثال للمعايير والتشريعات، مما يسهم في تعزيز القدرة التنافسية العامة للأعمال.[16]

- **أهمية تدقيق تكنولوجيا المعلومات في عمليات الدمج والاستحواذ:** تدقيق تكنولوجيا المعلومات ضروري في عمليات الدمج والاستحواذ. يتضمن الدمج والاستحواذ (M&A) دمج شركتين أو أكثر، مع نقل المعلومات والأصول الحساسة غالبًا. يقوم تدقيق الأمان السيبراني بتقييم المخاطر والضعف في الأمان السيبراني للشركة أو الاستثمار المُقتَنى كجزء من صفقة .M&A تحتاج الشركات إلى إجراء تدقيق أمان سيبراني لعدة أسباب: حماية ضد الخسائر المالية، الامتثال بالتشريعات، حماية المعلومات الحساسة، تحسين موقف الأمان العام، والحفاظ على ثقة العملاء وتجنب الضرر السمعي. تنفيذ تدقيق الأمان السيبراني يتضمن تطوير قائمة تدقيق ومراجعة سياسات وإجراءات الأمان، تقييم خطة الاستجابة للحوادث، ومراجعة تقنيات الأمان وبنية الشبكة. من خلال هذه الخطوات، يمكن للشركات تحسين موقفها الأمني وتقليل الاحتمالات المحتملة للهجمات السيبرانية[17].
- **تمكين حوكمة تكنولوجيا المعلومات من خلال التدقيق:** تمكين حوكمة تكنولوجيا المعلومات من خلال التدقيق يشير إلى العملية التي تهدف إلى تعزيز وتحسين كفاءة وفعالية حوكمة تكنولوجيا المعلومات داخل المؤسسات. يعتمد هذا على إجراء تقييم شامل لممارسات وسياسات وإجراءات حوكمة تكنولوجيا المعلومات الحالية للتأكد من تناسقها مع أهداف المؤسسة ومعايير الأمان الدولية والمحلية. يتضمن ذلك أيضًا تقييم مدى فعالية وكفاءة استخدام التكنولوجيا في دعم أهداف الأعمال وتحقيق التوافق مع اللوائح والقوانين ذات الصلة. تمكين حوكمة تكنولوجيا المعلومات من خلال التدقيق يعتبر عملية حيوية لتحقيق أهداف الأمان والامتثال والاستدامة التنافسية للمؤسسة في عصر تكنولوجيا المعلومات المتقدمة[18].
- **تحقيق خصوصية البيانات و حمايتها من خلال تدقيق تكنولوجيا المعلومات :** تعد حماية البيانات أحد أولويات الشركات، ويقوم تدقيق تكنولوجيا المعلومات بتقييم فعالية تدابير حماية البيانات والامتثال للتشريعات مثل GDPR ، مما يساهم في تعزيز ثقافة الوعي بالبيانات في المؤسسة . حيث إن خصوصية البيانات وأمن المعلومات يعتبران من بين القضايا الأكثر إلحاحًا بالنسبة للشركات. إذ يمثل ضمان حماية البيانات وتأمينها بأساليب فعالة واقتصادية تحديًا مستمرًا نظرًا

[16] Sathyanarayanan, Kishan. "Disaster Recovery and Business Continuity Preparedness for Cloud-based Start-ups." ISACA Now Blog, 2023

[17] https://atlantsecurity.com/cybersecurity-audits-are-necessary-in-the-due-diligence-of-ma-deals/

[18] Auditing IT Governance – Pempal www.pempal.org

لتعقيد تهديدات الأمن السيبراني المتزايدة وكمية التشريعات الخاصة بحماية البيانات. ومن ثم، فإن المؤسسات تتعرض باستمرار للضغوط من أجل ضمان أمان أنظمتها تكنولوجية وخصوصية بيانات عملائها. ويُعد التدقيق في تكنولوجيا المعلومات أحد أكثر الطرق فعالية لتحقيق هذه الأهداف. إذ يمكن للتدقيق في تكنولوجيا المعلومات مساعدة أي مؤسسة في تقييم فعالية ضوابطها وتحديد المجالات المحتملة للمخاطر والضعف .ويخدم التدقيق في تكنولوجيا المعلومات أغراضًا متعددة، منها[19]:

- مساعدة المنظمات في تحديد أي ثغرات في أنظمتها أو عملياتها.
- المساعدة في تقييم الامتثال بالتشريعات والمعايير ذات الصلة.
- تقديم أساس لتقديم التوصيات وخطط التصحيح للتحسين.

- **تقييم أمان السحابة من خلال تدقيق تكنولوجيا المعلومات:** مع تزايد الاعتماد على الحوسبة السحابية، ينبغي للتدقيق أن يتبنى نهجًا استباقيًا تجاه مبادرات السحابة ويمكنه من تحقيق ذلك بتوجيه الإدارة كمستشار موثوق به. يجب على التدقيق أيضًا المشاركة في عمليات الشراء المبكرة لتأكيد حالات استخدام الأعمال، وضمان تضمين بنود الحق في التدقيق في العقود، وتقديم رؤى موضوعية. كما يمكن للتدقيق مساعدة المؤسسات في اكتشاف وتقليل المخاطر، وتقديم إرشادات بشأن تأثير التشريعات على أمان البيانات في السحابة. ويمكن أيضًا تقديم خدمات ضمان أخرى، مثل تدقيق هجرة البيانات، وتدقيق تنفيذ النظام، واختبار التحكم، واستعراض تقارير مراقبة تنظيم الخدمة (SOC). ولتسهيل تدقيق السحابة، يمكن استخدام الأدوات المتاحة مثل مصفوعة ضوابط تحالف أمان السحابة، واستبيان مبادرة تقييم الاتفاق (CAIQ) ، أو حلول برمجيات الامتثال للمساعدة في حساب الضوابط الضرورية للتخفيف من المخاطر. من خلال ذلك، يمكن للمؤسسة التركيز على بيئة التحكم بشكل استباقي بدلاً من رد الفعلي.[20]
- **تأثير تدقيق تكنولوجيا المعلومات على مبادرات التحول الرقمي :** يوفر تدقيق تكنولوجيا المعلومات رؤى قيمة حول إدارة مبادرات التحول الرقمي، مما يساعد في تقييم استراتيجيات التحول، قدرات إدارة المشاريع، وممارسات إدارة التغيير.

[19] https://www.isaca.org/resources/news-and-trends/industry-news/2023/managing-data-privacy-and-information-security-with-it-audits

[20] Kim Pham, CIA, Market Advisor ,Cloud Computing — What IT Auditors Should Really Know, ISACA Now Blog ,2022- https://www.isaca.org

- **تدقيق تكنولوجيا المعلومات في سياق إنترنت الأشياء (IoT)** : يعتبر تدقيق تكنولوجيا المعلومات في سياق إنترنت الأشياء امراً جوهريًا في عصرنا الحالي نظرًا للتطورات الرقمية السريعة. يقدم هذا التدقيق تقييمًا موضوعيًا ومستقلاً لأنظمة وضوابط المؤسسات التكنولوجية، مما يساعدها في تحديد الثغرات الأمنية وتقييم الضوابط المعتمدة وضمان الامتثال للتشريعات والمعايير القائمة. بالإضافة إلى ذلك، يساعد تدقيق تكنولوجيا المعلومات في إثبات القيمة المضافة لحلول إنترنت الأشياء من خلال التحقق من جاهزية وفعالية الأنظمة والبرامج المستخدمة. يلعب تدقيق تكنولوجيا المعلومات دورًا حيويًا في ضمان سلامة وأمان البيانات في بيئة إنترنت الأشياء، حيث يقيم أمان البيانات المنقولة بين الأجهزة المتصلة، ويحدد المخاطر المحتملة والضعف في النظام، ويوفر التوجيهات لتعزيز الضوابط الأمنية. من الضروري أن يتبنى مدققو تكنولوجيا المعلومات نهجًا استباقيًا ودقيقًا في تقييم أمان إنترنت الأشياء، وهو ما يتطلب فهمًا عميقًا لتكنولوجيا إنترنت الأشياء والتحديات التي تواجهها[21].
- **تخطيط استجابة الحوادث السيبرانية من خلال تدقيق تكنولوجيا المعلومات:** يقيّم تدقيق تكنولوجيا المعلومات جاهزية المنظمة للتعامل مع الحوادث السيبرانية، بما في ذلك تصميم وفعالية خطة الاستجابة للحوادث.

في عصر يتزايد فيه تعقيد وانتشار التهديدات السيبرانية، لم يكن تدقيق تكنولوجيا المعلومات أكثر أهمية من أي وقت مضى. تعتبر هذه التدقيقات أدوات أساسية لحماية بيئة تكنولوجيا المعلومات في المنظمة، وضمان الامتثال التنظيمي، وتخفيف مخاطر الهجمات السيبرانية. يلعب تدقيق تكنولوجيا المعلومات دورًا حيويًا في تقييم جاهزية المؤسسات للتعامل مع التحديات السيبرانية وإدارة الموردين وضمان تطوير البرمجيات بمعايير عالية وتأثيره على إدارة خدمات تكنولوجيا المعلومات وكذلك في تقييم وتأمين تقنيات الذكاء الاصطناعي. تعتبر هذه التدقيقات أدوات أساسية لحماية بيئة تكنولوجيا المعلومات وضمان الامتثال التنظيمي وتخفيف مخاطر الهجمات السيبرانية.

2. أهداف تدقيق تكنولوجيا المعلومات

ساهم ظهور تقنية المعلومات في تغيير الطريقة التي نعمل بها جميعنا في العديد من المجالات، ويتضح هذا التغيير في مهنة التدقيق دون استثناء. فقد أصبح الحاسوب مستخدما في كل مكان تقريبان حيث انه وبلا شك أحد أكثر أدوات العمل فعالية، إلا أن ذلك صاحبه ظهور نقاط ضعف ذات عالقة وثيقة ببيئة

[21] https://audit.guru/it-audit-implications-of-the-internet-of-things-iot

الأعمال الآلية. حيث يجب أن يتم تحديد كل نقطة من نقاط الضعف الجديدة وتقليل أثرها والتحكم بها من خلال تقييم مدى دقة كل العمليات الرقابية باستخدام أساليب تدقيق جديدة.[22]

الهدف من تدقيق تكنولوجيا المعلومات هو ضمان أن تمكن موارد تكنولوجيا المعلومات المؤسسة من تحقيق أهدافها بفعالية واستخدام الموارد بكفاءة. يمكن أن يشمل التدقيق تطبيقات تكنولوجيا المعلومات، والعمليات، والحوكمة، وأنظمة تخطيط موارد المؤسسة، وأمن نظم المعلومات، واستحواذ الحلول الأعمال، وتطوير الأنظمة، واستمرارية الأعمال – كلها مجالات محددة من تنفيذ أنظمة المعلومات، أو يمكن أن يكون هدفها النظر إلى القيمة المضافة التي قدمتها أنظمة المعلومات[23].

بعض أمثلة أهداف التدقيق هي:

- مراجعة ضوابط أنظمة تكنولوجيا المعلومات للتأكد من كفايتها وفعاليتها.
- تقييم العمليات المتضمنة في عمليات منطقة معينة مثل نظام الرواتب، أو نظام المحاسبة المالية.
- تقييم أداء النظام وأمانه، على سبيل المثال، نظام حجز السكك الحديدية.
- فحص عملية تطوير النظام والإجراءات.

–يمكن أن يشمل التقييم فحص العمليات المتعلقة بعمليات محددة مثل نظام الرواتب أو نظام المحاسبة المالية.

تشمل أهداف تدقيق تكنولوجيا المعلومات حسب المراقب المالي والمراجع العام للهند (CAG) تقييم العمليات التي تضمن حماية الأصول. وتشمل هذه الأصول البيانات (جميع أنواع البيانات، سواء كانت خارجية أو داخلية، منظمة أو غير منظمة، مثل الرسومات والصوت وتوثيق النظام)، نظم التطبيقات (مجموعة من الإجراءات اليدوية والمبرمجة)، التكنولوجيا (الأجهزة وأنظمة التشغيل ونظم إدارة قواعد البيانات والشبكات والوسائط المتعددة)، المرافق (الموارد اللازمة لاستضافة ودعم نظم المعلومات مثل الإمدادات)، والأشخاص (مهارات الموظفين والوعي والإنتاجية في تخطيط وتنظيم واكتساب وتسليم ودعم ومراقبة نظم وخدمات المعلومات) .كما تشمل الأهداف الحفاظ على سمات البيانات السبعة[24]:

- **الفعالية:** تتعلق بكون المعلومات ذات صلة وعلاقة بالعملية التجارية وكذلك تسليمها في الوقت المناسب، بدقة، وبشكل متسق وقابل للاستخدام. تتعلق فعالية النظام بتقييم ما إذا كان نظام تكنولوجيا المعلومات يحقق الأهداف العامة للإدارة العليا والمستخدمين.

[22] دليل تدقيق تكنولوجيا المعلومات، المجلد الأولى، المراقب المالي والمراجع العام للهند (CAG)

[23] AFROSAI-E INFORMATION TECHNOLOGY AUDIT GUIDELINE – 2017, P5

[24] https://cag.gov.in/

- **الكفاءة:** تتعلق بتوفير المعلومات من خلال الاستخدام الأمثل (الأكثر إنتاجية واقتصادية) للموارد. تتعلق كفاءة النظام بكيفية استخدام الأنظمة الموارد بشكل أمثل لتحقيق الأهداف المطلوبة.
- **السرية:** تتعلق بحماية المعلومات الحساسة من الكشف غير المصرح به.
- **النزاهة:** تتعلق بدقة واكتمال المعلومات وكذلك صلاحيتها وفقًا لمجموعة القيم والتوقعات الخاصة بالأعمال.
- **التوافر:** تتعلق بتوافر المعلومات عند الحاجة إليها من قبل العملية التجارية، ومن ثم تتعلق بحماية الموارد.
- **الامتثال:** تتعلق بالامتثال للقوانين واللوائح والترتيبات التعاقدية التي تخضع لها العملية التجارية؛ أي المعايير التجارية المفروضة خارجيًا. هذا يعني أساسًا أن الأنظمة تحتاج إلى العمل ضمن نطاق القواعد واللوائح والشروط الخاصة بالمنظمة.
- **موثوقية المعلومات:** تتعلق بتقديم الأنظمة للإدارة معلومات مناسبة لاستخدامها في تشغيل الكيان، وتقديم التقارير المالية لمستخدمي المعلومات المالية، وتقديم التقارير للهيئات التنظيمية بشأن الامتثال للقوانين واللوائح.

لذا، تدقيق تكنولوجيا المعلومات يتعلق بفحص ما إذا كانت عمليات تكنولوجيا المعلومات وموارد تكنولوجيا المعلومات تتحد معًا لتحقيق الأهداف المقصودة للمنظمة لضمان الفعالية، والكفاءة، والاقتصاد في عملياتها مع الامتثال للقواعد السارية.

III. تحديات وأدوار للأجهزة العليا للرقابة المالية العامة والمحاسبة في مجال الرقابة على نظم المعلومات.

تشير الأجهزة العليا للرقابة المالية العامة والمحاسبة (SAIs) إلى الهيئات الوطنية المسؤولة عن ضمان المساءلة في عمل الحكومات من خلال التدقيق الخارجي. تختلف ولايات ومسؤوليات وتنظيم هذه المؤسسات حسب نظم الحوكمة والسياسات الوطنية، مع التأكيد على أهمية استقلالية SAIs عن الدولة وجهازها التنفيذي لضمان الشفافية والنزاهة[25].

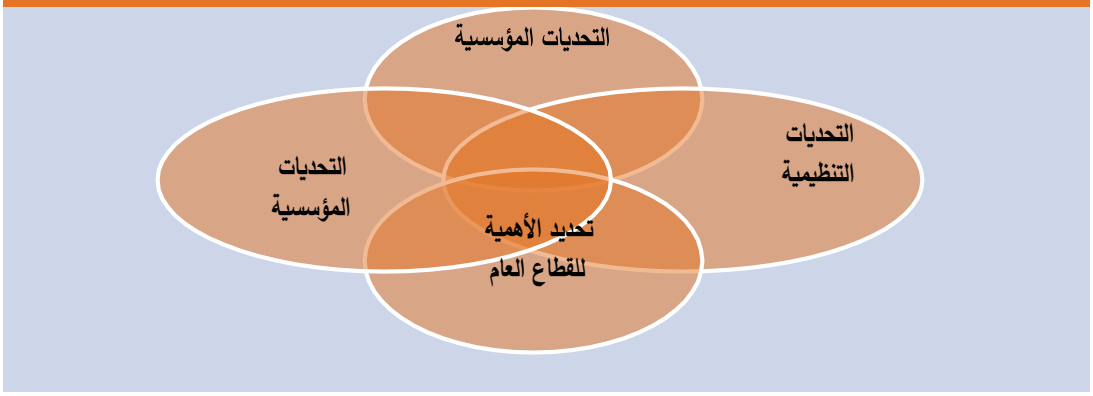
[25] Chatterjee, S. (2018). "Addressing the Challenges of IT Audits by Supreme Audit Institutions." ISACA Journal, Volume 4.

وتعرفها المنظمة العربية للأجهزة العليا للرقابة المالية والمحاسبة، ، على أنها "هيئة مستقلة تقوم بكافة أنواع الرقابة بموجب التشريعات النافذة، بهدف التحقق من الحفاظ على المال العام وضمان كفاءة وحسن استخدامه، وتقديم تقرير بشأن الحسابات والبيانات المالية إلى الجهات المعنية بالدولة [26].

1. التحديات في تدقيق تكنولوجيا المعلومات من قبل الأجهزة العليا للرقابة المالية:

كما هو موضح في الشكل 1، يمكن تصنيف التحديات في إجراء تدقيق تكنولوجيا المعلومات من قبل الأجهزة العليا للرقابة المالية إلى أربع فئات من التحديات، كما يلي[27]:

الشكل 01 - التحديات في تدقيق تكنولوجيا المعلومات من قبل الأجهزة العليا للرقابة المالية



- التحديات المؤسسية: تتعلق بغياب التفويض الكافي أو التشريعات التي تمكن الجهاز من إجراء تدقيقات تكنولوجيا المعلومات.
- **التحديات التنظيمية:** تتعلق بالأنظمة والهياكل داخل الجهاز التي تمكن تدقيق تكنولوجيا المعلومات.
- **تحديات الموظفين المهنيين:** تتعلق بتوافر الموظفين المدربين وذوي المهارات الكافية لإجراء تدقيقات تكنولوجيا المعلومات.
- **تحديد الأهمية للقطاع العام:** هذا أمر ضروري للأجهزة العليا للرقابة المالية نظرًا لزيادة الحوسبة في الإدارة وتقديم الخدمات من قبل القطاع العام.

[26] ابراهيم جبل، أدوات الرقابة المتاحة للأجهزة العليا للرقابة المالية والمحاسبة وسبل تطويرها، القاهرة: دار النهضة العربية،2015، ص86.
[27] Chatterjee, S. (2018). "Addressing the Challenges of IT Audits by Supreme Audit Institutions." ISACA Journal, Volume 4.

2. دور الأجهزة العليا للرقابة المالية العامة والمحاسبة في تعزيز الرقابة على نظم المعلومات

تلعب الأجهزة العليا للرقابة المالية العامة والمحاسبة دورًا حيويًا في تعزيز الرقابة على نظم المعلومات. على مر السنين، بذل المجتمع الدولي للأجهزة العليا للرقابة المالية جهودًا كبيرة لإنشاء وظائف تدقيق تكنولوجيا المعلومات قوية، وذلك من خلال معالجة التحديات المختلفة. مع التقدم التكنولوجي والتحول الرقمي في المؤسسات الحكومية، أصبحت الحاجة إلى رقابة فعالة على نظم المعلومات ضرورة لضمان الشفافية، الكفاءة، والأمن السيبراني. تقوم SAIs بدور رئيسي من خلال عدة جوانب:

تفويضات SAIs لإجراء تدقيقات تكنولوجيا المعلومات

إن التفويض الممنوح لجهاز الرقابة الأعلى لإجراء تدقيق لنظم تكنولوجيا المعلومات موجود ضمن المعايير الدولية للأجهزة العليا للرقابة المالية (ISSAIs) في إعلان ليما.[28] التفويض الممنوح للأجهزة العليا الرقابية لتدقيق تكنولوجيا المعلومات يستمد من التفويض العام الممنوح لجهاز الرقابة الأعلى للقيام بالتدقيق المالي، وتدقيق الالتزام، وتدقيق الأداء أو المزج بينهم[29]. حيث تستمد هذه الاجهزة صلاحيات التدقيق من دساتير بلدانها، والتي تُنَفَّذ من خلال التشريعات ذات الصلة

قد يكون لبعض الأجهزة العليا للرقابة المالية تفويضات محددة للقيام بتدقيق تكنولوجيا المعلومات. على سبيل المثال، في حال حصول جهاز الرقابة الأعلى على تفويض بالتدقيق على عملية الإيرادات الضريبية، يجب عليه تدقيق الجزء الآلي من هذه العملية بناء على تفويض يستمد من التفويض الأصلي. هذا التفويض يضمن شمولية وفعالية التدقيقات المالية والتكنولوجية، مما يعزز الشفافية والمساءلة في العمليات الحكومية المختلفة.[30]

- **دعم الأقران وتبادل المعرفة بين الأجهزة العليا للرقابة المالية**

من خلال جهود المنظمة الدولية للأجهزة العليا للرقابة المالية العامة (INTOSAI) ومجموعة العمل على تدقيق تكنولوجيا المعلومات (WGITA) والمبادرة الدولية لتطوير الأجهزة العليا للرقابة المالية(IDI) ، تطورت قدرة تدقيق تكنولوجيا المعلومات بشكل كبير خلال العقود الماضية. تم إنشاء WGITA في برلين عام 1989 لمعالجة اهتمامات الأجهزة العليا للرقابة المالية في مجال تدقيق تكنولوجيا المعلومات.[31]

[28] INTOSAI Lima Declaration, Part VII Section 22

[29] ISSAI 100 Fundamental Principles of Public Sector Auditing

[30] Chatterjee, S. (2018). "Addressing the Challenges of IT Audits by Supreme Audit Institutions." ISACA Journal, Volume 4.

[31] نفس المرجع السابق.

حاليًا، تضم المجموعة 59 دولة عضو وتشارك في وضع أجندة تدقيق تكنولوجيا المعلومات للأجهزة العليا للرقابة المالية. على مر السنين، دعمت WGITA جهود الأجهزة العليا للرقابة المالية في بناء صلاحياتها ومحفظتها في تدقيق تكنولوجيا المعلومات، ونشرت عدة أدلة في هذا المجال مثل "الدليل WGITA–IDI لتدقيق تكنولوجيا المعلومات للأجهزة العليا الرقابية" بعدة لغات.

- **إضافة الأدوار الإقليمية**

إلى جانب الجهود المبذولة من طرف منظمة الانتوساي، قامت المنظمة العربية للأجهزة العليا للرقابة المالية والمحاسبة (ARABOSAI) والمنظمة الأوروبية للأجهزة العليا للرقابة المالية (EUROSAI) بإنشاء لجان وأفواج متخصصة لتعزيز الرقابة على نظم المعلومات. تهدف هذه المبادرات الإقليمية إلى تحسين كفاءة وفعالية التدقيق على تكنولوجيا المعلومات عبر تبادل المعرفة وأفضل الممارسات بين الدول الأعضاء. من خلال هذه الجهود المشتركة، تسعى المنظمات الإقليمية إلى دعم التطوير المهني للأجهزة الرقابية وضمان تطبيق معايير عالية في تدقيق نظم المعلومات.

- **الجودة والمعايير في تدقيق تكنولوجيا المعلومات**

تطورت تدقيقات تكنولوجيا المعلومات كمسار عمل للأجهزة العليا للرقابة خلال فترة كانت فيها الأجهزة تعمل بنشاط على تطوير وتنفيذ معايير التدقيق في القطاع العام. قامت الانتوساي بتطوير المعايير الدولية للأجهزة العليا للرقابة المالية(ISSAIs) ، بهدف وضع معايير دولية لتدقيق القطاع العام. أحد هذه المعايير هو ISSAI 5310الذي تم تطويره خصيصًا لمراجعة منهجية أمن نظم المعلومات. إرشادات التدقيق التي تترجم المبادئ الأساسية إلى إرشادات تشغيلية محددة مثل اساي 5310 و الدليل المنهجي 5100 توفر الإطار العام لإجراء تدقيق نظم المعلومات ضمن الإطار الدولي للممارسات المهنية (IFPP) [32].

