وزارة الحكم المحلي

استراتيجية الرقمنة
في قطاع الحكم المحلي
(2030 - 2025)

أيار / 2024

تقديم:

تقديم

انطلاقاً من أولويات الحكومة الفلسطينية التاسعة عشرة، ومنها تنفيذ برنامج إصلاح وتطوير أداء المؤسسات الحكومية، وصولاً إلى نظام حوكمة يضمن الحكم الرشيد ويحسن أداء الخدمات في كافة القطاعات، واستمراراً لجهود الحكومات الفلسطينية السابقة في مجال التحول الرقمي، وانسجاما مع أجندة فلسطين الرقمية 2030، وما يرتبط بها من سياسات واستراتيجيات وجهود، تعتبر استراتيجية الرقمنة في قطاع الحكم المحلي أساساً مرجعياً للرقمنة على مستوى قطاع الحكم المحلي.

يعتبر قطاع الحكم المحلي من أهم القطاعات التي تقدم خدمات للمواطنين، خاصة عبر الهيئات المحلية وما تقوم به من وظائف، وفي هذا السياق تسعى وزارة الحكم المحلي بصفتها التوجيهية والإشرافية على القطاع، إلى رسم السياسات ووضع الإستراتيجيات التي تدعم تحسين الكفاءة، وجودة الخدمات المقدمة، والشفافية بما يحقق رفاهية المواطنين.

تُظهر هذه الوثيقة الاستراتيجية مدى تضافر الجهود بين الشركاء في القطاع وذوي العلاقة في إعدادها، والحرص على تحقيق تقدم في الرقمنة على المستوى المحلي ليواكب الرقمنة على المستوى الوطني والتسارع في التقدم التكنولوجي وفقا لأفضل الممارسات.

أتوجه بجزيل الشكر والتقدير لكل من ساهم في إعداد هذه الاستراتيجية، والتي ستكون عنواناً للفترة