- **دعم تطوير القدرات للأجهزة العليا للرقابة المالية**

حيث انه خلال الفترة 2013 و2016، تم تنفيذ برنامج تعاوني بين مبادرة تطوير الأجهزة العليا للرقابة المالية (IDI) و مجموعة العمل على تدقيق تكنولوجيا المعلومات (WGITA) لدعم الأجهزة العليا للرقابة المالية (SAIs) في تحسين قدراتها وأدائها في تدقيق تكنولوجيا المعلومات. جاء هذا البرنامج استجابة للتحديات المتزايدة التي تواجه الأجهزة العليا للرقابة المالية في بيئات النظم المعلوماتية المحوسبة، مما جعل

[32] المنظمة الدولية للأجهزة العليا للرقابة المالية والمحاسبة ((INTOSAI، مبادرة تطوير INTOSAI، ملحق لتقرير الأداء والمساءلة لعام 2015، [IDI Report](http://www.idi.no/en/about-idi/reports).

من الضروري بناء القدرات في مجال تدقيق تكنولوجيا المعلومات لتقديم توصيات تتماشى مع معايير وممارسات الانتوساي.[33]

- **التدريب والتطوير المهني**

نظمت الهيئات العليا للرقابة تدريبات لموظفيها الذين يقومون بتدقيق تكنولوجيا المعلومات. غطت هذه الدورات التدريبية مختلف جوانب تدقيق تكنولوجيا المعلومات وشارك فيها خبراء من وكالات مهنية ونظراء. بالإضافة إلى ذلك، شجعت هاته الهيئات موظفيها على الحصول على شهادات معترف بها مهنيًا مثل مدقق نظم المعلومات المعتمد (®CISA) ،و مدير أمن المعلومات المعتمد (®CISM) ، كما قامت بتقديم التدريب لهذه الشهادات وكذلك تعويض التكاليف المترتبة عليها. ساعد ذلك على تطوير مجموعة من المحترفين المدربين والمشهود لهم في تدقيق تكنولوجيا المعلومات.[34]

- **الأدوات والتقنيات المتقدمة**

استخدمت الهيئات العليا للرقابة برامج تدقيق مثل لغة أوامر التدقيق (ACL) وتحليل البيانات التفاعلي (IDEA)وتحليلات TeamMate كما طورت مجموعة العمل الأوروبية لتكنولوجيا المعلومات (EUROSAI)أداة تدقيق متخصصة تسمى CUBE لتسهيل تدقيق الحكومة الإلكترونية.

- **استخدام منصة تحليلات البيانات الكبيرة**

تعتبر الأجهزة العليا للرقابة المالية العامة والمحاسبة (SAIs) عنصراً حيوياً في تعزيز الرقابة على نظم المعلومات باستخدام منصات تحليلات البيانات الكبيرة. يعتمد هذا الدور على استخدام مجموعة متنوعة من البرامج المتقدمة، سواء كانت مفتوحة المصدر أو ملكية، لإجراء تحليلات دقيقة على كميات ضخمة من البيانات.

حيث تشير الدراسات إلى استخدام الأجهزة العليا للرقابة المالية العامة والمحاسبة لمزيج من البرامج مفتوحة المصدر والبرامج الملكية، مع تفضيل برامج مثل IDEA ، R و ACL لتحليلات البيانات. معظم الأجهزة العليا لا تزال تعتمد على برامج التدقيق العامة (GAS) مثل IDEA وACL، مما يعكس تركيزها على البيانات المنظمة واستخدام تقنيات التدقيق بمساعدة الحاسوب(CAATs) .

على الرغم من ذلك، بدأت بعض الأجهزة في تبني لغات برمجة مخصصة للتحليلات مثل R و Python . هذا التحول يعكس وعي الأجهزة العليا بأهمية التحليلات المتقدمة لتحقيق الرقابة الفعالة.

- **استخدام منصة تحليلات البيانات الكبيرة**

[33] نفس المرجع السابق .

[34]

في إطار تعزيز الرقابة على نظم المعلومات، تعتمد الأجهزة العليا للرقابة المالية العامة والمحاسبة على منصات تحليلات البيانات الكبيرة. تستخدم هذه الأجهزة مجموعة من البرامج المتقدمة، سواء كانت مفتوحة المصدر أو ملكية، لتحليل كميات كبيرة من البيانات. تشير الدراسات إلى أن هذه الأجهزة تستخدم مزيجًا من البرامج مثل IDEA و R و ACL لتحليلات البيانات مما يعكس تركيزها على البيانات المنظمة واستخدام تقنيات التدقيق بمساعدة الحاسوب(CAATs) . بينما تعتمد معظم الأجهزة على برامج التدقيق العامة (GAS)مثل IDEA وACL، بدأ بعضها في تبني لغات برمجة مخصصة للتحليلات مثل R و .Python يعكس هذا التحول وعي الأجهزة بأهمية التحليلات المتقدمة لتحقيق رقابة فعالة.[35]

- **طريقة جمع البيانات**

تمتلك معظم الأجهزة العليا للرقابة المالية العامة والمحاسبة (SAIs) السلطة القانونية لجمع البيانات من الجهة الخاضعة للتدقيق. ومع ذلك، فإن إجراءات جمع البيانات ليست محددة بشكل واضح في اللوائح. لكن هناك بعض الأجهزة التي ينص قانون التدقيق لديها بوضوح على أن الجهة الخاضعة للتدقيق يجب أن تقدم بيانات المعاملات المالية الحكومية إلكترونيًا. حيث تشير الدراسات إلى أن 21% فقط من الأجهزة تستخدم الإنترنت كوسيلة لنقل البيانات عن بُعد من الجهة الخاضعة للتدقيق، بينما يجمع الباقون البيانات باستخدام طرق تقليدية مثل الجمع اليدوي (25%)، الوصول للقراءة فقط في موقع الجهة الخاضعة للتدقيق (21%)، واستخدام وسائط التخزين القابلة للإزالة(21%) .[36]

- **مؤشرات الأداء والمقارنة المعيارية**

إطار قياس الأداء للأجهزة العليا للرقابة المالية (SAI PMF) هو إطار دولي لتقييم أداء الأجهزة العليا وفقًا لمعايير ISSAIs وأفضل الممارسات الدولية، مما يوفر تقييمًا شاملاً ومبنيًا على الأدلة لأداء الجهاز، بما في ذلك وظيفة التدقيق. أداة التقييم الذاتي لتدقيق تكنولوجيا المعلومات(ITASA) هي أداة جودة للتدقيق تتخذ شكل ورشة عمل بمشاركة من مختلف المستويات. يقود ITASA مشرف من جهاز رقابة آخر[37].

تلعب الأجهزة العليا للرقابة المالية العامة والمحاسبة دورًا محوريًا في تعزيز الرقابة على نظم المعلومات في ظل التطورات التكنولوجية المتسارعة والتحول الرقمي. من خلال اقتراح وتطوير التشريعات، إنشاء وحدات

[35] INTOSAI Working Group on Big Data (WGBD) , audit technology , research paper on innovative, September 2022

[36] نفس المرجع السابق.

[37] Chatterjee, S. (2018). Previously cited..

متخصصة، تدريب الكوادر، وتبني أفضل الممارسات والمعايير الدولية، تسهم هذه الأجهزة في ضمان الشفافية، الكفاءة، والأمن السيبراني. تعزيز التعاون بين الجهات المعنية وتطوير أدوات وتقنيات التدقيق يعزز من قدرة الأجهزة الرقابية على تنفيذ مهامها بفعالية، مما يساهم في حماية البيانات وضمان استمرارية العمليات الحكومية بشكل سلس وموثوق.

المبحث الثاني : الأمن السيبراني

في عصر التكنولوجيا الحديث، أصبح الأمن السيبراني أمرًا لا غنى عنه. يعد الحماية من التهديدات السيبرانية أمرًا حيويًا للحفاظ على سلامة الأنظمة والبيانات. تواجه الجزائر، مثل العديد من الدول، تحديات في مجال الأمن السيبراني. سنستعرض في هذا الفصل الإطار المفاهيمي للأمن السيبراني، وجهود الجزائر في هذا المجال، بهدف تعزيز القدرات التقنية وضمان الحماية الفعالة للبيانات والمعلومات الحساسة.

I. الإطار مفاهيمي للأمن السيبراني

1. ماذا يعني الامن السيبراني

وقد دفعت ثورة المعلومات والتكنولوجيا، إلى حدوث تحول في مفهوم القوة باتجاهها نحو الفضاء الإلكتروني أو الفضاء السيبراني، مع ظهور الإنترنت ومواقع الويب. حيث أصبح الفضاء السيبراني أحد أهم المساحات التي يتحرك بداخلها الفاعلون في النظام الدولي وفي مقدمتهم الدول. ما أثر بالضرورة على قدرات الدول على استخدام الأشكال المختلفة للقوة سواء كانت صلبة أو ناعمة[38] .ولأن الدول باتت تستخدم الفضاء السيبراني لاعتبارات الأمن والقوة العسكرية، فقد ضمت العديد منها الفضاء السيبراني ضمن أمنها القومي[39].

يعتبر الأمن السيبراني مصطلحًا جديدًا نسبيًّا لمجموعة من الممارسات القديمة حول أمان شبكات الكمبيوتر. إلا أنه يتَّسم بوجود تعارض في تعريفاته، ويتجلَّى ذلك في رفض بعض الجهات الحكومية في عدد من الدول الاتفاق على مفردات مشتركة. كما يتغيَّر معنى المصطلح عبر الزمن. في الوقت الحاضر، تتعامل الدوائر الحكومية العليا في الولايات المتحدة وعدد من الدول مع الأمن السيبراني باعتباره تحديًا رئيسيًّا للأمن القومي. ويرى عدد من الباحثين أن عدم وجود تعريف موجز ومقبول على نطاق واسع يلتقط الأبعاد المتعددة للأمن السيبراني، من المحتمل أن يؤدي إلى إعاقة التقدم التكنولوجي والعلمي، حيث يتم تعزيز النظرة التقنية

[38] إيهاب خليفة، القوة الإلكترونية وأبعاد التحول في مفهوم القوة، أوراق، 12، 2014، ص 20.
[39] المرجع السابق، ص 22.

السائدة للأمن السيبراني مع فصل التخصصات التي يجب أن تعمل بشكل متضافر لحل تحديات الأمن السيبراني المعقدة[40].

❖ **تعريفات مرجعية للأمن السيبراني**:

- **المعهد الوطني للمعايير والتقنية:**

– يعرف الأمن السيبراني بأنه "حماية المعلومات والأنظمة من الهجمات الإلكترونية من خلال استخدام تقنيات وإجراءات وأدوات محددة لضمان السرية والتكامل والتوافر للمعلومات والأنظمة."

- **ISO/IEC 27001**

– يُعرف الأمن السيبراني بأنه "الجهود المتعمدة لحماية استخدام الإنترنت والبنية التحتية المتصلة بالإنترنت، بما في ذلك البرامج والأجهزة والبيانات، من الهجمات والتدخلات الإلكترونية."

- **المعهد الأمريكي للمحاسبين القانونيين(AICPA)**

– يُعرّف الأمن السيبراني بأنه "مجموعة من الأنشطة المتعددة التي تشمل حماية الأنظمة والشبكات والبرمجيات والبيانات من الهجمات السيبرانية، وكذلك استعادة الأنظمة بعد حدوث الهجمات."

- **المنتدى الاقتصادي العالمي(World Economic Forum)**

– يُعرف الأمن السيبراني بأنه "مجموعة من التقنيات والعمليات والممارسات المصممة لحماية الشبكات والأجهزة والبرمجيات والبيانات من الهجمات أو التلف أو الوصول غير المصرح به.

بناءً على المفاهيم السابقة للأمن السيبراني، يمكننا تعريف الامن السيبراني:

الأمن السيبراني هو مجموعة من الممارسات والتقنيات والإجراءات المصممة لحماية الأنظمة والشبكات والبرمجيات والبيانات من الهجمات الإلكترونية والأضرار والتدخلات غير المصرح بها. يهدف الأمن السيبراني إلى ضمان سرية وتكامل وتوافر المعلومات من خلال تطبيق تدابير الحماية المتنوعة، بما في ذلك التشفير، إدارة الهوية والوصول، المراقبة المستمرة، والاستجابة للحوادث. بالإضافة إلى ذلك، يسعى الأمن السيبراني إلى تأمين البنية التحتية الرقمية وتعزيز القدرة على التصدي للتحديات السيبرانية المعقدة والناشئة، مما يضمن حماية الموارد الرقمية الحيوية للمؤسسات والدول.

[40]Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. Technology Innovation Management Review, No. 4 (10), October 2014. Previously cited.

2. تعريف حوكمة الأمن السيبراني

تشير "حوكمة الأمن السيبراني" أو "حوكمة تكنولوجيا المعلومات" إلى وسائل إدارة أمن المعلومات وكذلك وسائل تنظيم الأنظمة الأمنية المطبقة في المنظمة لتحقيق أهدافها. من هذا المنطلق، فإن حوكمة الأمن السيبراني هي عملية مستمرة وجزء لا يتجزأ من ثقافة المنظمة، وتتماشى مع أهدافها الاستراتيجية، حيث تحدد القواعد الأمنية التكتيكية والتشغيلية، مثل تنفيذ الضوابط المناسبة. ولذلك فهي تضمن الامتثال للمعايير المعمول بها والتناسق في تنفيذ الإطار المعياري. سواء أكانت المنظمة تخضع لمتطلبات NIST 800-53أو ISO/IEC 27000 أو معيار أمان بيانات صناعة بطاقات الدفع(PCI DSS) ، يجب على المنظمات الالتزام بمتطلبات محددة واعتماد أفضل الممارسات في الأمن السيبراني. يعد تطوير السياسات والمبادئ التوجيهية والإجراءات نقطة البداية لإطار عمل الحوكمة، وإنشاء برنامج أمان شامل لضمان تطبيق مبادئ وتدابير وضوابط الأمان داخل المنظمة.[41]

وفقاً لمعيار ISO/IEC 27001 من المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهروتقنية الدولية (IEC)، تُعرّف حوكمة تكنولوجيا المعلومات على أنها "النظام الذي توجه المنظمة من خلاله وتتحكم في حوكمة الأمن، وتحدد إطار المساءلة وتوفر الإشراف لضمان التخفيف المناسب من المخاطر، بينما تضمن الإدارة تنفيذ الضوابط للتخفيف من المخاطر[42].

تشير حوكمة قطاع الأمن السيبراني على وجه التحديد إلى تطبيق مبادئ الحوكمة لتوفير وإدارة ومراقبة الخدمات الأمنية، في سياق وطني معين. بالإضافة إلى ذلك، يستند مفهوم حوكمة الأمن السيبراني إلى فكرة أن قطاع الأمن يجب أن يخضع لنفس المعايير العالية مثل تلك المفروضة على مقدمي خدمات القطاع العام الآخرين. عدم استيفاء قطاع الأمن لهذه المعايير يمكن أن يقوض الاستقرار السياسي والاقتصادي والاجتماعي للدولة.[43]

II. الطريق إلى النضج السيبراني

في ظل تزايد تعقيدات التهديدات والمخاطر، تواجه العديد من المنظمات تحديات كبيرة في تنفيذ حوكمة فعالة للأمن السيبراني. يُظهر إنفوجرافيك "إدارة مخاطر الأمن السيبراني: أزمة ثقة" الذي أعده معهد CMMI

[41] Gouvernance & Conformité | Sécurité de l'information | Okiok. (2018). OKIOK - Sécurité dans un monde en changement.
[42] Swinton, B. & Hedges, M. (2019). "Cybersecurity Governance: A Strategic Framework for Managing Cyber Risk.
[43] Brantly, A. F. & Puyvelde, D. V. (2019). "Cybersecurity Governance: Enhancing Security Through Risk Management

وISACA أن قادة المؤسسات يدركون أهمية الأمن السيبراني الناضج للازدهار في الاقتصاد الرقمي الحديث. ومع ذلك، غالبًا ما يفتقرون إلى الرؤى والبيانات اللازمة لضمان إدارة المخاطر السيبرانية بشكل كفء وفعال.[44]

وتظهر الدراسات أن الأضرار الناجمة عن الجرائم الإلكترونية من المتوقع أن تكلف العالم 6 تريليونات دولار سنويًا بحلول عام 2021، مقارنة بارتفاع 3 تريليونات دولار في عام 2015 وفقًا لـ Cybersecurity Ventures في حين أن 87٪ من المتخصصين في C-Suite وأعضاء مجلس الإدارة يفتقرون إلى الثقة في قدرات الأمن السيبراني لشركتهم. إذن كيف يمكن لمتخذي القرار أن يثقوا في هذا المشهد غير المؤكد خاصة في ظل جائحة كورونا(COVID-19) ؟ يتمثل أول طلب موجه لمعظم المنظمات في تمكين برنامج حوكمة قوي للأمن السيبراني[45].

1. خطوات حوكمة الأمن السيبراني:

هناك سبع خطوات يجب أن يتبعها متخذو القرار لتنفيذ برنامج حوكمة الأمن السيبراني

1 .**تحديد الوضع الحالي:** تقييم المخاطر الإلكترونية لفهم الثغرات وإنشاء خارطة طريق لسد تلك الفجوات.

2 .**إنشاء، مراجعة، تحديث جميع سياسات ومعايير وعمليات الأمن السيبراني:** في هذه الخطوة، يجب أخذ الوقت الكافي لإنشاء هيكل وتوقعات حوكمة الأمن السيبراني.

3 .**مقاربة الأمن السيبراني من منظور المؤسسة:** تحديد البيانات التي يجب حمايتها وكيفية توافق المخاطر السيبرانية مع إدارة مخاطر المؤسسة، وأولوية الاستثمار في الأمن السيبراني مقارنة بأنواع الاستثمارات الأخرى.

4 .**زيادة الوعي والتدريب في مجال الأمن السيبراني:** الهدف من الوعي والتدريب هو ضمان التأكد من أن العاملين بالجهة لديهم التوعية الأمنية اللازمة وعلى دراية بمسؤولياتهم في مجال الأمن السيبراني. والتأكد من تزويد العاملين بالجهة بالمهارات والمؤهلات والدورات التدريبية المطلوبة في مجال الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة والقيام بمسؤولياتهم تجاه الأمن السيبراني.[46]

[44] Managing Cybersecurity Risk: A Crisis of Confidence. (2020). CMMI Institute and ISACA.
[45] https://cybersecurityventures.com/annual-cybercrime-report-2017/
[46] https://ega.ee

5 .تحليلات المخاطر السيبرانية: كيفية يجب على الإدارة المعنية بالأمن السيبراني في الجهة تحديد وتوثيق واعتماد منهجية وإجراءات إدارة مخاطر الأمن السيبراني في الجهة. وذلك وفقاً الاعتبارات السرية وتوافر وسالمة الأصول المعلوماتية والتقنية[47].

6 .المراقبة والقياس والتحليل والإبلاغ والتحسين: القيام ببرمجة فترات تقييم منتظمة، وقياس ما يهم، ثم تحليل البيانات وإنشاء خطة تحسين. مع تقديم تقرير لمتخذي القرار حول النضج السيبراني وموقف المخاطر السيبرانية.

7 .القيادة مهمة: يجب أن تكون حوكمة الأمن السيبراني أولوية لدى القيادة العليا بحيث تعمل جميع السياسات والمعايير والعمليات على مواءمة حوكمة الأمن السيبراني مع أولويات الأمن السيبراني بحيث لا يتغير التركيز مع تغير المبادرات .[48]

III. جهود الجزائر في حوكمة الأمن السيبراني

تسعى الجزائر إلى تعزيز حوكمة الأمن السيبراني من خلال عدة مبادرات وسياسات تهدف إلى حماية البنية التحتية الرقمية ومواجهة التهديدات الإلكترونية المتزايدة. تشمل هذه الجهود:

1. مساعي الدولة الجزائرية لوضع استراتيجية وطنية لأمن المعلومات

- **إعداد استراتيجية وطنية لأمن المعلومات**

أطلقت الجزائر استراتيجية وطنية للأمن السيبراني لتعزيز القدرات الوطنية في مجال مكافحة التهديدات السيبرانية وتحسين التنسيق بين الجهات المعنية. في هذا السياق، ترأس رئيس الجمهورية يوم 7 جوان 2023 مراسم افتتاح الملتقى الوطني حول الأمن السيبراني، الذي نظمته وزارة الدفاع الوطني تحت عنوان "الإستراتيجية الوطنية للأمن السيبراني: من أجل جزائر صامدة سيبرانيا.

ناقش الملتقى أهمية تعزيز الأمن السيبراني في ظل التطورات الحديثة في المجال الرقمي، واستعرض المشهد الرقمي الجزائري والتهديدات التي تواجه الأنظمة المعلوماتية الوطنية. تم تحديد المحاور الأساسية لإعداد الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية، والتي شملت الوضعية الوطنية الحالية في مجال الأمن السيبراني، حماية المنشآت الحساسة، الصمود السيبراني، التعاون الدولي، جيوسياسية الفضاء السيبراني، الشراكة بين القطاعين العام والخاص، وتعزيز القدرات الوطنية.

[47] مرجع سابق .

[48] https://searchsecurity.techtarget.com

- **مبادرات المحافظة السامية للرقمنة**

أطلقت المحافظة السامية للرقمنة، التابعة لرئاسة الجمهورية، عدة مبادرات تهدف إلى إعداد مشروع قانون الرقمنة ووضع استراتيجية وطنية للرقمنة بنظرة استشرافية حتى عام 2034. تتضمن هذه الاستراتيجية مخطط تنفيذ خماسي للفترة 2024–2029، بالإضافة إلى وضع البنية التحتية الإستراتيجية للشبكات الرقمية وفق نهج تشاركي وتشاوري[49].

- **تنظيم ورش العمل والأيام الدراسية**

تم تنظيم ورش العمل والأيام الدراسية حول المحاور الأساسية للاستراتيجية الوطنية للرقمنة، بمشاركة مختلف الفاعلين في هذا المجال. تهدف هذه الأنشطة إلى تعزيز الوعي وتبادل المعرفة حول أفضل الممارسات في مجال الأمن السيبراني[50].

من خلال هذه الجهود، تؤكد الجزائر التزامها بتعزيز الأمن السيبراني وتحقيق حوكمة فعالة في هذا المجال، مما يسهم في حماية البنية التحتية الرقمية ودعم التحول الرقمي الشامل للمؤسسات الوطنية.

2. تحسين التشريعات والقوانين السيبرانية:

تم تعزيز القوانين والتشريعات المتعلقة بالأمن السيبراني في الجزائر لتوفير الحماية القانونية اللازمة للبيانات الإلكترونية ومعاقبة المخالفين. وتضمنت هذه التعزيزات العديد من القوانين والأنظمة التي تنظم النشاطات المتعلقة بتكنولوجيا المعلومات والأمن السيبراني، بما في ذلك:

- قانون رقم 09 – 04 لسنة 2009: والذي يتضمن القواعد الخاصة للوقاية من جرائم التكنولوجيا الإعلامية ومكافحتها، ويهدف إلى وضع القواعد اللازمة للوقاية من هذه الجرائم.
- الانضمام إلى اتفاقية العربية لمكافحة جرائم تقنية المعلومات: بتاريخ 21 ديسمبر 2010، من خلال مرسوم رئاسي مؤرخ 8 سبتمبر سنة 2014، والذي يهدف إلى منع جرائم تقنية المعلومات ومكافحتها.
- قانون رقم 15 – 04 لسنة 2015: الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني، ويهدف إلى تطبيق القواعد اللازمة لهذه العمليات.
- قانون رقم 18 – 04 لسنة 2018: والذي يتضمن القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، بما في ذلك تحديد وتطبيق معايير إنشاء واستغلال خدمات الاتصالات الإلكترونية.

[49] https://mns.gov.dz/static/ajax/activiter_ministre.html

[50] مرجع سابق

- قانون رقم 18 – 07 لسنة 2018: الذي يتعلق بحماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية، ويهدف إلى تحديد القواعد الخاصة بحماية هذه البيانات.
- قانون رقم 05 – 18 لسنة 2018: الذي يتعلق بالتجارة الإلكترونية، ويحدد القواعد العامة لهذا النوع من التجارة.
- مرسوم رئاسي رقم 20–05 مؤرخ في 20 جمادى الأولى عام 1441 الموافق 20 جانفي سنة 2020 ، يتعلّق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.

بالإضافة الى ذلك قامت الدولة الجزائرية قامت الدولة الجزائرية بوضع المرجع الوطني لأمن المعلومات (RNSI) بهدف توحيد حوكمة أمن المعلومات داخل الهيئات والمؤسسات. يحدد المرجع الحد الأدنى من المتطلبات الأمنية لتسيير ومقاومة وتقليل أثر التهديدات المتوقعة، ويقدم الضوابط الأمنية وأفضل الممارسات التي يجب تبنيها. يركز المرجع على تدريب وتوعية المستخدمين بالمخاطر، ويشدد على التقييم الدوري للضوابط لضمان الاستجابة المستمرة للمتطلبات الأمنية والامتثال للالتزامات التنظيمية.[51].

3. الجانب الهيكلي والمؤسساتي:

لضمان التنفيذ الفعلي والجاد لمختلف التدابير الهادفة إلى تحقيق الأمن السيبراني، أوكل متخذو القرار في الجزائر هذه المهمة إلى هيئات ومراكز متخصصة ضمن المؤسسات السيادية للدولة، نذكر منها:

- **المصلحة المركزية لمكافحة الجريمة المعلوماتية:**

– تتبع هذه المصلحة وزارة الداخلية (المديرية العامة للأمن الوطني)

– يمتد نشاطها خارج الجزائر من خلال التعامل مع الإنتربول، أفريكوم، أو مصالح الشرطة في كبرى الدول.

– على المستوى الوطني، تتواصل هذه الهيئة مع الشرطة العلمية والمكاتب المركزية المختصة في الإجرام.

- **مركز الوقاية من جرائم العالم الافتراضي والجرائم المعلوماتية:**

– يتبع هذا المركز القيادة العامة للدرك الوطني (أي وزارة الدفاع الوطني).

– نشاطه ومهامه تشابه إلى حد كبير تلك التابعة للأمن الوطني سواء محلياً أو وطنياً.

– يتم التنسيق بينهما تحت المسؤولية المباشرة للنائب العام على مستوى دائرة الاختصاص.

- **المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني:**

[51] https://www.mdn.dz/site_principal

- يتبع المعهد القيادة العامة للدرك الوطني.
- يعتمد المعهد في أداء مهامه على الخبرة العلمية والتجارب المخبرية الدقيقة.
- يستخدم التكنولوجيات الحديثة في كشف ملابسات الجرائم وتوقيف مرتكبيها لتقديمهم للعدالة.

- **وكالة امن الانظمة المعلوماتية :**

- مؤسسة عمومية ذات طابع إداري، تتمتع بالشخصية المعنوية و الاستقلالية المادية ، تابعة لوزارة الدفاع،
- تتكفل بجملة من المهام، على غرار اقتراح كيفيات اعتماد مزودي خدمات التدقيق في مجال أمن هذا النوع من الأنظمة المعلوماتية لاستخلاص المعلومات الملائمة التي تسمح بتأمين منشآت المؤسسات الوطنية،

- **السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي :**

- مُكلّفة بالسّهر على مطابقة معالجة المعطيات ذات الطابع الشخصي مع أحكام القانون رقم 18-07،
- ضمان عدم تأثير استعمال تكنولوجيات الإعلام و الاتصال على المساس بحقوق الأشخاص والحريات العامّة و حرمة الحياة الخاصّة.

4. الجانب الإداري والتنظيمي

لتحديد الصلاحيات والمسؤوليات وتفادي تداخلها، حرص متخذو القرار من خلال التشريعات والقوانين على وضع ضوابط إدارية تنظم صلاحيات كل من الهيئات المدنية، العسكرية والتقنية في مجال الأمن السيبراني:

- **الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها:**

- أنشئت سنة 2009 وتحت السلطة المباشرة لوزير العدل، وبدأت العمل بعد صدور المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015.

- **مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة:**

- أُنشئت بتاريخ 11 جوان 2015، على مستوى دائرة الاستعمال والتحضير لهيئة أركان الجيش الوطني، ومهمتها حماية المنظومات والمنشآت الحيوية للبلاد ضد كل أنواع الجريمة السيبرانية.

- **إنشاء أول مركز للأمن السيبراني تابع لاتصالات الجزائر:**

- يوفر هذا المركز خدماته للعديد من المؤسسات والهيئات لمواجهة الهجمات السيبرانية. يعتمد تنظيم المركز العملياتي للأمن على ثلاثة جوانب محورية هي: الاستجابة، الاستباقية، وجودة الأمن.

5. الجانب التقني والعملياتي :

أصبح الوصول إلى التكنولوجيات الحديثة الخاصة بالحماية والرقابة في مجال الأمن السيبراني ضرورة قصوى. وفي هذا السياق، قامت الدولة الجزائرية بالعديد من الاستثمارات من خلال التعاقد مع شركات رائدة في مجال الأمن السيبراني من دول تُعتبر صديقة وحليفة. يهدف هذا التوجه إلى تعزيز القدرات التقنية للبلاد وضمان حماية البيانات والمعلومات الحساسة بشكل فعال.

أمام التحديات السيبرانية مثل البرمجيات الخبيثة والاختراقات وسرقة البيانات، تجد الجزائر نفسها مضطرة لاتخاذ إجراءات فعالة لحماية الأمن القومي. تتضمن هذه الإجراءات تبني استراتيجية وطنية للأمن السيبراني لتعزيز التنسيق بين الجهات المعنية، وحماية البنية التحتية الحيوية والمعلومات الحساسة، والاستثمار في البنية التحتية السيبرانية. كما تشمل تحديث التشريعات لمواكبة التطورات التقنية، وتكثيف برامج التدريب والتوعية لزيادة الوعي بالمخاطر السيبرانية وتعزيز القدرات البشرية اللازمة.

من خلال هذه الجهود، تسعى الجزائر إلى إنشاء بيئة سيبرانية آمنة ومستدامة، مما يعزز الأمن الوطني ويحمي المصالح الحيوية للدولة.

IV. الأجهزة العليا للرقابية والأمن السيبراني

في أعقاب التحول الرقمي السريع الذي أحدثته جائحة COVID-19 ، واجهت الأجهزة العليا للرقابية (SAIs) تحديات جديدة تتعلق بإدارة حجم غير مسبوق من البيانات، مما يزيد من تعرضها للتهديدات السيبرانية. ومن هنا، أصبح من الضروري أن تتبنى الأجهزة العليا للرقابة نهجًا استباقيًا للأمن السيبراني لضمان حماية أنظمتها وبياناتها. ومن اجل لتعزيز البنية التحتية السيبرانية للأجهزة العليا للرقابة المالية فيما يلي خطة شاملة تتضمن[52]:

- **أولوية تقييم المخاطر والنمذجة**

- يجب على الأجهزة العليا للرقابة التأكيد على أهمية نمذجة وتقييم المخاطر لتحديد وحماية أصولها وأنظمتها التشغيلية الحيوية بدقة.
- الانخراط في تقنيات نمذجة المخاطر المتقدمة لتحديد احتمالية وتأثير التهديدات السيبرانية المتنوعة.
- تنفيذ آلية منهجية لتسجيل تقييم المخاطر لتصنيفها بناءً على أهميتها.

- **صياغة بروتوكولات متقدمة للحوادث السيبرانية**

[52] https://medium.com

- ينصح الأجهزة العليا للرقابة المالية بتطوير بروتوكولات قوية للحوادث السيبرانية، لضمان الكشف السريع، والتبليغ، واستخلاص الدروس من التعديات السيبرانية.
- قد يتطلب ذلك إنشاء استراتيجية استجابة للحوادث معقدة أو التعاون مع الجهات التنظيمية لتحسين معايير التبليغ.

- **تحالفات استراتيجية مع خبراء الأمن السيبراني**

- للبقاء في طليعة المشهد المتطور للتهديدات السيبرانية، ينبغي للأجهزة العليا للرقابة المالية تعزيز التعاون مع خبراء الأمن السيبراني البارزين.
- دمج التقنيات الأمنية المتقدمة التي تشمل مجالات الذكاء الاصطناعي (AI) والتعلم الآلي (ML) و بروتوكولات الأمان السحابي المتقدمة.

- **استقطاب وتعزيز المواهب في مجال الأمن السيبراني**

- يجب على الأجهزة العليا للرقابة المالية النظر في الاستقطاب الاستراتيجي للمهنيين ذوي الخبرة العميقة في الأمن السيبراني أو الاستثمار في برامج تعزيز المهارات لموظفيها الحاليين، وبالتالي إنشاء فريق قوي لإدارة المخاطر السيبرانية.

- **نهج شامل لتقييم المخاطر**

- بما يتجاوز حدود الثغرات التكنولوجية، يُشجَّع الأجهزة العليا للرقابة المالية على القيام بتقييم شامل للمخاطر يأخذ في الاعتبار الجوانب الاجتماعية والإنسانية والبيئية.
- يجب أن يشمل هذا النهج الشامل العواقب المحتملة للتعديات السيبرانية على حقوق الإنسان والاستدامة البيئية والاستقرار الاقتصادي الكلي.

- **نصائح لتعزيز وضع الأمن السيبراني للأجهزة العليا الرقابية:**

- البقاء يقظين بشأن التهديدات السيبرانية الناشئة.
- تبني بنية أمنية متعددة الطبقات.
- التشجيع على استخدام آليات المصادقة القوية.
- ضمان النسخ الاحتياطي المنتظم للبيانات والتكرار.
- إجراء عمليات تدقيق دورية للبروتوكولات الأمنية.
- تسهيل التدريب المستمر على الأمن السيبراني للموظفين.
- إعداد خطة طوارئ دقيقة لإدارة الحوادث السيبرانية.

باتباع هذا الإطار الاستراتيجي، يمكن للأجهزة العليا للرقابة ضمان سلامة ومرونة عملياتها في مواجهة التحديات السيبرانية المتزايدة في العصر الرقمي.

المبحث الثالث : تدقيق الامن السيبراني:

في ظل تسارع التطورات التكنولوجية واعتماد المؤسسات على الأنظمة الرقمية، برزت أهمية الأمن السيبراني كركيزة أساسية لحماية البيانات الحساسة. مع تزايد المخاطر التي تهدد البنى التحتية المعلوماتية، أصبحت عمليات التدقيق السيبراني ضرورية لضمان فعالية واستمرارية هذه الأنظمة. تدقيق الأمن السيبراني، كجزء أساسي من أي استراتيجية أمنية، يتطلب نهجًا منهجيًا يمكن الأجهزة العليا للرقابة المالية من تقييم فعالية الضوابط الأمنية والالتزام بالمعايير والسياسات .

يُمكن للمدققين تحديد الثغرات وتقديم توصيات لتعزيز الأمن والحد من المخاطر. تحقيق مستوى عالٍ من الأمن السيبراني يتطلب تعاونًا مستمرًا بين المدققين والمسؤولين لضمان الامتثال لأفضل الممارسات والاستجابة للتهديدات المستجدة. هذا يعزز ثقة العملاء والشركاء في قدرة المؤسسة على إدارة المخاطر بكفاءة.

سيستعرض هذا الفصل الأسس النظرية والعملية لتدقيق الأمن السيبراني، مع التركيز على دور الأجهزة العليا للرقابة المالية في هذه العمليات، وكيف يمكنها تحسين الأمن السيبراني عبر مختلف القطاعات.

I. المفاهيم الأساسية حول تدقيق الامن السيبراني وأهميته.

1. ماهية تدقيق الامن السيبراني

تدقيق الأمن السيبراني عملية حيوية تمكن المنظمات بمختلف أحجامها من تحديد وتقليل مخاطر الأمن السيبراني التي تواجهها. يتمثل هذا التدقيق في فحص منهجي ودقيق لضوابط أمان المعلومات داخل المنظمة، بهدف التحقق من كفاءتها في حماية البيانات والأنظمة الحساسة بشكل فعال.[53]

كما يكمن تعريف تدقيقات الأمن السيبراني تُعد بمثابة قائمة تدقيق تمكّن المنظمات من مراجعة والتحقق من سياساتها وإجراءاتها الأمنية. تمكّن هذه التدقيقات المنظمات من تقييم مدى توافر الآليات الأمنية المناسبة ومدى التزامها بالمعايير التنظيمية المعمول بها. هذا يُمكن الشركات من تبني نهج استباقي في تصميم سياسات الأمن السيبراني، مما يعزز من فعالية إدارة التهديدات. تُجرى تدقيقات الأمن السيبراني عادةً بواسطة

[53] Six Benefits of a Cybersecurity Audit (and 6 Steps to Perform One)." *ISACA Journal*. Published on January 16, 2024.

مزودي خدمة خارجيين لضمان عدم وجود تضارب في المصالح، ولكن يمكن أيضًا إجراؤها بواسطة فرق داخلية شريطة أن تعمل هذه الفرق بشكل مستقل عن الإدارة العليا للمنظمة.[54]

التدقيق الأمن السيبراني وفقًا للمعايير الدولية

التعريف وفقًا للمعهد الوطني للمعايير والتكنولوجيا(NIST) : إطار عمل NIST للأمن السيبراني هو مجموعة من المعايير التي طورها المعهد الوطني للمعايير والتكنولوجيا (NIST) بهدف مساعدة الشركات على تحسين وضعها الأمني السيبراني بشكل شامل. يُعد هذا الإطار أداة طوعية تساعد المنظمات على تحديد المخاطر السيبرانية المختلفة التي قد تضر ببنيتها التحتية وبياناتها، ووضع خطط لتحديد هذه المخاطر وإدارتها ومراقبتها بطريقة أكثر شمولاً. كما يساهم الإطار في تحديد آليات الرقابة المختلفة التي يمكن تنفيذها للتخفيف من هذه المخاطر[55].

يتميز إطار NIST بأنه مصمم لتحديد وتقليل المخاطر السيبرانية عبر قطاعات البنية التحتية الحيوية، بما في ذلك تلك التي لا تغطيها اللوائح القائمة مثل قانون المساءلة والميناء الصحي (HIPAA) و معيار أمان بيانات صناعة البطاقات الدفع (PCI DSS) .يُستخدم هذا الإطار كأداة تعاونية طوعية وينطبق على جميع المنظمات والصناعات.

يُعد تدقيق الأمن السيبراني وفقًا لإطار NIST عملية تقييم تهدف إلى ضمان أن المنظمات تطبق ضوابط أمنية فعالة وفقًا للمعايير الواردة في الإطار، لتعزيز قدرتها على مواجهة التهديدات السيبرانية وإدارة المخاطر الأمنية بفعالية.

التعريف وفقًا لمنظمة الأيزو:(ISO) تعريف تدقيق الأمن السيبراني من منظمة الأيزو (ISO)[56] يعكس منهجاً شاملاً وموحداً لتقييم وإدارة الأمن السيبراني ضمن المنظمات. تقدم الأيزو مجموعة من المعايير، مثل ISO/IEC 27001 ، التي توفر إطارًا لإدارة أمن المعلومات يشمل جميع أنواع المخاطر الأمنية. يشتمل تدقيق الأمن السيبراني وفقاً لمعايير الأيزو على تقييم منهجي للسياسات الأمنية، الإجراءات، والضوابط التي تحمي المعلومات من التهديدات أو الخروقات.

تدقيق الأمن السيبراني في إطار التشريعات الوطنية والمحلية

تدقيق الأمن السيبراني يُعد جزءًا حاسمًا من استراتيجية الأمن القومي، وفقًا للمرجع الوطني لأمن المعلومات. الإصدار الأخير من هذا المرجع في عام 2020 يحدد عشرين مجالًا رئيسيًا للأمنا:

- الأمن المادي؛

[54] https://www.strongdm.com/blog/cybersecurity-audit

[55] ملحق 01: العناصر الرئيسية لإطار إدارة المخاطر للمعهد الوطني للمعايير والتقنية(NIST)

[56] ملحق 02 : عائلة المواصفة القياسية ISO 27001

- أنترنت الأشياء (IoT) ؛
- المراقبة وتسجيل الوقائع؛
- ادارة الحوادث الأمنية؛
- تسيير استمرارية النشاطات؛
- الموارد البشرية؛
- الأمن المتعلق باستخدام مواقع التواصل الاجتماعي؛
- دمج الأمن خلال دورة حياة تطوير البرمجيات
- متطلبات الأمن لمشاريع تكنولوجيات الاعلام والاتصال
- العلاقة مع الأطراف الثالثة.
- إدارة الموجودات؛
- حماية البيانات ذات الطابع الشخصي؛
- إدارة ومراقبة النفاذ ؛
- أمن أجهزة المحمول؛
- أمن الشبكات؛
- أمن أنظمة المعلومات؛
- الأمن المتعلق بالتشغيل؛
- أمن أنظمة المعلومات بالغ الأهمية؛
- أمن الحوسبة السحابية؛
- التشفير ؛

تدقيق الأمن السيبراني في هذا الإطار يشمل التقييم المنهجي لهذه المجالات، مع التركيز على تحديد الثغرات والمخاطر المحتملة، واقتراح تحسينات أمنية تعزز من قدرة المؤسسات العامة على مواجهة التحديات السيبرانية المستقبلية.

الإصدار الأول من المرجع الوطني لأمن المعلومات في عام 2016 شمل سبعة مجالات رئيسية، مما يدل على تطور وتوسع النطاق الأمني لتشمل مجالات جديدة ومتزايدة الأهمية بمرور الوقت. هذه التحديثات تعكس التزام الهيئات العليا الرقابية بتعزيز الأمن السيبراني وتطبيق أفضل الممارسات والمعايير الدولية بشكل فعال وشامل.

بناءً على ما تقدم، يمكن تصنيف تدقيق الأمن السيبراني، الذي تنفذه الهيئات العليا للرقابة في القطاع العام، كعملية رقابية شاملة. يمكن دمج هذا التدقيق ضمن أنواع مختلفة من العمليات الرقابية مثل رقابة الالتزام، الرقابة المالية، ورقابة الأداء. قد يتم تنفيذه كجزء من الرقابة على نظام المعلومات للهيئة الخاضعة للرقابة أو كمهمة مستقلة مخصصة لتدقيق الأمن السيبراني.

تمكّن هذه العمليات الرقابية الهيئات من تقييم مدى توافر وفعالية الآليات الأمنية، ومدى التزام الهيئات بالتشريعات والمعايير الأمنية السائدة. يشمل التدقيق تطبيق معايير متنوعة تغطي التخطيط للعملية الرقابية، ومنهجيات التدقيق المبنية على التقييم الشامل للمخاطر، وغيرها من المعايير الضرورية لضمان تقديم رؤية شاملة وفعالة لأمن المعلومات.

تشكل هذه المعايير المقبولة عمومًا الأساس المنهجي للمدققين الحكوميين، مما يعزز الاستقلالية، الشفافية، المساءلة، والجودة في عملية التدقيق.

2. أهمية التدقيق السيبراني:

في ظل التحول الرقمي المتسارع، أصبح الأمن السيبراني يشكل ركنًا أساسيًا في استراتيجيات الحماية للمؤسسات العامة. هذه التحولات تلعب دورًا حاسمًا في تعزيز الأمن السيبراني ضمن الأجهزة العليا للرقابة المالية العامة والمحاسبة، وتساهم في تحقيق مجموعة من الأهداف الاستراتيجية الهامة , من أهمها [57]:

- **تحديد الثغرات:** يساعد التدقيق السيبراني في تحديد نقاط الضعف والثغرات في أنظمة المعلومات، البنية التحتية للشبكة، وبروتوكولات الأمان الخاصة بالمؤسسة. من خلال فحص شامل للإجراءات الأمنية القائمة، يكشف التدقيق عن نقاط الدخول المحتملة للهجمات السيبرانية، مما يسمح للمؤسسات بتحديد أولويات ومعالجة هذه الثغرات بشكل سريع.[58]
- **حماية المعلومات الحساسة:** يضمن التدقيق السيبراني حماية البيانات الحساسة من خلال التأكد من تشفيرها وتقييد الوصول إليها للمخولين فقط، مع تطبيق إجراءات أمنية محكمة للحيلولة دون أي تعديل، تدمير أو كشف غير مصرح به.
- **الامتثال للتنظيمات:** يعد الامتثال للوائح الصناعية وقوانين حماية البيانات أمرًا بالغ الأهمية للمؤسسات في الحفاظ على ثقة عملائها وتجنب العواقب القانونية. يضمن التدقيق السيبراني أن المؤسسة تلبي متطلبات الامتثال اللازمة وتلتزم بالمعايير ذات الصلة بحماية البيانات، مما يخفف من مخاطر العقوبات أو الأضرار التي قد تلحق بسمعتها.[59]

[57] Six Benefits of a Cybersecurity Audit (and 6 Steps to Perform One ,Previously cited.
[58] https://agileblue.com/what-is-a-cybersecurity-audit-why-is-it-important
[59] مرجع سابق.

- **تحسين الوضع الأمني:** يساعد التدقيق السيبراني على تقوية الإجراءات الأمنية من خلال الكشف عن الثغرات في ضوابط الأمان وتحديث السياسات الأمنية، وهو ما يقلل من مخاطر الهجمات السيبرانية.
- **كسب ثقة العملاء والأطراف الفاعلة:** في ظل القلق المتزايد حول أمان البيانات، تلعب التدقيقات السيبرانية دورًا مهمًا في تعزيز الثقة بين المؤسسات والمستفيدين من خدماتها، مما يعكس الجدية في التعامل مع مسائل الأمن السيبراني.
- **الحفاظ على استمرارية الأعمال:** من خلال حماية الأنظمة والبيانات الحيوية، تضمن التدقيقات السيبرانية استمرارية العمليات الحكومية وتقلل من مخاطر الانقطاعات الناجمة عن الحوادث السيبرانية.

بناءً على دراسة أجرتها وحدة التفتيش المشتركة في الأمم المتحدة كجزء من برنامجها لعام 2020، أن أهمية الأمن السيبراني في العصر الرقمي ليست محدودة على المؤسسات الخاصة فقط، بل تمتد أيضًا إلى المؤسسات الحكومية. وتشير الدراسة إلى أن التحول الرقمي واعتماد تكنولوجيا المعلومات والاتصالات والحلول المميزة قد زادا من تعقيد ونطاق التهديدات السيبرانية التي تواجه المؤسسات الحكومية. ومن هنا، تبرز ضرورة توجيه اهتمام كبير للمخاطر الجديدة والناشئة، وخاصة التهديدات العالمية والحرجة في مجال تسيير الأعمال، والمخاطر الناشئة عن تطبيق التكنولوجيا الجديدة والمواكبة لتسارع وتيرة التحول الرقمي. وتؤكد هذه الدراسة على أهمية تقديم الأمم المتحدة وحدة التفتيش المشتركة في المشاركة في دراسة سياسات الأمن السيبراني وممارساتها في منظمات الأمم المتحدة، كونها تُعد الدراسة الأحدث في سلسلة من المراجعات حول التكنولوجيا تتناول مواضيع متعلقة بالحوكمة لتكنولوجيا المعلومات والاتصالات وإدارة مواقع الإنترنت واستخدام خدمات الحوسبة السحابية.[60]

يؤكد التدقيق السيبراني على أهميته كأداة ضرورية لأي مؤسسة حكومية تسعى لحماية مواردها في عصر تزايد فيه التهديدات. من خلال تحسين الوضع الأمني وضمان الامتثال للمعايير الدولية، تسهم هذه العمليات في بناء نظام حكومي آمن وموثوق يخدم المصلحة العامة بفعالية وكفاءة.

3. تحديات الهيئات العليا الرقابية في مجال التدقيق على الأمن السيبراني

يعد الأمن السيبراني جزءًا أساسيًا من حماية البنية التحتية الحيوية في العصر الرقمي. تلعب الهيئات العليا الرقابية دورًا حيويًا في ضمان فعالية استراتيجيات الأمن السيبراني، ومع ذلك، تواجه هذه الهيئات تحديات كبيرة في تنفيذ عمليات التدقيق بشكل فعال.

أولًا: التحديات التقنية

[60] تقرير وحدة التفتيش المشتركة، الأمن السيبراني في مؤسسات منظومة الأمم المتحدة، الأمم المتحدة، 2021، ص 19.

1 .التعقيد التقني:

- **فهم الأنظمة المتطورة:** تتطلب الأنظمة الحديثة والبيئات الرقمية المتقدمة فهمًا عميقًا للهيكلية التقنية والتكنولوجية.

- **التغيرات السريعة في التهديدات السيبرانية:** تتطور الهجمات السيبرانية بسرعة وبشكل مستمر، مما يجعل من الصعب على المدققين مواكبة هذه التغيرات بشكل فعال. يظهر التهديد السيبراني بانتظام بواسطة نواقل وتقنيات هجومية جديدة، مما يجعل من الضروري لمحللي أمن تكنولوجيا المعلومات أن يظلوا على اطلاع دائم بأحدث التهديدات ونقاط الضعف لحماية الأصول الرقمية بشكل فعال.

2 .نقص المهارات والمعرفة:

نقص المهارات والمعرفة يعد من التحديات البارزة في مجال الأمن السيبراني. يتعين على المدققين ومحللي أمن تكنولوجيا المعلومات تحديث معارفهم ومهاراتهم باستمرار لمواكبة أحدث التطورات في هذا المجال المتغير بسرعة. يجب أن يكون لدى المحللين فهماً عميقاً لمبادئ ومفاهيم الأمن السيبراني وأفضل الممارسات المتبعة. يتضمن ذلك الإلمام بمختلف موجهات الهجوم، وتحليل البرمجيات الخبيثة، والأطر الأمنية مثل NISTو ISO 27001، بالإضافة إلى ممارسات الترميز الآمن. يعتبر البقاء على اطلاع بأحدث الاتجاهات والتهديدات الناشئة في مشهد الأمن السيبراني أمراً بالغ الأهمية لضمان حماية الأنظمة والشبكات بشكل فعال[61].

ثانيًا: التحديات التنظيمية

1 .الطبيعة الطوعية للإطار التنظيمي:

- **عدم القدرة على فرض التنفيذ:** الهيئات العليا الرقابية غالبًا ما تكون غير قادرة على فرض تبني المعايير والإجراءات الأمنية بشكل إلزامي.

2 .العوائق التشريعية:

- **القوانين التي تحد من جمع البيانات:** قوانين مثل قانون تخفيض الأعمال الورقية تعيق قدرة الهيئات على جمع البيانات بشكل شامل وفعال.

ثالثًا: التحديات المتعلقة بالموارد

1 .**الفجوة بين الشركات الكبيرة والصغيرة:**

[61] https://www.cybersecurityconsultingops.com/

- **تفاوت الموارد:** تمتلك الشركات الكبيرة موارد كافية لمعالجة قضايا الأمن السيبراني، في حين تعاني الشركات الصغيرة من نقص في الموارد اللازمة.

2 .تخصيص الموارد:

- **الأولويات المتنافسة:** غالبًا ما تتنافس الأولويات بين الأمن السيبراني والأمن المادي والاستجابة للكوارث، مما يقلل من التركيز على الأمن السيبراني.

رابعًا: التحديات المتعلقة بالأولويات

1 .الاعتقاد بعدم التعرض للهجوم:

- **تصورات خاطئة:** يعتقد بعض الشركات الصغيرة أنها ليست هدفًا محتملاً للهجمات السيبرانية، مما يقلل من اهتمامها بتبني تدابير الأمن السيبراني.

2 .تعدد الأولويات:

- **توزيع الجهود:** توزيع الموارد بين مختلف الأولويات يمكن أن يؤثر على فعالية التدقيق في مجال الأمن السيبراني.

تواجه الهيئات العليا الرقابية تحديات كبيرة في مجال تدقيق الأمن السيبراني. من خلال فهم هذه التحديات والعمل على تطوير استراتيجيات فعالة للتغلب عليها، يمكن تعزيز حماية البنية التحتية الحيوية وضمان أمن المعلومات والنظم الرقمية بشكل أفضل.

II. منهجية تدقيق الامن السيبراني

يُعتبر أمن المعلومات تحدياً أساسياً في العصر الرقمي الحالي، حيث تتطلب استراتيجيات الأمان التطور المستمر واعتماد منهجيات تدقيق متطورة وموثوقة. تقوم عمليات تدقيق أمن المعلومات على أسس قوية مبنية على المعايير المعتمدة عموماً لتدقيق الحكومة والعمليات النظامية. تشكل هذه المعايير إطاراً أساسياً يسهم في تقييم الأمان، وتحديد نقاط الضعف، وتقديم التوصيات لتعزيز الأمن وحماية المعلومات.

من بين النماذج البارزة في هذا المجال يأتي دليل تدقيق برنامج أمن المعلومات الصادر عن مكتب محاسبة الحكومة. يُعَد هذا الدليل مرجعاً شاملاً يقدم إرشادات دقيقة ومبتكرة لإجراءات التدقيق الأمنية بطريقة فعّالة. بفضل هذا الدليل، يستطيع المحللون والمدققون الاستفادة من أدوات وتقنيات متطورة لتقييم الأمان وتحليل التهديدات بشكل شامل وفعال.

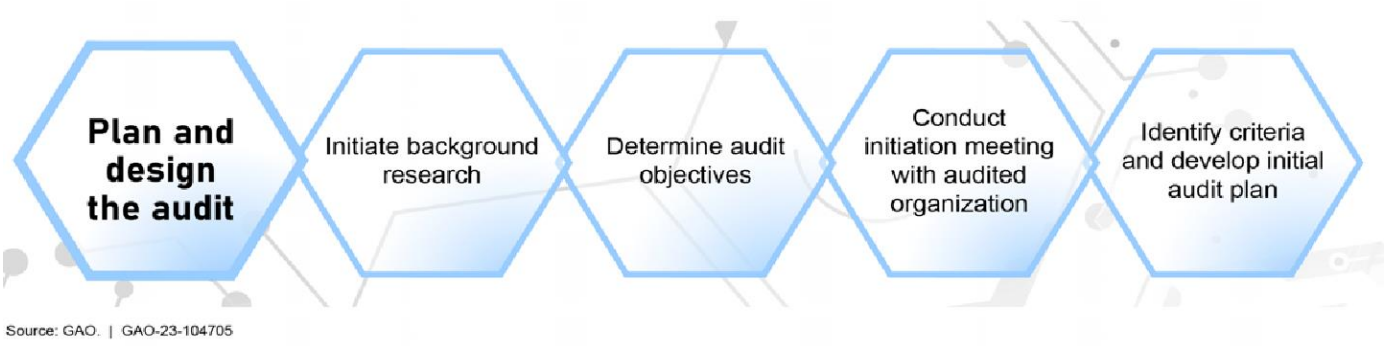
تستند عمليات تدقيق الأمن السيبراني إلى المعايير المقبولة عموماً لتدقيق الحكومة والعمليات النظامية، والتي توفر إطاراً فعّالاً لتحقيق المساءلة وتحسين العمليات والخدمات الحكومية. توفر المعايير الدولية للأجهزة العليا للرقابة المالية والمحاسبة، المعروفة بمعايير (ISSAI) إطاراً لأداء تدقيق عالي الجودة بكفاءة ونزاهة وموضوعية واستقلالية، بهدف دعم التحسين المستمر وتحقيق أعلى معايير الجودة والمساءلة في عمليات التدقيق.

تنص متطلبات العمل الميداني في معايير التدقيق والمراجعة الحكومية على نهج عام للمدققين لتخطيط وتنفيذ التدقيق للحصول على أدلة كافية ومناسبة توفر أساسًا معقولًا للنتائج والاستنتاجات القائمة على أهداف التدقيق.[62]

1. التخطيط لعملية تدقيق الامن السيبراني

التخطيط هو جزء أساسي من كل تدقيق. يساعد التخطيط الكافي في معالجة أهداف التدقيق، تصميم منهجية للحصول على أدلة كافية، تقليل مخاطر التدقيق إلى مستوى منخفض مقبول، وتوفير أساس معقول للنتائج والاستنتاجات استنادًا إلى أهداف التدقيق. خلال مرحلة التخطيط، من المهم القيام بأبحاث أولية، تحديد أهداف التدقيق، إجراء اجتماع تمهيدي مع المنظمة المدققة، وتحديد المعايير وتطوير خطة تدقيق أولية. قد تتبنى الهيئات العليا للرقابة المالية والمحاسبة تخطيط المراجعة القائمة على المخاطر لمراجعة نظم المعلومات وفقًا للمعايير الدولية.[63]

الشكل 02: تخطيط وتصميم التدقيق



المرجع: دليل تدقيق برنامج الأمن السيبراني، مكتب مساءلة الحكومة الأمريكية، (2023)، ص 13.

تضمّن مرحلة التخطيط ثلاث خطوات رئيسية يجب أن ينتبه إليها المدقق[64]:

[62] **GAO's Cybersecurity** Program **Audit** Guide (CPAG), p 11

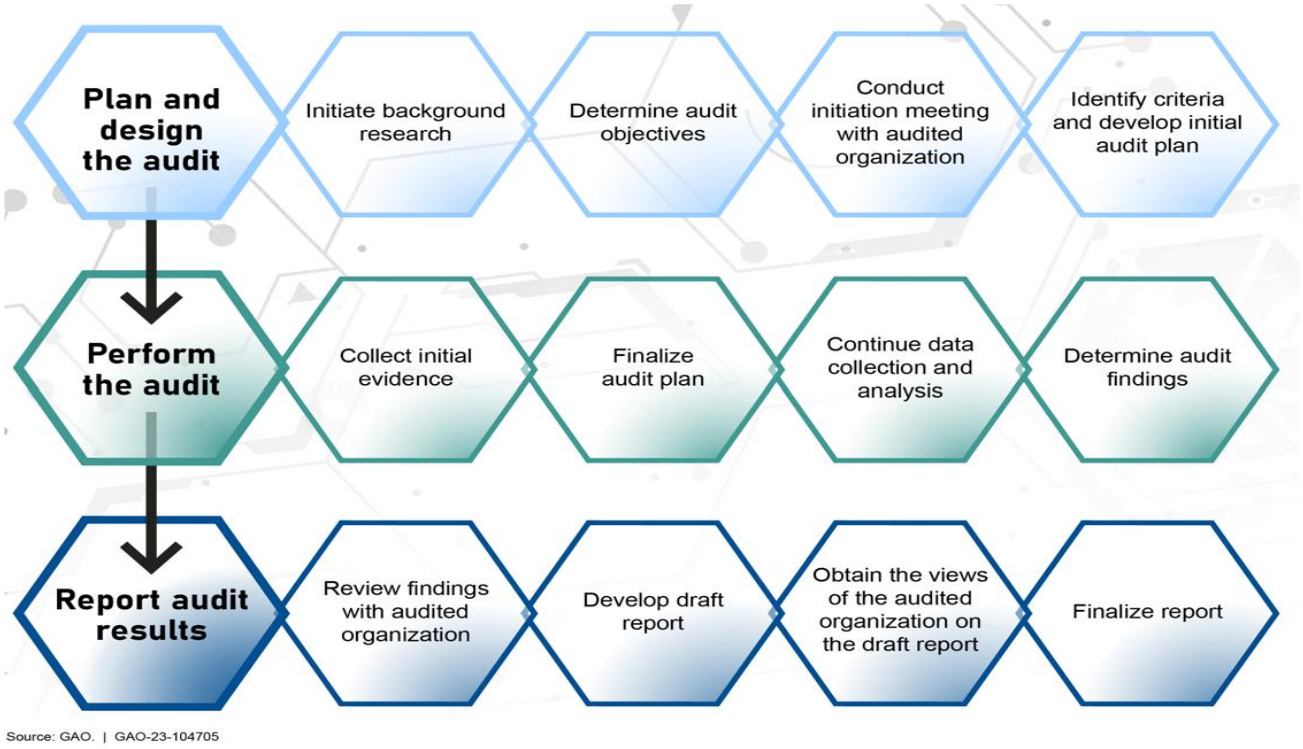
[63] الدليل إرشادي للانتوساي 5100 توجيهات بشأن مراجعة نظم املعلومات، ص 09

[64] How Effective Is Your Cybersecurity Audit?,**Author:** Matej Drašček, *ISACA Journal*. Published on June 2022

- **إعداد الخطط الاستراتيجية وفهم توقعات أصحاب المصلحة:** يستلزم من المدقق تحليل اتجاهات الصناعة في إدارة مخاطر الأمن السيبراني، وتحديد وتوضيح المخاطر السيبرانية الناشئة للإدارة العليا، والمشاركة في مناقشة توجيهية للمستقبل حول التهديدات والمخاطر السيبرانية مع الإدارة والمجلس أو لجنة التدقيق لفهم توقعاتهم. ومع ذلك، فإن هذه الخطوة غالبًا ما تُغفل من قِبل المدققين.
- **إجراء تقييم المخاطر الأولي:** توجّه هذه الخطوة مهمة التدقيق السيبراني. يتضمّن ذلك تحديد الأصول الرقمية الأكثر قيمة للمؤسسة (الجواهر الثمينة) ومستويات الحماية التي تستحقها استنادًا إلى قيمتها للمؤسسة. يجب على المدقق تقييم ضعف الأصول الرقمية الرئيسية المحددة والتأثير المحتمل في حالة سرقة أو تعرض هذه الأصول الرقمية للخطر. يمكن تنفيذ كل هذا بالتعاون مع الخطوط الأولى والثانية في إدارة مخاطر السيبرانية ، فريق تكنولوجيا المعلومات ورئيس معلومات الشركة (CIO) أو وظيفة مماثلة.
- **تحديد معايير التدقيق:** تُحدّد هذه الخطوة المعايير التي يعتمد عليها المدققون اثناء عملهم. إذا استخدمت المؤسسة المعايير الدولية لرسم الخرائط وقياس عمليات إدارة مخاطر الأمن السيبراني، مثل مثل المنظمة الدولية للتوحيد/(ISO) اللجنة الكهروتقنية الدولية (IEC) القياسية ISO/IEC 27001لإدارة أمن المعلومات، و®COBIT ، ومعايير المعهد الوطني للمعايير والتكنولوجيا (NIST)، الخيارات الأخرى تشمل قائمة CIS لأفضل 20 تهديدًا سيبرانيًا، وأداة تقييم السيبراني لمجلس المؤسسات المالية الفدرالي الأمريكي (FFIEC) ، وإطار إدارة مخاطر الأمن السيبراني لجنة الجهات المتعاونة في لجنة COSO، والمعايير المطورة ذاتيًا. يُنصح باستخدام مثل هذه المعايير لأنها تم تطويرها في العديد من التحولات من قِبل الجمعيات المهنية والعديد من الخبراء.

تم توضيح المراحل الثلاث الرئيسية لتدقيق الأمن السيبراني – التخطيط والتصميم والأداء والتقارير – كما هو موضح في الشكل 2. وعلى الرغم من أن كل مرحلة والأنشطة الرئيسية المرتبطة بها تم مناقشتها بشكل متسلسل، إلا أن العديد من الأنشطة قد تتداخل خلال التدقيق.

الشكل 03: مراحل التدقيق الاساسية



المرجع: دليل تدقيق برنامج الأمن السيبراني، مكتب مساءلة الحكومة الأمريكية، (2023)، ص 12.

يعتبر التخطيط جزءًا أساسيًا من كل عملية تدقيق. يساعد التخطيط الكافي في تحديد أهداف التدقيق، صياغة منهجية للحصول على الأدلة اللازمة، التقليل مخاطر التدقيق إلى مستوى منخفض مقبول، وتوفير أساس معقول للاستنتاجات والنتائج بناءً على أهداف التدقيق. خلال مرحلة التخطيط، يكون من الأهمية بدء البحث الخلفي، وتحديد أهداف التدقيق، وإجراء اجتماع تمهيدي مع الهيئات الخاضعة للرقابة، وتحديد المعايير وتطوير خطة تدقيق أولية.

بدء البحث الخلفي

قبل التفاعل مع الهيئة الخاضعة للرقابة ، يمكن أن يساعد فهم تلك المؤسسة في مرحلة التخطيط. يمكن الحصول على معلومات ذات صلة بالمشاركة من خلال مراجعة الأعمال التدقيقية السابقة وغيرها من مصادر المعلومات المتاحة للجمهور (مثل موقع الويب للمؤسسة، والرسوم التنظيمية، ووثائق السياسات،

وتقارير التدقيق السابقة، والمقالات المنشورة ذات الصلة). من الأهمية بشكل خاص مراجعة التقارير ذات الصلة الصادرة مسبقًا والتوصيات المرتبطة بها.[65]

تحديد أهداف التدقيق

تحديد أهداف التدقيق هو خطوة أساسية في عملية التدقيق. والأولوية الأولى هي تحديد موضوع التدقيق. فماذا يعني الأمن السيبراني في الشركة؟ تعرّف ISACA الأمن السيبراني بأنه "حماية الأصول المعلوماتية عن طريق التصدي للتهديدات التي تواجه المعلومات المعالجة والمخزنة والمنقولة عبر الأنظمة المعلوماتية المتصلة بالشبكة". وفعلًا، يشمل عالم التدقيق في الأمان السيبراني جميع مجموعات التحكم وممارسات الإدارة والحوكمة، ومخاطر الامتثال المعمول بها على مستوى المؤسسة. وفي بعض الحالات، قد يشمل عالم التدقيق الموسع أطرافًا ثالثة مرتبطة بعقد.[66]

توثيق أهداف التدقيق في مجال الأمن السيبراني أمر بالغ الأهمية في عملية التدقيق، حيث تُعتبر الأهداف الهدف الذي يسعى التدقيق لتحقيقه. تُعتبر أهداف التدقيق كأسئلة يسعى المدققون للإجابة عليها باستخدام الأدلة المتاحة ومقابل المعايير المعمول بها. ويمكن تعديل الأهداف ونطاق العمل والمنهجية أثناء أداء العمل. وتشمل الأهداف: [67]

- قد تتعلق أهداف التدقيق بتقييم الامتثال بالمراجع الوطنية والتشريعات الأخرى المتعلقة،
- وتوسيع فعالية الأمن السيبراني ضمن سياق تقييم أوسع للأنظمة، وتحسين فعالية جوانب الأمن السيبراني الأخرى مثل حماية البيانات وموثوقية النظام.
- كما تشمل أهداف التدقيق تحديد فعالية وتقييم ضوابط الأمن السيبراني وتحديد المخاطر المحتملة المرتبطة بتنفيذها، بالإضافة إلى فحص عمليات وإجراءات تطوير النظام.

في هذا الصدد، يبرز التقرير الصادر عن الأمن الداخلي للاتحاد الأوروبي للأمن السيبراني في مؤسسات الاتحاد الأوروبي الجهود الواسعة المبذولة لإعداد وتنفيذ تدقيقات الأداء المركزة على الأمن السيبراني. هذه التدقيقات تقيّم مجموعة متنوعة من المخاطر، مثل تلك المتعلقة بالتهديدات على حقوق المواطنين الأوروبيين نتيجة سوء استخدام البيانات الشخصية، وعدم قدرة المؤسسات على تقديم الخدمات العامة الأساسية بشكل كامل أو محدود، والمخاطر التي قد تؤدي إلى تبعات خطيرة على الأمن العام والرفاهية والاقتصاد في الدول الأعضاء، فضلاً عن تأثيرها على الأمن السيبراني داخل الاتحاد. عند تصميم تدقيقاتها، تعتمد هذه الهيئات على منهجيات مثل تقييم الوثائق الاستراتيجية أو السياسات المحددة، أو تحليل الإجراءات لتقييم مدى

[65] **GAO's Cybersecurity** Program **Audit** Guide (CPAG),, Previously cited , p 13.
[66] ISACA, *Information Systems Auditing: Tools and Techniques, Creating Audit Programs*, USA, 2016
[67] **GAO's Cybersecurity** Program **Audit** Guide (CPAG), Previously cited p 13 ,14

الامتثال لمعايير COBIT ، أو تقييم فعالية أنظمة إدارة تكنولوجيا المعلومات القائمة. وقد شملت التدقيقات تقييم قضايا قد تؤثر سلبًا على البنية التحتية أو الخدمات العامة.

تحديد نطاق وحدود التدقيق

النطاق يمثل حدود التدقيق ويرتبط مباشرة بأهداف التدقيق. يحدد النطاق الموضوع الذي سيقوم المدققون بتقييمه، مثل برنامج معين أو جانب من البرنامج، والوثائق أو السجلات اللازمة، والفترة الزمنية المراجعة، والمواقع التي سيتم تضمينها. يشمل نطاق التدقيق في مجال الأمن السيبراني تحديد الأنظمة الحاسوبية، والوظائف، والعمليات التي ستُقَيَّم. قد يشمل أيضًا تحديد السياسات والإجراءات التي يجب تغطيتها. على سبيل المثال، يمكن أن يتضمن النطاق:

- التعامل مع منظمة بأكملها أو جزء منها، أو شبكة، أو الاستهداف بشكل ضيق لتطبيق معين، أو تقنية محددة (مثل اللاسلكية، والسحابية، والبلوكتشين، والذكاء الاصطناعي)، أو موقع (مثل الأنظمة أو التطبيقات التي تديرها كيانات أخرى).
- تضمين كافة الضوابط أو فقط عدد محدد من الضوابط ضمن فئة مثل إدارة التكوين.

يمكن أن يكون نطاق التدقيق في الأمن السيبراني أكثر تقييدًا مقارنةً بالفحوصات العامة لتكنولوجيا المعلومات، نظرًا لتعقيداته وتفاصيله التقنية المرتفعة. لذا، يُفضل تقسيم النطاق الكلي إلى عمليات فحص واستعراضات قابلة للإدارة، سواء كان النطاق سنويًا أم متعدد السنوات، مع تجميعها حسب المجالات المعنية والنهج المعتمدين.[68]

تعد خطوة تحديد النطاق الأولى في إجراء تدقيق تكنولوجيا المعلومات من الأمور الحيوية لتدقيق أنظمة المعلومات. يشمل هذا التحديد التعرف على الأنظمة والتطبيقات والعمليات التي سيتم تدقيقها. من الضروري أن تكون محددًا بشأن أهداف التدقيق وما تسعى المؤسسة لتحقيقه والمجالات المستهدفة. يضمن تحديد النطاق أن الأنظمة والبيئات المتأثرة فقط هي التي يتم اختبارها، مما يمنع التوسع غير المقصود للنطاق والذي يمكن أن يؤدي إلى عدم الكفاءة، التأخيرات، وإرهاق الموارد، وتقليل فعالية التدقيق. يمكن للأجهزة العليا للرقابة أن تركز على وحدات عمل محددة أو تطبيقات، أو تهدف إلى تقييم فعالية برنامج الأمن السيبراني بأكمله.[69]

في سياق تحديد نطاق وحدود التدقيق، يعكس التقرير الصادر عن وحدة التفتيش المشتركة للأمن السيبراني في مؤسسات منظومة الأمم المتحدة الجهد الوافر الذي بُذل لتحديد نطاق العمل بدقة. تمت مراجعة جميع المنشآت ذات الصلة، بما في ذلك الأمانة العامة والإدارات والمكاتب، بالإضافة إلى المنظمات والبرامج

[68] ISACA, Transforming Cybersecurity, USA, 2013, www.isaca.org/knowledgecenter/research/researchdeliverables/pages/ transforming-cybersecurity-using-cobit-5.aspx

[69] Denise Owens, Managing Data Privacy and Information Security With IT Audits, *ISACA Journal*. Published on 23 May 2023

والوكالات الخاصة بالأمم المتحدة. ومن خلال التركيز الخاص على دور وحدة التفتيش المشتركة في تقديم خدمات الأمن السيبراني، تم توجيه الجهود وتحديد الأولويات بشكل دقيق.

تم أيضًا تحديد الإطار المؤسسي والقانوني الذي يحدد نطاق العمل والتدقيق، مما ساهم في توجيه الجهود وتركيزها على المسائل الأساسية. وفي الختام، أُكد على الجوانب التي لم تشمل في نطاق التدقيق، وتم استعراضها بوضوح، مما يبرز دقة العمل والتحليل المقدم في التقرير".

هذه الصياغة تحافظ على تسلسل الأفكار وتوجيه الانتباه إلى أهمية تحديد نطاق التدقيق وأثره على جودة التحليل المقدم في التقرير.

عقد اجتماع تمهيدي مع الهيئات الخاضعة للعملية الرقابية

ينبغي لفريق التدقيق إجراء اجتماع أولي مع الهيئة الخاصة للتدقيق لإعلامها بالأهداف، النطاق المبدئي، والمنهجية والجداول الزمنية المتوقعة. خلال هذا الاجتماع، يجب طلب الحصول على الوثائق ذات الصلة من المنظمة. بناءً على الأهداف، قد تُطلب معلومات عامة تشمل[70]:

- **المهام والعمليات التشغيلية:** الحصول على الوثائق التي توضح كيف تساهم العمليات التشغيلية، المرتبطة بأهداف التدقيق، في تحقيق المنظمة لمهمتها، ومدى اعتماد هذه العمليات على أنظمة وبنى تحتية لتكنولوجيا المعلومات. يشمل الأدلة التي يمكن طلبها جمع إجراءات التشغيل القياسية للمنظمة، ومخططات السير، ورسومات العمليات.
- **بنية تقنية المعلومات التنظيمية، الإدارة، والوظائف:** الحصول على وثائق تخص المكونات والفرق المهمة المتعلقة بتكنولوجيا المعلومات مثل تلك المخصصة لحماية الأمن السيبراني واستجابة الحوادث.
- **الميزانية والتمويل:** الحصول على وثائق تتعلق بمصروفات تكنولوجيا المعلومات والأمن السيبراني.
- **الأفراد والمواقع:** الحصول على وثائق تتعلق بحجم وتكوين منظمات تكنولوجيا المعلومات والأمن السيبراني من حيث الموظفين والمقاولين والمواقع.
- **البنية والنظام الشبكي:** الحصول على وثائق تتعلق ببنية الشبكة العامة للمنظمة وبنية الأنظمة ذات الصلة بالتدقيق، بالإضافة إلى الضوابط الأمنية والخصوصية المتوقع وجودها.
- **الأحداث الأخيرة والتدقيقات السابقة:** الحصول على وثائق تتعلق بالأحداث الكبرى الأخيرة مثل الحوادث الكبرى لتكنولوجيا المعلومات والأمن السيبراني.

في نهاية عملية التدقيق، يجب على الفريق تقييم مدى نجاح الاجتماع التمهيدي والإجراءات اللاحقة في تحقيق الأهداف الموضوعة. التغذية الراجعة والوثائق المحصلة خلال هذه المراحل تُسهم في تقديم رؤى قيمة لتعزيز نوعية النتائج الرقابية.

[70] **GAO's Cybersecurity** Program **Audit** Guide (CPAG), Previously cited ,p 14 ,

إطار وسياق العملية الرقابية

بمجرد تحديد أهداف التدقيق، يجب أن تحدد عملية التخطيط وتحديد النطاق جميع المجالات والجوانب المتعلقة بالأمن السيبراني التي سيتم تغطيتها. بمعنى آخر، ما هي حدود التدقيق؟ يمكن أن يشمل ذلك بلدًا محددًا، أو منطقة جغرافية، أو قسمًا، أو مجالًا من مجالات العملية، أو جانبًا معينًا من الأمن السيبراني. ويجب أن يستند هذا التحديد إلى تقييم المخاطر[71].

عادةً ما تكون نطاقات تدقيق الأمن السيبراني أكثر تحديدًا من تلك الخاصة بتدقيق تكنولوجيا المعلومات العام بسبب مستوى التعقيد العالي والتفاصيل الفنية التي يجب تغطيتها. بالنسبة لنطاق سنوي أو متعدد السنوات، يُنصح بتقسيم النطاق الكلي إلى تدقيقات ومراجعات قابلة للإدارة، وتصنيفها حسب المنطقة التي يتم تناولها وبحسب النهج المتبع.[72]

في سياق تحديد منهجية التدقيق، يعكس التقرير الصادر عن الأمن الداخلي للاتحاد الأوروبي للأمن السيبراني في مؤسسات منظومة الاتحاد الأوروبي، الجهود الكبيرة التي بُذلت لإعداد وتنفيذ تدقيقات أداء تركز على الأمن السيبراني. فقد أجرت معظم الهيئات العليا للرقابة تدقيقات أداء حول موضوعات متعلقة بالأمن السيبراني، بينما قامت هيئتين، في بولندا وهنغاريا، بإجراء تدقيقات الامتثال، وأجرت محكمة المحاسبات الأوروبية تحليل السياسات ذات الصلة.

تنوعت الموضوعات المعالجة في تدقيقات الأمن السيبراني بشكل كبير، حيث ركزت بعض الهيئات العليا للرقابة على مجالات ذات اهتمام عام خاص، مثل دفاعات بحرية وأنظمة إدارة المياه، بينما ركزت هيئات أخرى مثل الإيرلندية والمجرية على قضايا أكثر شمولية مثل تنفيذ الاستراتيجية الوطنية للأمن السيبراني وحماية البيانات الشخصية وأصول البيانات الوطنية. جميع هذه الجهود فحصت قضايا يمكن أن تؤثر سلبًا على البنى التحتية أو الخدمات العامة. هيئات الرقابة العليا في إستونيا وليتوانيا أكدت على الأهمية الاستراتيجية لأصول البيانات الوطنية الضرورية للأمن الوطني وحماية سلامتها من الهجمات السيبرانية الخارجية. الهيئة الدانماركية أجرت تدقيقًا لتقييم مدى قدرة أربع هيئات عامة على مقاومة الهجمات ببرامج الفدية. هيئات الرقابة العليا في هولندا، بولندا، والبرتغال نفذت تدقيقات لفعالية أنظمة المعلومات المختلفة المستخدمة في التحكم بالحدود. هذه التدقيقات تناولت أيضًا الأمن الداخلي للاتحاد الأوروبي.

2. الاستعانة بخبراء خارجيين

في ظل قيود الموارد، قد تلجأ الهيئات العليا للرقابة المالية والمحاسبة إلى الاستعانة بخبراء خارجيين مثل المستشارين والمقاولين في مجال تكنولوجيا المعلومات لإجراء مراجعات نظم المعلومات. تضمن هذه الهيئات أن يكون هؤلاء الخبراء مدربين ومطلعين جيدًا على المبادئ التوجيهية للسلوك المهني ومعايير المراجعة

[71] Ian Cooke, Previously cited ,P03 .
[72] *Transforming Cybersecurity*, ISACA USA, 2013- https://www.isaca.org ›

المعمول بها. يجب أن يخضع عملهم لمراقبة دقيقة من خلال عقود موثقة أو اتفاقيات مستوى الخدمة، مع مشاركة فعالة من موظفي الهيئة في مراحل التخطيط والمراجعة وإعداد التقارير والمتابعة. كما يجب أن يضمن وجود أعضاء في الفريق ذوي المهارات والمعرفة الكافية لضمان الامتثال للمعايير المتفق عليها.
يجوز للمدققين أن يستخدموا الاعمال التي قام بها المدققين الداخلين أو غيرهم من المدققين أو الخبراء؛ إذا كان ذلك ملائما أو ضرورياً ، وبما يتماشى مع تفويض الجهاز الأعلى للرقابة المالية والمحاسبة والتشريع المعمول به. ويجب أن توفر إجراءات المدقق اساسا كافيا لاستخدام أعمال الاخرين، وعلى المدقق في جميع الأحوال أن يحصل على براهين لكفاءة واستقلالية المدققين أو الخبراء الآخرين وجودة الأعمال التي نفذوها. غير أن الجهاز الاعلى للرقابة المالية والمحاسبة وحده مسئول عن أي رأي أو تقرير رقابي ينتجه بشأن الموضوع؛ وال يخفف من هذه المسئولية استخدامه للأعمال التي نفذها أطراف أخرى[73] .

3. تنفيذ التدقيق

لا يتعلق تنفيذ المهمة الرقابية بكيفية جمع الأدلة التدقيقية بشكل شامل فقط، بل يشمل أيضًا بُعدًا آخر وهو جمع هذه الأدلة بشكل دقيق. في دورة التدقيق، يجب جمع الأدلة بشكل منهجي عبر المجالات الأربعة المحددة في إطار الأمن السيبراني. تتضمن هذه المجالات مجموعات مختلفة من العمليات مثل إدارة الهوية والوصول، حماية البيانات، أمن السحابة والبرمجيات، وإدارة الجهات الخارجية والقوى العاملة، على سبيل المثال لا الحصر. لكي يكون تدقيق الأمن السيبراني فعالاً، يجب جمع أدلة كافية وملائمة لاتخاذ قرار مستنير [74].

تحدد المعايير الدولية للتدقيق (ISA) مجموعة من الإجراءات لجمع الأدلة (ISA 500) الاستفسار، الملاحظة، الاستفسار، الإجراءات التحليلية، وإعادة التشغيل. قد لا تكون بعض هذه الإجراءات موثوقة بما يكفي لاستخدامها بشكل منفرد لتحقيق تدقيق فعال للأمن السيبراني. على سبيل المثال، إذا جمع الفريق الرقابي الأدلة من خلال مقابلة الأدوار الأولى والثانية فقط (أي من خلال الاستفسار)، فقد يكون ذلك فعالاً من حيث الكفاءة ولكنه أقل فعالية مقارنة بإعادة بعض العمليات التي قام بها المسيرون. عادةً ما يتم جمع الأدلة الكافية من خلال مزيج من الطرق المختلفة لضمان جودة الأدلة وفقًا للمعايير.[75]

[73] انتوساي. (2010). المبادئ الأساسية لرقابة القطاع العام - اساي 100. إدارة فريق الرقابة ومهاراته، ص 14.
[74] E.E. El-Masry, K.A. Hansen,Factors affecting auditors' utilization of evidential cues. Taxonomy and future research directions Managerial Audit. J., 23 (1) (2008), pp. 26-50,
[75] Sergeja Slapničar, Effectiveness of cybersecurity audit, International Journal of Accounting Information Systems, Volume 44, March 2022, P 5

تشمل المراحل الرئيسية لتنفيذ التدقيق حسب المكتب الحكومي للمسائلة الامريك ما يلي: (1) جمع الأدلة الأولية، (2) وضع اللمسات الأخيرة على خطة التدقيق، (3) مواصلة جمع البيانات وتحليلها، و (4) تحديد نتائج التدقيق[76].

- **جمع الأدلة الأولية**

يمكن تصنيف الأدلة إلى مادية أو وثائقية أو شهاداتية.

-**الأدلة المادية (physical evidence)** : تُجمع من خلال فحص المدققين المباشر، أو المشي للأماكن، أو ملاحظة الأشخاص أو الممتلكات أو العمليات. تُسجل هذه الأدلة في مذكرات ملخصة، صور فوتوغرافية، فيديوهات، رسوم بيانية، خرائط، أو عينات مادية. يجب النظر فيما إذا كانت هناك حاجة إلى إذن من المنظمة قبل جمع الأدلة المادية، مثل أخذ صور لواجهة مبنى عام مقابل الصور داخل المنشأة.

-**الأدلة الوثائقية (Documentary evidence)** : هي المعلومات الموجودة بالفعل، مثل نسخ السياسات والإجراءات، نتائج الفحوصات السابقة، لقطات الشاشة، سجلات التدريب، سجلات الأحداث والوصول، جداول البيانات، مقتطفات قواعد البيانات، ومعلومات الأداء التي طورتها المنظمة. تشمل الأمثلة الإضافية للأدلة الوثائقية التي تُجمع أثناء التدقيقات السيبرانية:

- قوائم الجرد لأنظمة المعلومات الرئيسية
- تقارير التدقيق ذات الصلة
- خطط أمان النظام
- خطط الطوارئ واستعادة الكوارث
- تقييمات المخاطر
- تقييمات تأثير الخصوصية
- تقييمات الضوابط الأمنية
- تقارير التقييم الأمني
- خطط العمل التصحيحية(POA&M)
- مفاهيم العمليات
- مخططات الشبكة
- اتفاقيات مع الكيانات الخارجية
- قوائم الأدوات المستخدمة في التحليلات الجنائية وكشف التسلل وإدارة التكوين والتصحيحات
- حزم ترخيص النظام
- قوائم الحوادث السيبرانية (ضمن إطار زمني محدد)

[76] **GAO's Cybersecurity** Program **Audit** Guide (CPAG), Previously cited , P 27.

- عمليات فحص التكوين وإدارة التصحيحات
- قوائم الجرد لبعض أجهزة الشبكة
- قوائم الإعفاءات النشطة من الضوابط الأمنية

– **الأدلة الشهاداتية (Testimonial evidence)** : تُجمع من خلال الاستفسارات، المقابلات، المجموعات البؤرية، المنتديات العامة، أو الاستبيانات. تُقيَّم الأدلة المُجمعة لتحديد ما إذا كانت كافية وملائمة، بما في ذلك ضمان أنها ذات صلة، صحيحة، وموثوقة.

تقييم موثوقية البيانات: تُعتبر موثوقية البيانات الحاسوبية والنظم التي تعالج وتحافظ على هذه البيانات عاملًا هامًا في إجراء معظم التدقيقات، وخاصةً في تدقيقات الأمن السيبراني. تشمل عملية تقييم موثوقية البيانات عدة مراحل أساسية تأخذ في الاعتبار أهمية البيانات، قوة الأدلة المؤكدة، ومخاطر استخدام البيانات، إلى جانب ما يُتعلم خلال التقييم.

- **<u>إنهاء خطة التدقيق</u>**

قبل إنهاء خطة التدقيق، يجب على فريق التدقيق إجراء اختبار مبدئي كافٍ للبيانات الأساسية لتقديم ضمان معقول لتوافرها وموثوقيتها. تعد التوافرية مهمة لأنه إذا لم يتمكن الفريق من الوصول إلى البيانات المناسبة، أو إذا كانت البيانات المطلوبة لتحقيق الأهداف غير موجودة بسهولة، فسيتعين على الفريق إعادة تقييم أهدافه. تعتبر الموثوقية أمرًا أساسيًا لأنه إذا كانت البيانات غير موثوقة، فلن يتمكن الفريق من استخدامها لدعم الاستنتاجات والتوصيات. عند إنهاء الخطة، يجب على فريق التدقيق مراعاة التغييرات في الأهداف، والنطاق، وإجراءات التدقيق، والوقت، والموارد.

- **<u>متابعة جمع وتحليل البيانات</u>**

قبل إتمام خطة التدقيق، قام الفريق الرقابي بمتابعة جمع وتحليل البيانات وفقاً لخطة التدقيق اللاولية. عند تحليل الأدلة، خاصةً لتقييم الضوابط، قد يكون من المناسب استخدام مزيج من الفحوصات، المقابلات، والاختبارات.

–**الفحوصات (Examinations)**: تشمل مراجعة وفحص وملاحظة ودراسة وتحليل واحد أو أكثر من موضوعات التقييم (مثل المواصفات أو الآليات أو الأنشطة). تهدف الفحوصات إلى تسهيل فهم المدققين، تحقيق التوضيح، أو الحصول على الأدلة.

–**المقابلات (interviews)**: تتضمن إجراء مناقشات مع أفراد أو مجموعات داخل المنظمة لتسهيل فهم المدققين، تحقيق التوضيح، أو الحصول على الأدلة.

–**الاختبارات (Tests)** : تشمل ممارسة واحد أو أكثر من كائنات التقييم (مثل الأنشطة أو الآليات) تحت ظروف محددة لمقارنة الحالة الفعلية بالحالة المرغوبة أو السلوك المتوقع.

4. عرض وتقديم نتائج التدقيق

الشكل 04: تقديم نتائج التدقيق

المرجع: دليل تدقيق برنامج الأمن السيبراني، مكتب مساءلة الحكومة الأمريكية، (2023)، ص 28.

ينبغي تطبيق نظام إعداد التقارير المتبع في جهاز الرقابة الأعلى على تقارير تدقيق تكنولوجيا المعلومات، يجب أن تقيم تقارير تدقيق تكنولوجيا المعلومات التقنيات التي تم فحصها بناء على مستوى الدقة المطلوبة من قبل المهتمين بالتقرير[77].

تقديم تقرير شامل يُعد البُعد النهائي لتَحقق من فعالية الحوكمة الأمنية السيبرانية. فقط من خلال استعراض شامل لإدارة مخاطر الأمن السيبراني يمكن اكتشاف نقاط ضعف جوهرية في الضوابط، وبالتالي تجنب تزويد أصحاب المصلحة بشعور زائف بالأمان.[78]

يجب أن يكون التقرير دقيقًا وموضوعيًا وبناءً وشاملًا وفي الوقت المناسب وفقًا لمعيار 2420 لجمعية المدققين الداخليين لجودة الاتصالات. الطريقة لتحقيق ذلك هي إصدار رأي شامل كما هو محدد في المعايير. تقديم تقرير حول فعالية إدارة مخاطر الأمن السيبراني يُعتبر تحديًا خاصًا بسبب المصطلحات التقنية، مما يستدعي تقديمه بطريقة سهلة الفهم[79].

في هذه المرحلة، من المهم جداً تقييم كفاية الأدلة. عند تحليل الأدلة، يجب على فريق التدقيق تقييم ما يلي[80]:

-توثيق طبيعة وتوقيت وامتداد الاختبارات.

-أدلة على فعالية تقنيات التحكم أو عدمها (مثل المذكرات التي تصف الإجراءات والنتائج، مخرجات الأدوات، والتحليل المرتبط).

---

[77] دليل دقيق تكنولوجيا المعلومات للأجهزة العليا للرقابة المالية،2014، ص 28

[78] https://www2.deloitte.com › Deloitte ›

[79] https://iaonline. theiia.org/blogs/Jim-Pelletier/2020/Pages/3-

[80]GAO's Cybersecurity Program Audit Guide (CPAG), P 28.

-أي ضوابط تعويضية أو عوامل أخرى وأساس تحديد الفعالية.

-لكل نتيجة تقييمية، المعايير، الحالة، السبب، والأثر.

-الاستنتاجات والتوصيات المستندة إلى النتائج التقييمية.

يجب أن يتضمن مراجعة الأدلة وتحديد النتائج تحديد أي فجوات في المعلومات والمتابعة مع الهيئة الخاصعة، إذا لزم الأمر، لطلب أدلة إضافية أو توضيحات قبل إتمام التحليلات.

- **تقرير نتائج التدقيق**

بعد تنفيذ عمل التدقيق، يجب على الفريق الرقابي[81]:

1 .مراجعة النتائج مع المنظمة المدققة.

2 .إعداد مسودة التقرير.

3 .الحصول على آراء المنظمة المدققة على مسودة التقرير.

4 .إتمام التقرير.

- **مراجعة النتائج مع المنظمة المدققة**

عند إتمام عمل التدقيق، يجب على فريق التدقيق تقديم بيان بالحقائق للهيئة الخاضعة يصف نتائج التدقيق. يمكن للهيئة الخاضعة التعليق على هذا البيان ومناقشته وتقديم ملاحظات ووثائق داعمة قد تؤثر على النتائج والتوصيات. خلال هذه الفترة، يتم مناقشة أي مسائل حساسة قد تكون لدى العيئة الخاضعة وتحديث مسودة التقرير وفقًا لذلك. يجب التواصل مع هذه الاخيرة بشأن أي نتائج تتطلب إصلاحًا فوريًا طوال فترة التدقيق حسب الحاجة.

- **إعداد مسودة التقرير**

يجب أن تقدم تقارير التدقيق النتائج بطريقة واضحة ومفهومة. يجب أن يتضمن التقرير أهداف التدقيق، النطاق، المنهجية، النتائج، الاستنتاجات، والتوصيات. يجب دمج المعلومات المقدمة من الهيئة الخاصعة استنادًا إلى بيان الحقائق بشكل مناسب في التقرير. بالإضافة إلى ذلك، يُفضل استخدام الرسوم البيانية والجداول لتعزيز وضوح التقرير وقراءته.

- **الحصول على آراء المنظمة المدققة على مسودة التقرير**

تقديم مسودة التقرير مع النتائج للمراجعة والتعليق من قبل المسؤولين في الهيئة الخاصعة يساعد في تطوير تقرير عادل، شامل، وموضوعي. تُفضل التعليقات المكتوبة من المنظمة، ولكن التعليقات الشفهية مقبولة أيضًا.

- **تحديد حساسية التقارير**

[81] نفس المرجع ص 28

عند إعداد تقارير التدقيق في الأمن السيبراني، غالبًا ما تقوم المنظمات بإعداد تقريرين: تقرير عام وتقرير حساس يحتوي على محتوى لا يمكن نشره للجمهور. يتميز التقرير الحساس بتقديم تفاصيل إضافية حول المنظمة ونتائج التدقيق، ولكن عيبه هو خطر الكشف، خاصة إذا تم إصداره لمنظمة تشاركها مع عدد كبير من الموظفين لتسهيل التصحيح. يتمتع التقرير العام بجمهور أوسع وشفافية أكبر ولكنه لا يمكن أن يحتوي على معلومات حساسة[82] .

لتجنب الكشف العلني للمعلومات الحساسة، يجب تقديم مسودات تقارير الأمن السيبراني إلى الهيئة الخاصعة لمراجعة الحساسية. بعد تلقي نتائج مراجعة الحساسية، يتم إجراء التعديلات المناسبة على التقرير. اعتمادًا على التدقيق، يمكن إصدار تقرير عام أو حساس أو كليهما.

- **إنهاء التقرير**

بعد أن حصول الهيئة الخاضعة على الوقت الكافي لمراجعة مسودة التقرير وتقديم تعليقاتها، يمكن لفريق التدقيق إنهاء تقرير التدقيق. يتضمن إنهاء تقرير التدقيق معالجة تعليقات الهيئة الخاضعة أو رسالة استجابة الإدارة الموقعة. إذا تم تقديم تعليقات شفهية بدلاً من ذلك، يجب تحديد مصدر التعليقات في تقرير التدقيق. بعد إتمام هذه الخطوات، يمكن لفريق التدقيق المضي قدمًا في عملية نشر وتوزيع التقرير.

[82] نفس المرجع ص 28

خلاصة الفصل

يسلط هذا الفصل الضوء على أهمية تقييم أنظمة المعلومات والأمن السيبراني كأساس حيوي لحماية البنية التحتية المعلوماتية وضمان استمرارية الأعمال. تتناول عملية الرقابة على نظم المعلومات تقييم العمليات والمعلومات التقنية للتحقق من فعاليتها وأمانها في تحقيق أهداف العمل. تشمل هذه العملية فحص تطوير وتنفيذ وصيانة أنظمة تكنولوجيا المعلومات، مع ضمان توافقها مع احتياجات العمل دون المساس بالأمن، الخصوصية، والتكلفة.

ويُلاحظ أن الأمن السيبراني يلعب دورًا محوريًا في حماية الأصول المعلوماتية من التهديدات السيبرانية المتزايدة. يتطلب الأمن السيبراني مجموعةً من التقنيات والممارسات التي تهدف إلى حماية المعلومات من الوصول غير المصرح به، وضمان استقرار وأمان المؤسسات. يُسهم تطبيق حوكمة الأمن السيبراني وخطوات النضج السيبراني في بناء إطار متين لحماية البيانات وتعزيز فعالية العمليات داخل المؤسسات.

ويهدف تدقيق الأمن السيبراني إلى تقييم جاهزية المؤسسات للتعامل مع التحديات السيبرانية، ويشمل فحص مدى توافر وفعالية الآليات الأمنية، والالتزام بالتشريعات والمعايير الأمنية. تعتمد منهجية التدقيق على تقييم شامل للمخاطر وتطبيق معايير التدقيق الدولية، مما يضمن تقديم رؤية شاملة وفعالة لأمن المعلومات.

وفي هذا الصدد، تلعب الأجهزة العليا للرقابة المالية والمحاسبة دورًا حيويًا في تعزيز الرقابة على نظم المعلومات في ظل التحول الرقمي والتطورات التكنولوجية المتسارعة. من خلال إنشاء وحدات متخصصة، وتبني أفضل الممارسات والمعايير الدولية، تسهم هذه الأجهزة في ضمان الشفافية، الكفاءة، والأمن السيبراني. كما يعزز التعاون بين الجهات المعنية وتطوير أدوات وتقنيات التدقيق قدرة هذه الأجهزة على حماية البيانات وضمان استمرارية العمليات الحكومية.

وفي الختام، يُؤكد هذا الفصل على الأهمية البالغة لتقييم أنظمة المعلومات والأمن السيبراني لضمان تحقيق أهداف المؤسسات وحمايتها من التهديدات السيبرانية المتزايدة. ويبرز أن التعاون الوثيق بين الأجهزة العليا للرقابة والمؤسسات الحكومية والقطاع الخاص يمثل أساساً لتحقيق بيئة سيبرانية آمنة ومستدامة.

الجـــانب العمـــلي والتحليلي للمهمة الرقابية تقييم نظم معلومات شركة سونلغاز للتوزيع وأمنها السيبراني

تمهيـــد:

تُعَدّ الكهرباء والغاز عصب حياة العديد من التقنيات الحديثة وهي خدمة غالباً ما يُغفل عن دورها الحيوي، إذ يصعب على العديد من الأشخاص، خاصة في الدول المتقدمة، تصور الحياة بدونهما لاعتماد العديد من جوانب الحياة اليومية على توفر الكهرباء والغاز بشكل أساسي. بالإضافة إلى ذلك، تُعتبر بنية نقل وتوزيع الكهرباء والغاز جزءًا أساسيًا من البنية التحتية الحيوية لمعظم الدول في العالم إذ تسهم في تأمين استدامة توفير الطاقة وتشغيل الصناعات وتوفير الخدمات الأساسية للمجتمع.

تُعتبر مؤسسة سونلغاز من الهياكل الأساسية الهامة في القطاع الطاقوي في الجزائر، حيث تعمل على تحقيق التنمية الاقتصادية والاجتماعية في البلاد وذلك في ظل التحديات والتطورات الحالية. بدأت المؤسسة في تطبيق استراتيجيات تعتمد على تكنولوجيا المعلومات كجزء من خططها الاستراتيجية الأخيرة بهدف تحقيق الجودة بتكاليف أقل وتقليص الوقت المخصص للإنتاج والتوزيع.

نظرًا لأهمية البنية التحتية لنقل وتوزيع الطاقة، فإن حماية المؤسسات التي تدير هذه الخدمات من التهديدات السيبرانية أمر بالغ الأهمية خاصة مع زيادة التهديدات السيبرانية والهجمات المتطورة. وفقًا لدراسة أُجريت في عام 2021، تبين أن 83 في المائة من البنية التحتية الحيوية للمنظمات تعرضت لانتهاكات في التكنولوجيا التشغيلية خلال الـ 36 شهرًا السابقة[83].

ونتيجة لهذه الأحداث، فقد تم استحداث الالتزام بضوابط ومعايير الأمن السيبراني لشركات الكهرباء والغاز في جميع أنحاء العالم، والتي صدرت عن الهيئات الدولية.، حيث قامت منظمات الأمن السيبراني مثل الوكالة الأوروبية لأمن المعلومات (ENISA)، وISACA، والمنظمة الدولية للتوحيد (ISO)، والمعهد الوطني للمعايير والتقنية (NIST) الأمريكي بإصدار إرشادات، طرق، ونهجًا للتعامل مع المشكلة وزيادة الوعي بالاستعداد ضد الهجمات السيبرانية[84]. في الاتحاد الأوروبي، قامت ENISA بمراجعة وضع الوعي بالأمن السيبراني بين الدول الأعضاء[85].

تهدف هذه الضوابط إلى توفير الحد الأدنى من المتطلبات الأساسية للأمن السيبراني، والتي تستند إلى أفضل الممارسات والمعايير لتقليل المخاطر السيبرانية على الأصول المعلوماتية والتقنية للجهات من

[83] Center for St[illegible]national Studies (CSIS), Significant Cyber Incidents Since 2006, USA, 2021, https://csis-website-prod. s3.amazonaws.com/s3fs-public/220104_ Significant_Cyber_Events.pdf

[84] Volume 1, 2023, ISACA Journal, Case Study: Performing a Cybersecurity Audit of an Electric Power Transmission Systems Operator .

[85] European Union Agency for Cybersecurity (ENISA), *Raising Awareness of Cybersecurity: A Key Element of National Cybersecurity Strategies*, Greece, 29 November 2021, *https://www.enisa.europa.eu/publications/*

التهديدات الداخلية والخارجية. وتتطلب حماية الأصول المعلوماتية والتقنية للجهة التركيز على الأهداف الأساسية للحماية، والتي تشمل[86]:

- سرية المعلومات (Confidentiality)
- سلامة المعلومات (Integrity)
- توافر المعلومات (Availability)

المصدر: المعهد الوطني الأمريكي للمعايير

وتأخذ هذه الضوابط بعين الاعتبار المحاور الأربعة الأساسية التي يعتمد عليها الأمن السيبراني، وهي:

- الاستراتيجية (Strategy)
- الأشخاص(People)
- الإجراءات (Process)
- التقنية (Technology)

تأمين البنية التحتية والأنشطة لمؤسسات توزيع الغاز والكهرباء يعد أمرًا بالغ الأهمية في ظل التهديدات السيبرانية المتزايدة أين يصبح من الضروري تقييم استعداد المؤسسات في هذا القطاع لمواجهة هذه التحديات. تُعتبر العملية الرقابية للأمن السيبراني التي أُجريت من قبل مجلس المحاسبة الجزائري في إطار تقييم تسيير مؤسسة الغاز للتوزيع أحد أهم عمليات التدقيق في مجال الأمن السيبراني في قطاع الطاقة بالجزائر، حيث تهدف هذه الدراسة إلى تقييم جاهزية نظام المعلومات لمواجهة التهديدات السيبرانية وتحديد الثغرات والتحديات، ومدى وضع الشركة لاستراتيجيات لتعزيز الأمن وحماية البنية والأنشطة من مختلف التهديدات.

I. دوافع وأهداف رقابة مجلس المحاسبة الجزائري لرقابة نظام معلومات وأمنها السيبراني في شركة سونلغاز للتوزيع:

مجلس المحاسبة الجزائري هو الهيئة الرقابية العليا المسؤولة عن رقابة الأموال العمومية، ويتمتع بصلاحيات دستورية وقانونية في مجال الرقابة البعدية على مالية الدولة والجماعات المحلية، تكلف هذه

[86]https://ega.ee › Essential-Cybersecurity-Controls

الهيئة بتطوير الحكم الرشيد للمال العام وتعزيز الشفافية في الإدارة العامة، وتمتلك صلاحيات إدارية وقضائية تمكنها من ممارسة الرقابة الشاملة على الأموال العمومية.

يقوم المجلس بإجراء جميع أنواع الرقابة، بما في ذلك رقابة الالتزام، المالية والأداء، وذلك وفقًا للتشريعات الوطنية والمعايير الدولية للأجهزة العليا للرقابة المالية والمحاسبة، ويتولى المجلس مهمة الرقابة على مختلف أنواع الهيئات، بما في ذلك تلك التي تقدم خدمات عامة مثل الصحة والتعليم والطاقة.

إن **التفويض الممنوح لجهاز الرقابة الأعلى لإجراء تدقيق لنظم تكنولوجيا المعلومات** موجود ضمن المعايير الدولية لأجهزة الرقابة العليا ISSAI في إعلان ليما، حيث أن التفويض الممنوح لجهاز الرقابة الأعلى لتدقيق تكنولوجيا المعلومات مستمد من التفويض العام الممنوح لجهاز الرقابة الأعلى للقيام بالتدقيق المالي، وتدقيق الالتزام، وتدقيق الأداء، أو المزج فيما بينهم[87].

الشكل 04: توصيل المزارع بالكهرباء والغاز قبل نهاية نوفمبر 2022

المصدر : سونلغاز الجزائر.[88]

تتمثل **دوافع وأهداف رقابة مجلس المحاسبة الجزائري لرقابة نظام معلومات شركة سونلغاز للتوزيع وأمنها السيبراني** في تقييم جاهزية الشركة كمُشغل رئيسي في قطاع الطاقة بالجزائر، ويهدف ذلك إلى تقييم قدرتها على حوكمة نظام معلوماتها ومواجهة التهديدات السيبرانية التي قد تؤثر على توزيع التيار الكهربائي والغاز للمستهلكين، وذلك لضمان استقرار وموثوقية توزيع الطاقة في البلاد.

بالإضافة إلى ذلك، يسعى المجلس إلى تعزيز قدراته في تقييم نظم المعلومات، مواكبة للبيئة الرقابية والتوجيهات العامة للحكومة الجزائرية، كما يسعى المجلس إلى الالتزام بتوجيهات منظمة الأجهزة العليا للرقابة المالية والمحاسبة الدولية (الإنتوساي) والهيئات الإقليمية التابعة لها.

II. إطار وسياق العملية الرقابية

في إطار عمليات التدقيق على نظم المعلومات وبالأخص الأمن السيبراني، قامت الهيئات الرقابية العليا بإجراء عمليات تدقيق أداء في مواضيع تتعلق بالأمن السيبراني حيث قامت بعضها بعمليات تدقيق الامتثال،

[87] دليل الرقلبة على تكنلوجيا المعلومات ، ص 13

[88] https://fibladi.com/

وتركزت الأخرى على تحليل السياسات. قامت بعض الهيئات بتقسيم المواضيع وفقًا لمجالات محددة، مثل تقييم الاستراتيجية أو السياسات الوطنية، أو تحليل الإجراءات لمطابقتها لمنهجية COBIT المعتمدة كما استعانت بعض الهيئات بالقراصنة الأخلاقيين لاختبار فعالية أنظمة السيبراني.

تنوعت المواضيع المعالجة في إطار عمليات التدقيق بشكل كبير، حيث ركزت بعض الهيئات على مجالات ذات أهمية مثل السيبرأمن في الدفاعات البحرية الحرجة وأنظمة إدارة المياه، بينما اهتمت أخرى بقضايا أفقية مثل تنفيذ الاستراتيجية الوطنية للسيبرأمن وحماية البيانات الشخصية والأصول الوطنية للبيانات. جميع الهيئات فحصت قضايا قد تؤثر سلبًا على البنية التحتية أو الخدمات العامة، وذلك رغم هذا التنوع.[89]

في هذا السياق، **تمت عملية تقييم نظام المعلومات لشركة سونلغاز للتوزيع كمحور أساسي من محاور التدقيق على أدائها للفترة من 2019 إلى 2022. يُعتبر الأمن السيبراني أحد أهم مواضيع الرقابة على نظم المعلومات،** وذلك بما يتماشى مع سياق وإطار العمليات الرقابية. تمت عملية التدقيق بواسطة فريق العمل المكلف بتطوير التدقيق على نظم المعلومات لدى مجلس المحاسبة، وهذا بعد الاستعانة به من طرف الغرفة الثامنة المختصة بقطاع الطاقة، وهذا وفقًا لقرار رقم 55 المؤرخ في 17 فيفري 2021، والمتضمن تعيين هذا الفريق، لا سيما تلك المتعلقة بتقديم الاستشارة والمساعدة التقنية اللازمة لهياكل الرقابة، حيث ان هذه العملية مدرجة ضمن رقابة نوعية التسيير ومسجلة ضمن البرنامج السنوي للغرفة الثامنة لسنة 2022. اما بالنسبة للمحور الخاص بالأمن السيبراني فهو من محاور العملية الرقابية.

شركة سونلغاز للتوزيع تُعتبر هدفًا محتملاً للهجمات السيبرانية نظرًا لأهمية دورها في توزيع الطاقة الكهربائية. تأتي أهمية هذه الشركة من دورها الحيوي في توفير الطاقة الكهربائية للمنازل، الشركات، وجميع المنشآت والهيئات العمومية، مما يجعلها جزءًا لا يتجزأ من البنية التحتية الوطنية. تواجه الشركة تحديات كبيرة تتمثل في الحفاظ على أمان أنظمتها الإلكترونية وحمايتها من الاختراقات السيبرانية التي يمكن أن تؤدي إلى توقف في توزيع الكهرباء أو سرقة المعلومات الحساسة مثل بيانات العملاء. من المهم للشركة اتخاذ إجراءات أمنية فعالة للوقاية من هذه المخاطر وتعزيز مستوى حماية أنظمتها ومواردها المعلوماتية.

اعتراف الحكومة الجزائرية بأهمية الأمن السيبراني يعكس تحديات العصر الحديث وتطور التهديدات التي تواجه الأمن الوطني والدولي. فتهديدات الأمن السيبراني تمثل خطرًا جديًا على الأمن القومي، حيث يمكن

[89] Comité de contact des ISC de l'UE, Compendium d'audit: La cyber sécurité dans l'UE et ses États membres, Audit de la résilience des systèmes d'information et des infrastructures numériques critiques aux cyberattaques, décembre 2020

أن تؤدي إلى تعطيل البنية التحتية للدولة وتسبب في خسائر فادحة للاقتصاد والموارد الوطنية. واستجابة لهذه التحديات، اتخذت الحكومة الجزائرية سلسلة من الإجراءات والسياسات لتعزيز الأمن السيبراني[90].

شركة سونلغاز كهيئة رائدة للتوزيع في قطاع الطاقة الجزائري: شركة سونلغاز تعتبر هيئة رائدة في قطاع الطاقة في الجزائر، حيث تقدم خدمات الكهرباء والغاز لأكثر من 11.4 مليون عميل للكهرباء وأكثر من 7.3 مليون عميل للغاز. في عام 2022، بلغ إجمالي إنتاج الشركة من الكهرباء حوالي 85,754 جيجاوات ساعة، مما ساهم في تعزيز التنمية الاقتصادية والاجتماعية في البلاد. تمتلك الشركة بنية تحتية متطورة تضم شبكات نقل وتوزيع كهرباء وغاز ممتدة على نطاق واسع، مما يضمن توفير الخدمات بشكل موثوق وفعال للمجتمعات المخدومة، ويؤكد على دورها الحيوي في تعزيز التنمية في الجزائر. بالإضافة إلى ذلك، فإن تعيين شركة ELIT كشركة فرعية متخصصة في إدارة أنظمة المعلومات يعكس التزام شركة سونلغاز للتوزيع بحماية وتأمين أنظمتها الحاسوبية، مما يعزز قدرتها على التصدي لمخاطر الهجمات السيبرانية وضمان استمرارية الخدمات المقدمة للمستهلكين.[91]

يعتبر مخطط العمل الاستراتيجي حول الأمن السيبراني لشركة سونلغاز جزء أساسي من المخطط استراتيجي 2035، حيث يركز على تعزيز الوعي وتمكين الشركات التابعة لها في مجال الأمن السيبراني. يهدف المخطط إلى تحسين حماية معداتها وشبكاتها وأنظمتها وبياناتها، ويتضمن تطبيق سياسات الأمن القائمة على أفضل الممارسات المتاحة في السوق. يتعاون معه جميع الشركات التابعة لسونلغاز، بقيادة شركة الجزائر لتكنلوجيا المعلومات (ELIT). من أهداف المخطط، تحقيق رد فعل فعّال بشأن الأمن السيبراني وضمان توافر أنظمة المعلومات بشكل مستمر، بالإضافة إلى جعلها أقل عرضة للمخاطر المحتملة. يعتمد تطوير المخطط على تحليل احتياجات الشركات التابعة في مجال الأمن السيبراني والأمن المادي للبنى التحتية التكنولوجية.[92]

[90] في الفترة الأخيرة، اتخذت الحكومة الجزائرية سلسلة من الإجراءات لتعزيز الأمن السيبراني، بما في ذلك تعزيز التشريعات والقوانين ذات الصلة وتوسيع نطاق الوعي بأهميته. كما تم تطوير القدرات التقنية والبشرية لمكافحة التهديدات السيبرانية، بالإضافة إلى إنشاء هيئات مختصة بمتابعة الأمن السيبراني وحماية البيانات. تم أيضًا تحديث المنشآت القاعدية لتعزيز القدرات البشرية والتقنية للتصدي للجرائم الإلكترونية، مع إنشاء مدرسة وطنية عليا للأمن السيبراني ووكالة لأمن الأنظمة المعلوماتية لتعزيز التنسيق والرقابة في هذا القطاع.

[91] https://www.sonelgaz.dz

[92] https://www.sonelgaz.dz/

III. الأهداف والنطاق والمنهجية

❖ الأهداف:

أول خطوة يجب اتخاذها من قبل مدقق نظم المعلومات هي تحديد موضوع الرقابة [93] . يهدف هذا التحديد إلى توضيح مفهوم الأمن السيبراني في سياق الشركة.

بالنسبة لعملية التدقيق على نظم معلومات مؤسسة سونلغاز للتوزيع، تهدف هذه العملية إلى تقييم شامل للنظام المعلوماتي، مع التركيز على جوانب حوكمة أنظمة المعلومات[94].

أما بالنسبة لعملية تقييم نظام معلومات مؤسسة سونلغاز للتوزيع وأمنها السيبراني تستلزم تحديد أهداف التدقيق بدقة ووضوح. يهدف تحديد هذه الأهداف إلى توضيح الغايات المرجوة من العملية الرقابية، ويُمكن اعتبارها كأسئلة يسعى المدققون للإجابة عنها باستناد إلى الأدلة والمعايير المعتمدة.[95] يُسهم تحديد الأهداف في توجيه الجهود الرقابية نحو الجوانب الحيوية لأمن السيبراني، وضمان التوافق مع متطلبات الشركة والقوانين.

تشمل الأهداف الرئيسية لعملية تقييم الأمن السيبراني لمؤسسة سونلغاز للتوزيع ما يلي:

1. التحقق من وجود وتوافق سياسة الأمن السيبراني مع أهداف المؤسسة والمتطلبات القانونية.
2. تقييم مراقبة الأمن السيبراني وفقًا للمعايير الوطنية والتشريعات المتعلقة بأمن المعلومات.
3. تعزيز الرقابة على الأداء من خلال تقييم فعالية الأمان السيبراني ضمن سياق تقييم نظام معلومات المؤسسة.
4. تقييم موثوقية البيانات وسرية ونزاهة النظام وتوفرها.
5. تحديد فعالية آليات الأمان السيبراني وتحديد المخاطر المحتملة المتعلقة بتنفيذها.
6. تقييم إدارة المخاطر والقدرة على استعادة المعلومات بعد الحوادث.

---

[93] ISACA, Auditing Cybersecurity, journal 2019 volume-2O19,p 1

[94] وتحديدًا، فقد كانت الأهداف كالتالي:

- **تقييم المطابقة:** تقدير مدى مطابقة ممارسات إدارة نظام المعلومات للشركة مع المعايير الدولية المعتمدة، بما في ذلك إطار COBIT 4.1وأهداف التحكم في المعلومات والتقنيات ذات الصلة.
- **الفحص التنظيمي:** تقييم تخطيط وتنظيم أنشطة نظام المعلومات، من خلال تحديد النقاط القوية والضعف في العمليات والهيكل التنظيمي.
- **تحليل العمليات:** فحص عمليات اقتناء وتنفيذ أنظمة المعلومات، مع التركيز على كفاءتها وملاءمتها مع احتياجات الشركة.
- **تقييم خدمة الدعم:** تقييم آليات تقديم الدعم والخدمة لأنظمة المعلومات، من خلال التركيز على الممارسات المثلى والمجالات التي تحتاج إلى تحسين.
- **الفحص الأمني**: فحص عمليات المراقبة والتقييم للنظام المعلوماتي، بما في ذلك إدارة المخاطر وقياس الأداء.

[95] وفقًا للدليل الخاص ببرنامج الأمن السيبراني لإجراء فحوصات أداء الأمن السيبراني(GAO-23-104705) ، الصفحة رقم 13.

❖ نطاق التدقيق

تحديد نطاق التدقيق هو خطوة حيوية بعد تحديد أهداف التدقيق. يجب أن تتضمن عملية التخطيط وتحديد النطاق تحديد كافة المجالات والجوانب التي يجب تغطيتها في مجال الأمن السيبراني. يتعلق هذا بتحديد حدود التدقيق، ويمكن أن يشمل ذلك بلدًا معينًا، أو منطقة جغرافية، أو قسمًا أو عملية محددة في المؤسسة، أو جانبًا معينًا من الأمن السيبراني. ومن الأفضل أن يكون هذا التحديد مبنيًا على تقييم المخاطر، حيث يساعد ذلك في تحديد الأولويات والتركيز على المجالات الأكثر أهمية والأكثر عرضة للمخاطر[96].

تركز استراتيجية مجموعة سونلغاز على تطوير "وسائل السيطرة" في مجال نظم المعلومات، الأمر الذي أدى إلى إعادة تنظيم كبير للمسؤوليات في إدارة تقنية المعلومات داخل الشركة. تم تعيين شركة الجزائر لتكنولوجيا المعلومات (ELIT) كشركة فرعية متخصصة مسؤولة عن أنظمة المعلومات، وذلك بفضل تفويض ملكية أنظمة المعلومات لهذه الشركة، مع إعادة تركيز قدرات كل فرع على أنشطته الأساسية.

في هذا الصدد، يتمحور تدقيق مجلس المحاسبة بشكل رئيسي حول الجوانب المتعلقة بحكومة أنظمة المعلومات داخل شركة سونلغاز للتوزيع.[97] كما يهدف التدقيق أيضًا إلى تقييم شرعية وفعالية الاتفاقية التي تحدد شروط وأحكام الخدمات المقدمة من تقوم شركة الجزائر لتكنولوجيا المعلومات (ELIT) لصالح سونلغاز للتوزيع.

عادةً ما يكون نطاق التدقيق في مجال الأمن السيبراني أكثر تقييدًا من تلك المتعلقة بتدقيق تقنية المعلومات العامة، بسبب الطبيعة الفنية والتعقيد المرتفع في الأمن السيبراني. ولتنظيم هذه العملية بشكل فعال، يُفضل تقسيم النطاق الكلي للتدقيق إلى جولات تدقيقية صغيرة قابلة للإدارة، تحتوي على مجموعات محددة من المجالات أو العمليات، مما يساعد على تحديد التركيز وتوزيع الجهود بشكل فعال.[98]

ويشتمل نطاق العملية الرقابية المتعلق بالأمن السيبراني على الترتيبات الداخلية للأمن السيبراني داخل شركة سونلغاز للتوزيع. يتمحور ذلك حول الترتيبات المؤسسية التي تهدف إلى ضمان إدارة الأمن السيبراني بفعالية داخل الشركة، وذلك من خلال تقييم لمدى الاستجابة المؤسسة للتوجيهات الوطنية في مجال الأمن السيبراني من خلال القوانين واللوائح المعمول بها. يتم في هذا السياق دراسة كيفية تنفيذ السياسات والإجراءات الأمنية المطبقة في الشركة ومدى مطابقتها للمعايير الوطنية والدولية للأمن السيبراني.

---

[96] الدليل الخاص ببرنامج الأمن السيبراني ، مرجع سابق

[97] مع التذكير ان نطاق العملية الرقابية المتعلق بتقييم حوكمة نظام المعلومات كان كالتالي: اعتمد الفريق الرقابي في مهمته على إطار COBIT 4.1(أهداف التحكم في المعلومات والتقنيات ذات الصلة). بهدف تحديد المجالات ذات الأهمية الحيوية، قامت المهمة بتحديد مدى تدخلها في المجالات الرئيسية التالية: التخطيط والتنظيم، الاقتناء والتنفيذ، التسليم والدعم، المراقبة والتقييم.

[98] الدليل الخاص ببرنامج الأمن السيبراني ، مرجع سابق

بالإضافة إلى ذلك، يتم تقييم فعالية الإجراءات الأمنية المتخذة في حماية البيانات والمعلومات الحساسة للشركة من التهديدات السيبرانية المحتملة. يتم التركيز على مجالات مثل إدارة الهوية والوصول، وتشفير البيانات، والنسخ الاحتياطي واستعادة البيانات، والتوعية بأمان المعلومات.

تمثلت هذه العناصر المجتمعة إطارًا منهجيًا جد مضبوط لتقييم جودة إدارة نظام معلومات شركة سونلغاز للتوزيع وامنها السيبراني للفترة من 2019 إلى 2022.

❖ المنهجية وادوات العملية الرقابية

تمت المهمة باستخدام منهجية تقييمية صارمة تتضمن عدة خطوات رئيسية، بما في ذلك جمع المستندات، التحليل والتقييم والمقابلات الموجهة مع الأطراف المعنية المختلفة بالإضافة الى الاجتماعات التنسيقية مع الفريق الرقابي. تم تأكيد الاستقلالية والنزاهة لعملية التقييم من خلال الحوار المستمر مع الأطراف المعنية ومشاركتهم في التقييم وصياغة النتائج.

- **صياغة بروتوكول لتبادل المعلومات بين مراجعي نظم المعلومات والمراجعين الآخرين:** عندما تكون مراجعة نظم المعلومات هي جزء من عملية المراجعة، فقد يضمن الجهاز أن يعمل فريق المراجعة ككل بطريقة متكاملة لتحقيق هدف المراجعة الشامل .لتحقيق التكامل الفعال، قد تنظر الأجهزة العليا للرقابة المالية صياغة بروتوكول لتبادل المعلومات بين مراجعي نظم المعلومات والمراجعين الآخرين[99] ، وفي هذا السياق، خلال اجتماع افتتاح العملية الرقابية، قام فريق التدقيق المكلف بتطوير التدقيق على نظم المعلومات بالاتفاق مع الفريق الرقابي للغرفة الثامنة، بالإضافة إلى التنسيق مع الخبير المعين لصياغة طريقة العمل ومنهجية وطريقة تبادل المعلومات والبيانات، حيث تم توثيق جميع هذه المعلومات ضمن محضر الاجتماع كجزء من توثيق عملية التدقيق.
- **النهج القائم على المخاطر:** بمجرد تحديد نطاق التدقيق، يصبح من الضروري تحديد هدف التدقيق، أو لماذا يجرى التدقيق؟ يُنصح من وجهة نظر التدقيق باتباع رؤية مبنية على المخاطر وتحديد الأهداف وفقًا لذلك[100]. ولتمكين الجهاز العليا للرقابة من استخدام إطار تقييم المخاطر بشكل فعال، يتعين عليه الحصول على معلومات عن الجهات المعنية، وغالباً ما تتم هذه المعلومات من خلال إجراء استبيانات موجهة.[101] وفي هذا السياق، قام الفريق الرقابي بإعداد مجموعة من الاستبيانات مستندة إلى إطار COBIT ، حيث يغطي كل استبيان مجالًا معينًا من مجالات الكوبيت ، ومن

---

[99] الدليل الارشادي للانتوساي 5100 ، ص 11

[100] Cooke, I., & Raghu, R. V. (2019, March 1). IS Audit Basics: Auditing Cybersecurity. IS Audit Basics. Retrieved from [https://www.isaca.org/]

[101] دليل الرقابة على نظم المعلومات 5300 ص 19، 20

خلال تحليل الإجابات، والاجتماعات مع إدارة نظم المعلومات في الشركة، والمعلومات التوضيحية الإضافية، تم تحديد نطاق المخاطر ودرجتها.

- **اعتماد منهجية للتدقيق وفق إطار الرّقابة على تقنية المعلومات كوبيت** (COBIT).

يُعرّف إطار العمل كوبيت (COBIT) بأنه إطار حوكمة تقنية المعلومات المُعترَف به دولياً، ويُسمّى أيضاً الإطار/ النموذج المرجعي، للأمن ولضمان استغلال تقنية المعلومات بالشكل الأمثل، يُستخدم لتحسين أداء الأعمال بإطار متوازن لخلق قيمة لتقنية المعلومات وخفض المخاطر المحتملة منها.

ويعتبر إطار العمل COBIT إطار عمل متكامل لقدرته على التوافق أو الاندماج مع أحدث الأُطر والمعايير ذات الصلة، مثل : CMMI Prince 2، ITIL , ISO 38500 , ISO 27001، ISO 9001، ويعد الوسيلة الشاملة لتغطية المنشأة بشكل متكامل مع إطار الإدارة والحوكمة، كما أنه يوفر أساس قوي لدمج الأُطر والمعايير والممارسات الأُخرى بشكل فعّال.

ووعيا منه بالأهمّية القصوى التي تكتسيها هذه الأدوات، تبنى فريق العمل إطار الكوبيت من خلال إدماجه ضمن أبرز أهدافه المسطرة خلال سنة 2022.

- **الاستعانة بالخبرة المنصوص بموجب أحكام المادة 58 من الأمر 95-20 المعدل و لمتمم، من خلال تعيين خبير في تكنولوجيا المعلومات:**

في إطار ممارسة فريق العمل المكلف بتطوير التدقيق على نظم لمهامه المرتبطة بتقديم الاستشارة والمساعدة التقنية اللازمة لهياكل الرقابة، ومن أجل تقديم خدمات ذات جودة قام فريق العمل خلال سنة 2022 باللجوء إلى الخبرة عملا بأحكام المادة 58 من الأمر 95-20 المعدل والمتمم، وفي هذا الصدد تم إبرام اتفاقية مع خبير في مجال تكنولوجيا المعلومات خلال الفترة من 11 نوفمبر 2022 إلى 11 أفريل 2023، اشتملت هذه الاتفاقية على ضمان المهام التالية:

- شرح وتفسير الوثائق ذات الطابع التقني،
- إنجاز الاختبارات الفنية،
- تكوين ومرافقة (coaching) فريق العمل أثناء تقديم للاستشارة والمساعدة التقنية للمهمتين الرقابيتين النموذجيتين للغرفة الأولى والثامنة التي تم التطرق إليها أعلاه.

- **الاستبيان والاستعراض المكتبي:**

تم اعتماد مجموعة متنوعة من مصادر البيانات النوعية والكمية من قبل فريق العمل الرقابي، الذي يتألف من قضاة الغرفة الثامنة والفريق الرقابي والخبير الخارجي، لضمان دقة النتائج وموثوقيتها. شملت هذه

المصادر الاستبيانات والمراجعات المكتبية، حيث جمع الفريق المعلومات من خلال استبيانات أُرسلت إلى إدارة نظم المعلومات في الشركة. تم تحليل المكونات الرئيسية للبيانات المتاحة، بما في ذلك السياسات والقرارات الإدارية والاستراتيجيات المؤسسية والتقنيات المستخدمة وسياسات الأمن والإجراءات التشغيلية والتقارير الداخلية والخارجية. كما تم إجراء استعراض نقدي للوثائق الثبوتية والقدرات المؤسسية والتشغيلية في مجال الأمن السيبراني، مع مراعاة الجوانب القانونية ذات الصلة، بما في ذلك خرائط البيانات وهندسة نظم المعلومات.

- **معايير التدقيق (منهجية العملية الرقابية المبنية على الكوبيت)**

يجب على مدققي تكنولوجيا المعلومات تحديد معايير التقييم التي يجب أن تكون قابلة للقياس وموثوق بها، وأن تتماشى مع أهداف ومواضيع التدقيق المحددة في هذه المرحلة[102]. وفي هذا الصدد اعتمد الفريق الرقابي على الإطار الدولي COBIT 4.1 أهداف التحكم في المعلومات والتقنيات ذات الصلة. بهدف استهداف المجالات ذات الأهمية الحاسمة، حددت المهمة مدى تدخلها في المجالات الرئيسية التالية، وفقًا لإطار COBIT 4.1:

-التخطيط والتنظيم (PO1) إلى (PO10)

-الاستحواذ والتنفيذ (AI1) إلى (AI7)

-التسليم والدعم (DS1) إلى(DS13)

-المراقبة والتقييم (ME1) إلى(ME4)

قامت الفريق الرقابي بدمج هذه العناصر لتحديد إطار منهجي دقيق لتقييم جودة إدارة نظام المعلومات لشركة سونلغاز للتوزيع للفترة من 2019 إلى 2022.وفيما يخص تقييم إدارة الأمن السيبراني في للشركة فقد تم التركيز على العمليات والمجالات ذات الصلة التالية:

❖ **تحديد خطة استراتيجية لتكنولوجيا المعلومات:(PO1)**

- مراجعة وتقييم الاستراتيجية الحالية لتكنولوجيا المعلومات وفحص مدى ملاءمتها لأهداف الأمن السيبراني.
- تطوير أو تحسين استراتيجية تكنولوجيا المعلومات بما يضمن تكاملها وتوافقها مع أهداف الأمن السيبراني.
- التحقق من تضمين جوانب الأمن السيبراني كعنصر أساسي في خطط تكنولوجيا المعلومات المستقبلية.

[102] دليل مجموعة العمل حول تدقيق تكنولوجيا المعلوماتISSAI.ORG -

❖ **تقييم وإدارة مخاطر تكنولوجيا المعلومات:(PO9)**

- تحليل وتقييم التهديدات السيبرانية المحتملة وتصنيفها وفقًا للأولويات.
- مراجعة وتقييم التدابير الأمنية المطبقة للتصدي للتهديدات السيبرانية.
- تقييم جاهزية المؤسسة للتعامل مع حالات الطوارئ السيبرانية وفقًا للسيناريوهات المختلفة.

❖ **الحصول على وصيانة تطبيقات البرمجيات:(AI2)**

- التحقق من مطابقة عمليات الحصول على وصيانة تطبيقات البرمجيات لمتطلبات الأمن السيبراني.
- اختبار الثغرات الأمنية وتقييم التدابير المتخذة للحد من المخاطر السيبرانية المحتملة.
- التأكد من تنفيذ المعايير الأمنية المعتمدة في تطوير وصيانة التطبيقات.

❖ **الحصول على وصيانة البنية التحتية التكنولوجية:(AI3)**

- التأكد من تطبيق ممارسات الأمان السيبراني في الحصول على وصيانة البنية التحتية التكنولوجية.
- تقييم الأنظمة والبنية التحتية لضمان تحقيق مستويات الأمان المطلوبة.
- التحقق من تحديثات الأمان وتنفيذ الضوابط الوقائية لمواجهة التهديدات السيبرانية الجديدة.

❖ **تحديد وإدارة مستويات الخدمة:(DS1)**

- تحديد متطلبات الأمان لمستويات الخدمة في مجال الأمن السيبراني.
- التحقق من تنفيذ وصيانة إجراءات الأمان المطلوبة للحفاظ على مستويات الخدمة.
- مراجعة وتحسين إجراءات الخدمة لتعزيز الأمان وتحقيق الامتثال.

❖ **ضمان أمان الأنظمة:(DS5)**

- تقييم فعالية إجراءات أمان الأنظمة والتأكد من توافقها مع متطلبات الأمان السيبراني.
- مراجعة وتحسين الضوابط الوقائية لضمان حماية الأنظمة من الهجمات السيبرانية.
- التحقق من التزام الموظفين بسياسات الأمان وتعزيز الوعي الأمني داخل المؤسسة.

- **العمل مع الجهة الخاضعة للتدقيق**

يجب أن يتم إطلاع الجهة الخاضعة للتدقيق على مجال التدقيق، وأهدافه، ومعايير التقييم الخاصة به والتيس ت ناقش إذا تطلب الامر ذلك، ويمكن لجهاز الرقابة الأعلى إذا لزم الأمر، أن يخاطب الجهة الخاضعة للتدقيق وأن يصف أعمال التدقيق المطلوبة، يجب على جهاز الرقابة الأعلى التأكيد على ضرورة

التعاون والدعم من الجهة الخاضعة للتدقيق لاستكمال عملية التدقيق، بما في ذلك الاطلاع على السجلات والمعلومات، سواء كانت يدوية أو إلكترونية103.

في سياق الاتصال مع الكيانات المراقبة خلال مرحلة تخطيط العملية الرقابية، نظرًا لعدم وجود تجربة سابقة لمؤسسة سونلغاز للتوزيع في التعامل مع مجال تقييم الأداء للمجالس المحاسبية، تم عقد اجتماع افتتاح في 29 سبتمبر 2022. كان هدف هذا الاجتماع توضيح النهج المنهجي الذي اعتمده فريق التدقيق والإجراءات التي ستتبعها طوال المهمة. تم أيضًا تقديم منهجية التدقيق المستندة إلى الإطار الدولي COBIT 4.1 ، ومنهجية التدقيق المبنية على المخاطر.

حافظ فريق المراقبة على حوار بناء مع أصحاب المصلحة طوال الاجتماع، من خلال مشاركة الملاحظات ووجهات النظر الأولية بانتظام كما تم صياغتها وتقييمها. تم إجراء هذا الحوار بحفظ استقلالية ونزاهة الرقابة. في النهاية، تم قبول الهيئة المراقبة لمنهجية العمل الرقابي، ولتعزيز العمل الرقابي تم شرح وتسليم أول استبيان حول المحور الأول من عملية التقييم "التخطيط والتنظيم".

- **الاستفادة من التعاون الدّولي:**

في إطار تبادل الخبرات مع منظمات دولية في مجال رقابة تقنيات المعلومات، عقد مجلس المحاسبة شراكة مع الهيئة التطوعية للخدمات المالية. قدمت الهيئة المرافقة اللازمة لهذه المهمة الرقابية، حيث تمت مناقشة الأهداف والمحاور الرئيسية ومنهجية التدقيق ونطاقه. كما تمت مناقشة استبيانات التدقيق وعرض النتائج الأولية للخبير الدولي. استفاد مجلس المحاسبة الجزائري من 8 اجتماعات خلال مرحلة التخطيط للعملية الرقابية، حيث تم استعراض منهجيات متنوعة بما في ذلك منهجية المعهد الوطني للمعايير والتقنية (NIST) الأمريكي، وتم تنفيذ منهجية تقييم المخاطر وفقًا لإطار العمل COBIT 4.1، نظرًا لتوافق موضوعات وأهداف الرقابة مع هذا الإطار.

IV. مراحل ومجريات تنفيذ العملية الرقابية

كان التدقيق عبارة عن تدقيق أداء يستند إلى معايير ومبادئ الانتوساي(INTOSAI) ، وكان السؤال الرئيسي للتدقيق هو ما إذا كانت مؤسسة سونلغاز للتوزيع قد أدارت الأمن السيبراني بشكل فعّال. تضمنت المراحل الرئيسية لتنفيذ التدقيق ما يلي: (1) جمع الأدلة الأولية، (2) وضع اللمسات الأخيرة على خطة التدقيق، (3) مواصلة جمع البيانات وتحليلها، و(4) تحديد نتائج التدقيق. الفترة الخاضعة للعملية الرقابية كانت من 2019 إلى 2021.

103 دليل مجموعة العمل حول تدقيق تكنولوجيا المعلومات ، مرجع سابق ص 25 .

بدأ التدقيق في أكتوبر 2022 وتم تقديم 4 تقارير خبرة للغرفة الثامنة خلال الفترة من فبراير إلى أكتوبر 2023، تماشياً مع وتيرة إنجاز مهمة الرقابة "تقييم أداء مؤسسة سونلغاز للتوزيع". كان فريق التدقيق مكونًا من قاضٍ مراجع، قاضٍ مساعد، رئيس فريق عمل التدقيق على نظم المعلومات، بالإضافة إلى خبير تكنولوجيا المعلومات الذي تم التعاقد معه. قام فريق التدقيق بإعداد خطة التدقيق، وطلب الوثائق والاستبيانات المتعلقة بحوكمة نظم معلومات الشركة في مجالاتها الأربع كما تم التطرق إليه سابقاً.

❖ جمع الأدلة الأولية

بدأ فريق التدقيق بإعداد خطة التدقيق التي تشمل جميع جوانب حوكمة نظم معلومات الشركة في مجالاتها الأربع. كخطوة أولى، طلب الفريق الوثائق والاستبيانات ذات الصلة. تم تنفيذ أكثر من 8 مقابلات واختبار تطبيقين متعلقين بالمالية والمحاسبة. استخدم المدققون إطار COBIT 4.1 وأهداف التحكم في المعلومات والتقنيات ذات الصلة، ومعيار ISO/IEC 27001 لتقنية المعلومات وتقنيات الأمان وأنظمة إدارة أمان المعلومات – متطلبات الضوابط.(2020)

1. تصنيف الأدلة:

الأدلة المادية:

- تم جمع الأدلة المادية من خلال الفحص المباشر من طرف الفريق الرقابي، زيارة مختلف المديريات والمصالح، وملاحظة الأشخاص والممتلكات والعمليات.
- سُجلت الأدلة في مذكرات ملخصة، أخذ صور التقاط الشاشة، رسوم بيانية، خرائط، أو عينات مادية.
- تمت مراعاة الحاجة إلى إذن من المنظمة قبل جمع الأدلة المادية، مثل أخذ صور التقاط الشاشة لبعض التطبيقات.

الأدلة الوثائقية:

- تشمل الأدلة الوثائقية نسخ السياسات والإجراءات، نتائج الفحوصات السابقة، لقطات الشاشة، سجلات التدريب، سجلات الأحداث والوصول، جداول البيانات، مقتطفات قواعد البيانات، ومعلومات الأداء التي طورتها المنظمة.
- أمثلة إضافية للأدلة الوثائقية التي تم جمعها :
- قوائم الجرد لأنظمة المعلومات الرئيسية.
- تقارير التدقيق ذات الصلة.

- خطط أمان النظام.
- خطط الطوارئ واستعادة الكوارث.
- تقارير التقييم الأمني.
- مفاهيم العمليات.
- مخططات الشبكة.
- اتفاقيات مع الكيانات الخارجية.
- حزم ترخيص النظام.
- قوائم الجرد لبعض أجهزة الشبكة.
- قوائم الإعفاءات النشطة من الضوابط الأمنية.

الأدلة الاستشهادية:

- تم جمع الأدلة الشهاداتية من خلال الاستفسارات، المقابلات ، المنتديات العامة، أو الاستبيانات.
- تم تقييم الأدلة المُجمعة لضمان كفايتها وملاءمتها، بما في ذلك التأكد من أنها ذات صلة، صحيحة، وموثوقة.

بهذا النهج المنظم، تمكن فريق التدقيق من جمع الأدلة اللازمة لتقييم فعالية إدارة الأمن السيبراني لدى مؤسسة سونلغاز للتوزيع بشكل دقيق وشامل.

2. تقييم موثوقية البيانات:

تُعتبر موثوقية البيانات عاملاً حاسمًا في عمليات الرقابة على نظام معلومات مؤسسة سونلغاز للتوزيع وأمنها السيبراني. يشمل هذا التقييم عدة مراحل أساسية تأخذ في الاعتبار أهمية البيانات وقوة الأدلة المؤكدة ومخاطر استخدام البيانات، إلى جانب الدروس المستفادة خلال التقييم.

قبل تنفيذ خطة الرقابة، قام الفريق بإجراء اختبارات أولية كافية للبيانات الأساسية لضمان توفرها وموثوقيتها. فالتوفر ضروري؛ إذ إن عدم توفر البيانات اللازمة أو عدم موثوقيتها يستدعي إعادة تقييم الأهداف. وتعد الموثوقية أساسية، حيث إن البيانات غير الموثوقة لا يمكن الاعتماد عليها في دعم الاستنتاجات والتوصيات. خلال فترة الاختبار، تم اختبار 30 مجالًا من مجالات COBIT 4.1 من إجمالي 34. بعد جمع ما يكفي من المعلومات والأدلة. وفي هذا الصدد قام خبير تكنولوجيا المعلومات باعداد أربع تقارير جزئية في شكل مصفوفات مخاطر.

❖ انهاء خطة التدقيق

قبل الانتهاء من خطة الرقابة، قام الفريق بتعديل وتحديث الأهداف، والنطاق، وإجراءات الرقابة، والجدول الزمني، وكذلك توجيه الموارد بناءً على النتائج المستخلصة من التقييم الأولي.

❖ متابعة جمع وتحليل البيانات:

بعد تحيين خطة التدقيق، قام الفريق الرقابي بجمع وتحليل البيانات وفقًا للخطة الموضوعة. عند تحليل الأدلة، خاصةً فيما يخص تقييم الضوابط، تم استخدام مزيج من الفحوصات، المقابلات، والاختبارات.

- **الفحص والتقييم:**

في سياق تقييم نظام معلومات مؤسسة سونلغاز وأمنها السيبراني، تشمل الفحوصات مراجعة، فحص، ملاحظة، متابعة، دراسة، أو تحليل واحد أو أكثر من عناصر التقييم (مثل المواصفات، الآليات، أو الأنشطة). تهدف هذه الفحوصات إلى تسهيل فهم المدققين للأنظمة المعقدة، توضيح النقاط الغامضة، والحصول على الأدلة اللازمة لدعم نتائج التدقيق.

- **الاستبيان والاستعراض المكتبي:**

تم اعتماد مجموعة متنوعة من مصادر البيانات النوعية والكمية من قبل فريق العمل الرقابي، الذي يتألف من قضاة الغرفة الثامنة والفريق الرقابي والخبير الخارجي، لضمان دقة النتائج وموثوقيتها. شملت هذه المصادر الاستبيانات والمراجعات المكتبية، حيث جمع الفريق المعلومات من خلال استبيانات أُرسلت إلى إدارة نظم المعلومات في الشركة. تم تحليل المكونات الرئيسية للبيانات المتاحة، بما في ذلك السياسات والقرارات الإدارية والاستراتيجيات المؤسسية والتقنيات المستخدمة وسياسات الأمن والإجراءات التشغيلية والتقارير الداخلية والخارجية. كما تم إجراء استعراض نقدي للوثائق الثبوتية والقدرات المؤسسية والتشغيلية في مجال الأمن السيبراني، مع مراعاة الجوانب القانونية ذات الصلة، بما في ذلك خرائط البيانات وهندسة نظم المعلومات.

- **المقابلات والاجتماعات:**

بالإضافة إلى ذلك، قام الفريق الرقابي بإجراء مقابلات مع مجموعة متنوعة من الأشخاص، بما في ذلك مدير العصرنة، مدير نظم المعلومات، ومسؤولي الهياكل التابعة، بالإضافة إلى ممثلي شركة الجزائر لتكنلوجيا المعلومات (ELIT)، بما في ذلك المسؤولين عن تكنولوجيا المعلومات والأمن السيبراني، ومدير التدقيق الداخلي، ومدير المالية والمحاسبة والهياكل التابعة له، ومستعملي التطبيقات الخاصة بالمالية والمحاسبة. كما تم استكشاف مواضيع محددة غير مشمولة في الاستبيانات. وقد قدمت شركة الجزائر لتكنلوجيا المعلومات (ELIT) معلومات حول قدرات مؤسسة سونلغاز للتوزيع في مجال

الأمن السيبراني. كما استفاد الفريق الرقابي من التركيز على دراسة عدد من المديريات الجهوية وموظفي نظم المعلومات الأمن، وتعرفوا من خلالها على عمليات النظم المعلومات وكيفية تنفيذ السياسات الأمنية. هذه المقابلات والاجتماعات كانت فرصة لجمع المعلومات المحورية والحصول على رؤى مفيدة حول أداء الجهات المعنية في مجال الأمن السيبراني وتحديد النقاط القوية والضعف.

- **الاختبارات**

في سياق تقييم نظام معلومات مؤسسة سونلغاز وأمنها السيبراني، شملت الاختبارات نشاط واحد أو أكثر من عناصر التقييم مثل الأنشطة أو الآليات، تحت ظروف محددة لمقارنة الحالة الفعلية بالحالة المطلوبة أو السلوك المتوقع. يهدف هذا النشاط إلى إجراء تحقيقات دقيقة واختبارات فنية خاصة على جوانب محددة، وذلك لتحقيق فهم أعمق وتحقيق التوضيح اللازم، والحصول على الأدلة الضرورية لدعم النتائج.

٧. تقرير نتائج التدقيق

تم تقديم أربع تقارير خبرة للغرفة الثامنة خلال الفترة من فبراير إلى أكتوبر 2023، بشكل مصفوفات مخاطر. تم التنسيق مع الفريق الرقابي للغرفة الثامنة طوال جميع مراحل العملية الرقابية ، و كانت اعداد جميع مخرجات العملية الرقابية من خلال التنسيق المستمر مع الغرفة الثامنة و كذلك مع الهيئة الخاضعة من الاجل لوصول الى نتائج رقابية ذات جودة ، كما تم تكليف الفريق الرقابي للغرفة الثامنة بجمع ادلة الاثبات الكافية من اجل منح الحجة الاثباتية للنتائج الرقابية المتوصل اليها ، بالنسبة لصياغة التقرير النهائي هو من صلاحيات القاض المقرر الذي سيقوم بادراج النتائج المتوصل اليها ضمن تقريره حسب شكل و موضوع تقريره النهائي ، كما تم فتح الملف الرقابي للمهمة في شكل الكتروني ، و ذلك بعد الاستعانة بتطبيق الفريسكو(Alfrisco).

بعد تنفيذ عملية التدقيق، قام الفريق الرقابي بالخطوات التالية:

❖ مراجعة النتائج مع المنظمة المدققة

عند الانتهاء من عملية التدقيق ، قام الفريق ب تقديم بيان بالحقائق للمنظمة المدققة يصف نتائج التدقيق من خلال مراسلات رسمية و اجتماعات تنسيقية . حيث قامت مديرية تكنلوجيا المعلومات بالتعليق على هذا البيان ومناقشته مع الفريق الرقابي وتقديم ملاحظات ووثائق. خلال هذه الفترة، يتم مناقشة أي مسائل بناء على هذا الأساس تم تحديث مسودة التقرير وفقًا لذلك.

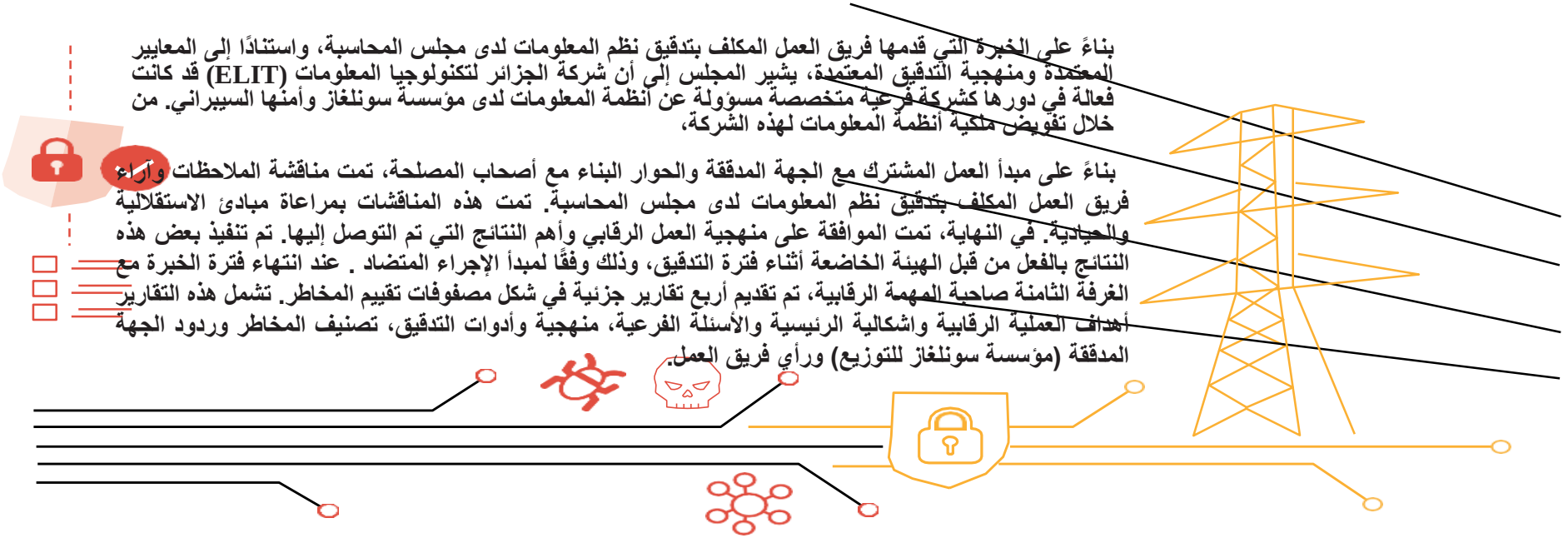
❖ **إعداد مسودة التقرير**

قام الفريق الرقابي بعرض مسودة النتائج بطريقة واضحة ومفهومة. تصمنت هذه المسودة أهداف التدقيق، النطاق، المنهجية، النتائج، الاستنتاجات. حيث تم دمج المعلومات المقدمة من المنظمة المدققة استنادًا إلى بيان الحقائق بشكل مناسب. بالإضافة إلى ذلك، كما تم استخدام الرسوم البيانية والجداول لتعزيز وضوح التقرير وقراءته.

❖ **الحصول على آراء المنظمة المدققة على مسودة التقرير**

في هذا الصدد تم مناقشة مسودة التقرير مع النتائج للمراجعة والتعليق من قبل المسؤولين في المنظمة المدققة مما ساعد في تطوير تقرير عادل، شامل، وموضوعي. من خلال التعليقات المكتوبة من هيئة الخاصعة، كما تم قبول التعليقات الشفهية.

VI. ابداء راي مجلس المحاسبة



بناءً على الخبرة التي قدمها فريق العمل المكلف بتدقيق نظم المعلومات لدى مجلس المحاسبة، واستنادًا إلى المعايير المعتمدة ومنهجية التدقيق المعتمدة، يشير المجلس إلى أن شركة الجزائر لتكنولوجيا المعلومات (ELIT) قد كانت فعالة في دورها كشركة فرعية متخصصة مسؤولة عن أنظمة المعلومات لدى مؤسسة سونلغاز وأمنها السيبراني. من خلال تفويض ملكية أنظمة المعلومات لهذه الشركة،

بناءً على مبدأ العمل المشترك مع الجهة المدققة والحوار البناء مع أصحاب المصلحة، تمت مناقشة الملاحظات وآراء فريق العمل المكلف بتدقيق نظم المعلومات لدى مجلس المحاسبة. تمت هذه المناقشات بمراعاة مبادئ الاستقلالية والحيادية. في النهاية، تمت الموافقة على منهجية العمل الرقابي وأهم النتائج التي تم التوصل إليها. تم تنفيذ بعض هذه النتائج بالفعل من قبل الهيئة الخاضعة أثناء فترة التدقيق، وذلك وفقًا لمبدأ الإجراء المتضاد . عند انتهاء فترة الخبرة مع الغرفة الثامنة صاحبة المهمة الرقابية، تم تقديم أربع تقارير جزئية في شكل مصفوفات تقييم المخاطر. تشمل هذه التقارير أهداف العملية الرقابية واشكالية الرئيسية والأسئلة الفرعية، منهجية وأدوات التدقيق، تصنيف المخاطر وردود الجهة المدققة (مؤسسة سونلغاز للتوزيع) ورأي فريق العمل.

VII. النتائج المتوصل إليها

أول خطوة يجب اتخاذها من قبل مدققي نظم المعلومات هي تحديد موضوع الرقابة، وهذا يسهل فهم مفهوم الأمن السيبراني في سياق شركة سونلغاز للتوزيع. يتيح تحديد موضوع الرقابة للمدققين تركيز جهودهم وتحديد الجوانب الرئيسية التي يجب التركيز عليها في تقييم أمن المعلومات وتقنياته، وهو أمر أساسي لضمان فعالية العملية الرقابية. يمكن تلخيص أهم النتائج التي توصلت إليها الدراسة الميدانية كالتالي:

- اختيار المحور الأساسي للرقابة: اختار مجلس المحاسبة الجزائري تقييم نظام معلومات شركة سونلغاز للتوزيع وأمنها السيبراني كمحور أساسي للرقابة، بهدف تقييم جاهزية الشركة كمُشغل رئيسي في قطاع الطاقة بالجزائر.
- تأثير خبير نظم المعلومات وأمن المعلومات: أظهرت النتائج أن ضمان إدراج خبير في نظم المعلومات وأمن المعلومات كان له تأثير إيجابي على جودة النتائج الرقابية.
- أهمية معايير التدقيق: كان اختيار معايير التدقيق ذات أهمية بالغة لمراجعة استعداد الشركة للتصدي للهجمات السيبرانية.
- الحاجة لخبراء إضافيين في القرصنة الإلكترونية: تشير النتائج إلى ضرورة إدراج خبراء إضافيين في مجال القرصنة الإلكترونية واختبار الاختراق في فريق التدقيق.
- ضرورة تحديد موضوع الرقابة بدقة: من الجوانب الرئيسية التي تم التركيز عليها في الدراسة، ضرورة تحديد موضوع الرقابة بعناية.
- ضرورة التنسيق بين الأقسام المختلفة: تحدثت النتائج عن ضرورة تعزيز الاتصال والتنسيق بين الأقسام المختلفة في الشركة.
- تقديم التدريب المناسب: كما تشير النتائج إلى ضرورة تقديم التدريب المناسب للموظفين لزيادة فهمهم وقدراتهم في مجال الأمن السيبراني.
- تحديات إدارة التطبيقات: تحدثت الدراسة عن تعقيد إدارة التطبيقات وضرورة تقييمها بشكل دقيق لضمان توافقها مع متطلبات الأمان السيبراني والوظيفية.
- أمان البيانات وحماية الخصوصية: واحدة من التحديات الرئيسية التي تواجه عمليات الرقابة على نظم المعلومات، خاصةً في ظل التهديدات السيبرانية المتزايدة.

- إدارة تعقيد نظام المعلومات: يجب إدارة تعقيد نظام المعلومات بعناية لتجنب تأثيرها السلبي على عمليات الشركة، وهو أمر يتطلب رقابة فعالة.
- بعد الانتهاء من التدقيق، يتم مراجعة النتائج مع المؤسسة المدققة وتطوير مسودة التقرير، والحصول على آرائهم حولها. ينبغي للتقرير النهائي أن يعرض الأهداف والنطاق والمنهجية والنتائج والاستنتاجات والتوصيات بشكل واضح ومفهوم، مستخدمًا الرسوم البيانية والجداول لتعزيز قابلية القراءة. كما يجب مراجعة حساسية التقارير لضمان عدم إفشاء المعلومات الحساسة. تُصدر التقارير النهائية بعد مراجعة آراء المؤسسة المدققة ومعالجة التعليقات بشكل مناسب.

خاتمة

تتطلب البيئة الرقمية الحديثة تقديم جهود مستمرة لتعزيز الرقابة على نظم المعلومات والأمن السيبراني من قبل الهيئات العليا للرقابة المالية والمحاسبة. يتعين على هذه الهيئات التكيف مع التحديات المستمرة التي تطرأ مع تقدم التكنولوجيا، وتطوير استراتيجيات الرقابة والتدقيق لمواجهة التهديدات السيبرانية المتزايدة.

توضح الدراسة أهمية فهم المفاهيم الأساسية للرقابة على نظم المعلومات والأمن السيبراني، وتحديد الأهداف الرئيسية لتدقيق تكنولوجيا المعلومات وأهميته. كما تسلط الضوء على الجهود التي تبذلها الجزائر في تعزيز الحوكمة السيبرانية وتطوير استراتيجيات الأمن السيبراني.

في ظل تعقيدات وانتشار التهديدات السيبرانية، يصبح تدقيق تكنولوجيا المعلومات ذا أهمية بالغة لحماية بيئة تكنولوجيا المعلومات، وضمان الامتثال التنظيمي، وتقليل مخاطر الهجمات السيبرانية. ومع تطور المشهد الرقمي، سيلعب النهج الاستباقي لتدقيق تكنولوجيا المعلومات دورًا حيويًا في مواجهة تحديات تكنولوجيا المعلومات في المستقبل.

تلعب الأجهزة العليا للرقابة المالية والمحاسبة دورًا محوريًا في تعزيز الرقابة على نظم المعلومات في ظل التحول الرقمي. من خلال تطوير التشريعات، وإنشاء وحدات متخصصة، وتدريب الكوادر، وتبني أفضل الممارسات والمعايير الدولية، تساهم هذه الأجهزة في ضمان الشفافية، والكفاءة، والأمن السيبراني .

من المهم أيضًا فهم منهجيات تدقيق الأمن السيبراني وتطبيقها بفعالية، مع التركيز على التحديات التي تواجه الهيئات العليا للرقابة المالية. يجب على المدققين تطوير معرفتهم بتكنولوجيا المعلومات واستخدام الحلول التكنولوجية المساعدة لتحقيق أهداف الرقابة والتدقيق بنجاح.

باختصار، يتطلب تأمين نظم المعلومات وضمان أمنها التعاون الوثيق بين الهيئات العليا للرقابة والمؤسسات الحكومية والقطاع الخاص. إن تعزيز الرقابة على نظم المعلومات والأمن السيبراني يسهم في تحقيق الشفافية والكفاءة والأمان السيبراني، مما يؤدي إلى بناء نظام حكومي واقتصادي قائم على البيانات يخدم المصلحة العامة بفعالية وكفاءة.

النتائج

بناءً على الفرضية الرئيسية والفرضيات الفرعية المقترحة، يُظهر أن تطبيق أساليب وأدوات الرقابة على نظم المعلومات والأمن السيبراني يلعب دورًا حيويًا في تحسين كفاءة الرقابة المالية والمحاسبة، وتعزيز قدرتها على مواجهة التحديات الحالي، كما توصلت الدراسة الى النتائج التالية :

- **قبول الفرضية الفرعية الأولى:** إذا قامت الأجهزة العليا للرقابة المالية والمحاسبة بفهم وتطبيق المفاهيم الأساسية للرقابة على نظم المعلومات والأمن السيبراني، فستكون أكثر قدرة على مواجهة التحديات الحالية بفعالية.
- **قبول الفرضية الفرعية الثانية** :إذا تبنت الأجهزة العليا للرقابة المالية والمحاسبة خطوات رئيسية ومنهجية عملية فعالة في تقييم نظم المعلومات والأمن السيبراني، فسيؤدي ذلك إلى تعزيز كفاءة عمليات التدقيق وتحقيق الأهداف الرقابية بكل فعالية ونجاعة.
- **قبول الفرضية الفرعية الثالثة** :إذا عملت الأجهزة العليا للرقابة المالية والمحاسبة على تحسين الإجراءات والسياسات المتعلقة بتدقيق نظم المعلومات والأمن السيبراني، فسيتم بناء نظام حكومي آمن وموثوق يتماشى مع المعايير الدولية ويعزز الأمن السيبراني الوطني.
- **قبول الفرضية الفرعية الرابعة** :إذا تم تعزيز التنسيق والتعاون بين الهيئات الرقابية المختلفة، فسيزيد ذلك قدرتها على مكافحة التهديدات السيبرانية بشكل أكثر فعالية.

النتائج العامة

يمكن استعراض بعض النتائج الهامة ذات الصلة بالموضوع وذلك على النحو التالي:

1. .توضح الدراسة أهمية تطبيق أساليب وأدوات الرقابة على نظم المعلومات والأمن السيبراني في تعزيز كفاءة الرقابة المالية والمحاسبة.
2. .يلعب التحسين المستمر لاستراتيجيات الرقابة والتدقيق دورًا حيويًا في مواجهة التهديدات السيبرانية المتزايدة وتأمين بيئة تكنولوجيا المعلومات.
3. .تسهم الأجهزة العليا للرقابة المالية والمحاسبة في تطوير الحوكمة السيبرانية وضمان الشفافية والكفاءة والأمن السيبراني.

4 .يتطلب تأمين نظم المعلومات وضمان أمنها التعاون الوثيق بين الهيئات العليا للرقابة والمؤسسات الحكومية والقطاع الخاص.

5 .**تعزيز التعاون والتنسيق:** وجود تنسيق وتعاون فعال بين الهيئات الرقابية المختلفة يعزز قدرتها على مكافحة التهديدات السيبرانية بشكل أكثر فاعلية، مما يسهل تبادل المعلومات وتحسين الفهم المشترك للتهديدات السيبرانية.

6 .**تحقيق الامتثال التنظيمي:** تدقيق تكنولوجيا المعلومات يساعد في ضمان الامتثال للتشريعات والمعايير الأمنية السائدة، مما يحسن الوضع الأمني ويسهم في بناء نظام حكومي آمن وموثوق.

7 .**دور الهيئات الرقابية:** تلعب الأجهزة العليا للرقابة المالية والمحاسبة دورًا حيويًا في اقتراح وتطوير التشريعات، إنشاء وحدات متخصصة، وتبني أفضل الممارسات والمعايير الدولية، مما يسهم في ضمان الشفافية، الكفاءة، والأمن السيبراني.

8 .**النهج الاستباقي:** تبني النهج الاستباقي في تدقيق تكنولوجيا المعلومات يلعب دورًا محوريًا في مستقبل إدارة مخاطر تكنولوجيا المعلومات، مما يساعد في مواجهة التهديدات السيبرانية المتزايدة بفعالية.

من خلال هذه النتائج، يتضح أن الجهود المبذولة لتعزيز الرقابة على نظم المعلومات والأمن السيبراني تساهم بشكل كبير في حماية البيانات وضمان استمرارية العمليات الحكومية بشكل سلس وموثوق، مما يعزز الثقة في النظام الحكومي والاقتصادي القائم على البيانات.

التوصيات:

بناءً على النتائج السابقة، يمكن تلخيص أهم التوصيات على النحو التالي:

1. تعزيز التدريب والتطوير المستمر للمدققين والمراقبين لتعزيز فهمهم ومعرفتهم بأحدث التقنيات والتهديدات السيبرانية.
2. تعزيز التعاون وتبادل المعلومات بين الهيئات الرقابية المختلفة لتحسين قدرتها على مكافحة التهديدات السيبرانية.
3. تعزيز الحوكمة السيبرانية على مستوى الحكومة من خلال وضع وتنفيذ إطار تشريعي وتنظيمي قوي.

4. تشجيع المؤسسات على تبني أفضل الممارسات في مجال أمن المعلومات والامتثال التنظيمي.
5. تعزيز الوعي بأهمية الأمن السيبراني وضرورة اتخاذ التدابير الوقائية والتقنيات الحديثة لحماية البيانات.

قائمة المراجع

مراجع باللغة العربية:

1. دهمش، نعيم وأبو زر، عفاف إسحق. الضوابط الرقابية والتدقيق الداخلي في بيئة تكنولوجيا المعلومات. المؤتمر العلمي الدولي السنوي الخامس لكلية الإدارة والاقتصاد والعلوم الإدارية، جامعة الزيتونة الأردنية، تحت شعار "اقتصاد المعرفة والتنمية الاقتصادية"، عمان، الأردن، 2005.
2. مصلح، ناصر عبد العزيز. أثر استخدام الحاسوب على أنظمة الرقابة الداخلية في المصارف العاملة في قطاع غزة. رسالة ماجستير، الجامعة الإسلامية، كلية التجارة، غزة، 2007.
3. الحميري، بشير، القوي، محمد، الشمري، عبد القادر. استخدام تقنية المعلومات والرقابة على البيانات باستخدام .COBIT الجهاز المركزي للرقابة والمحاسبة، اليمن، 2011.
4. سعيد، هويدا النور. الرقابة على تقنية المعلومات. ديوان المراجعة القومي، السودان، 2011.
5. إيهاب خليفة، القوة الإلكترونية وأبعاد النحول في خصائص القوة، مكتبة االسكندرية، مصر، 2014.
6. ابراهيم جبل، أدوات الرقابة المتاحة للأجهزة العليا للرقابة المالية والمحاسبة وسبل تطويرها، القاهرة: دار النهضة العربية،2015.

❖ **المعايير والأدلة:**

1. مجموعة عمل انتوساي لتدقيق تكنولوجيا المعلومات (WGITA) ومبادرة انتوساي للتنمية (IDI)، دليل تدقيق تكنولوجيا المعلومات لأجهزة الرقابة العليا، تمت ترجمته من قبل ديوان المحاسبة الكويتي في فبراير 2014،
2. مجموعة عمل انتوساي لتدقيق تكنولوجيا المعلومات (WGITA) ومبادرة انتوساي للتنمية (IDI)، حول تدقيق تكنولوجيا المعلومات لأجهزة الرقابة العليا ، 2022.
3. المنظمة الدولية لأجهزة الرقابة العليا(INTOSAI) ، الدليل الإرشادي 5100: توجيهات بشأن مراجعة نظم المعلومات.
4. الدليل الإرشادي – 5300 – ISSAI حول تدقيق تقنية المعلومات.
5. دليل تدقيق برنامج الأمن السيبراني، مكتب مساءلة الحكومة الأمريكية، (2023).
6. لمنظمة الأجهزة العليا للرقابة (INTOSAI) ، اساي 100 – المبادئ الأساسية لرقابة القطاع العام – إدارة فريق الرقابة ومهاراته، 2019 .

❖ **القوانين والمراسيم التنفيذية:**

1. القانون 09/04 المؤرخ في 5غشت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.
2. قانون رقم 18-04 المؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018 يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية.
3. قانون رقم 18-07 مؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.
4. قانون 05-18مؤرخ في 24 شعبان عام 1439 الموافق 10 مايو 2018.يتعلق بالتجارة الإلكترونية.
5. مرسوم رئاسي رقم 20-05 مؤرخ في 20 جمادى الأولى عام 1441 الموافق 20 جانفي سنة 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.
6. المرسوم الرئاسي رقم 15-261 المؤرخ في 18 أكتوبر 2015 يحدد تشكيل وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

❖ **المصادر الأجنبية:**

1. Center for Strategic and International Studies (CSIS). "Significant Cyber Incidents Since 2006." USA, 2021.
2. Deloitte. "IT audit in the era of digital transformation: How to adapt and thrive." Deloitte Insights, 2021.
3. PwC. "Digital transformation." PwC, 2018.
4. EY, Ajak. "Navigating the risk and regulatory landscape: Technology and digital transformation." EY Insights, 2020.
5. Siponen, M., & Vance, A. "Neutralization: New insights into the problem of employee information systems security policy violations." MIS Quarterly, 2010.
6. ISACA Journal, Volume 1, 2023. "Case Study: Performing a Cybersecurity Audit of an Electric Power Transmission Systems Operator."
7. European Union Agency for Cybersecurity (ENISA). "Raising Awareness of Cybersecurity: A Key Element of National Cybersecurity Strategies." Greece, 29 November 2021.
8. Comité de contact des ISC de l'UE. "Compendium d'audit: La cyber sécurité dans l'UE et ses États membres, Audit de la résilience des systèmes

d'information et des infrastructures numériques critiques aux cyberattaques." December 2020.

9. ISACA. "Auditing Cybersecurity." ISACA Journal, 2019.

10. Cooke, I., & Raghu, R. V. (2019, March 1). "IS Audit Basics: Auditing Cybersecurity." IS Audit Basics. Retrieved from [https://www.isaca.org/].

11. Sathyanarayanan, Kishan. "Disaster Recovery and Business Continuity Preparedness for Cloud-based Start-ups." ISACA Now Blog, 2023.

12. Kim Pham, CIA, Market Advisor. "Cloud Computing — What IT Auditors Should Really Know." ISACA Now Blog, 2022.

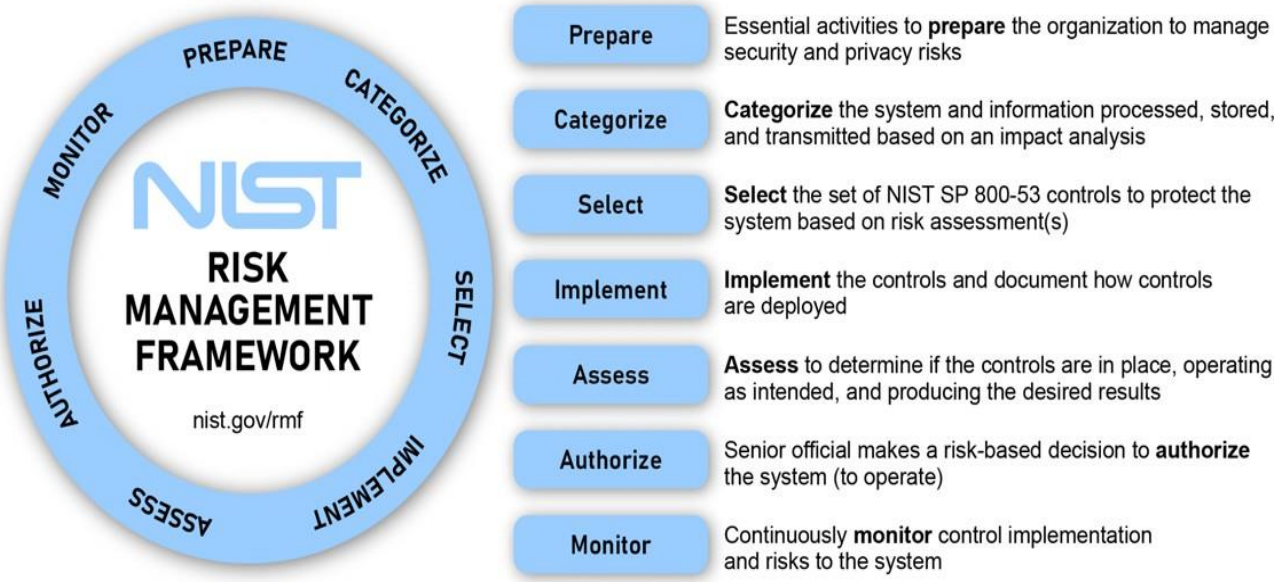
❖ **المواقع الالكترونية:**

1. ENISA (European Union Agency for Cybersecurity). https://www.enisa.europa.eu/publications/
2. eGA (e-Governance Academy). https://ega.ee - Essential Cybersecurity Controls
3. Fibladi. https://fibladi.com/
4. Sonelgaz. https://www.sonelgaz.dz/
5. National Audit Office of Bahrain. https://www.nao.gov.bh/category/information-systems-audit
6. Audit Guru. https://audit.guru/disaster-recovery-and-business-continuity-in-it-audits/#:~
7. Atlant Security. https://atlantsecurity.com/cybersecurity-audits-are-necessary-in-the-due-diligence-of-ma-deals/
8. Pempal. https://www.pempal.org - Auditing IT Governance
9. ISACA. https://www.isaca.org/resources/news-and-trends/industry-news/2023/managing-data-privacy-and-information-security-with-it-audits
10. UpGuard. https://www.upguard.com/blog/cyber-hygiene
11. Deloitte. https://www2.deloitte.com
12. Internal Auditor Online (The Institute of Internal Auditors). https://iaonline.theiia.org/blogs/Jim-Pelletier/2020/Pages/3-
13. TechTarget. https://searchsecurity.techtarget.com

14. Ministère de la Défense Nationale (Algeria). https://www.mdn.dz/site_principal
15. Medium. https://medium.com
16. strongDM. https://www.strongdm.com/blog/cybersecurity-audit
17. Cybersecurity Consulting Ops. https://www.cybersecurityconsultingops.com/
18. e-Governance Academy. https://ega.ee
19. AgileBlue. https://agileblue.com/what-is-a-cybersecurity-audit-why-is-it-important

الملاحق:

الملحق 01 : العناصر الرئيسية لإطار إدارة المخاطر للمعهد الوطني للمعايير والتقنية(NIST)



Source: *National Institute of Standards and Technology, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Revision 2,* SP-800-37 (Gaithersburg, MD: Dec 2018); images: agency logos. | GAO-23-104705

ملحق 02: عائلة المواصفة القياسيةISO 27001

عائلة المواصفة القياسية ISO 27001 هي مجموعة من المعايير الدولية التي تم تطويرها لتوفير إطار عمل لأنظمة إدارة أمن المعلومات .(ISMS) تهدف هذه المواصفات إلى ضمان أن المؤسسات لديها عمليات فعالة لحماية معلوماتها من التهديدات الأمنية وضمان سرية وسلامة وتوافر البيانات. تشمل هذه العائلة العديد من المعايير، من أبرزها:

- ISO/IEC 27001: حدد متطلبات إنشاء وتنفيذ وصيانة وتحسين نظام إدارة أمن المعلومات .(ISMS) و يشمل تحديد وتقييم ومعالجة مخاطر أمن المعلومات.
- ISO/IEC 27002: يوفر إرشادات حول الضوابط الأمنية بناءً على أفضل الممارسات، ويوفر مجموعة من الضوابط لاستخدامها في إطار ISMS .
- ISO/IEC 27003 : يقدم إرشادات لتنفيذ نظام إدارة أمن المعلومات، بما في ذلك شرح كيفية وضع وتنفيذ نظام ISMS بناءً على.ISO/IEC 27001
- ISO/IEC 27004 : يركز على قياس فعالية أنظمة إدارة أمن المعلومات، بما في ذلك كيفية قياس ومراقبة وتحليل أداء.ISMS

- ISO/IEC 27005 : يوفر إرشادات لإدارة مخاطر أمن المعلومات، ويكمل ISO/IEC 27001 من خلال توفير منهجية منظمة لإدارة المخاطر.
- ISO/IEC 27006 :يحدد المتطلبات التي يجب أن تلتزم بها الهيئات التي تقدم خدمات التدقيق والشهادات لـ.ISO/IEC 27001
- ISO/IEC 27007 يوفر إرشادات حول التدقيق الداخلي لأنظمة إدارة أمن المعلومات (ISMS).
- ISO/IEC 27008: وفر إرشادات لمراجعي ISMS حول تقييم ضوابط أمن المعلومات.
- ISO/IEC 27017: يقدم إرشادات لأمن المعلومات المتعلقة بالخدمات السحابية، ويكمل ISO/IEC 27002 بتقديم ضوابط إضافية خاصة بالخدمات السحابية.
- ISO/IEC 27018 : يركز على حماية البيانات الشخصية في الخدمات السحابية العامة، ويقدم ضوابط بناءً على ISO/IEC 27002 .

هذه المواصفات تساهم في وضع أسس قوية لأمن المعلومات داخل المؤسسات، وتساعد في الامتثال للمتطلبات التنظيمية والتشريعية، وتحسين كفاءة العمليات الأمنية.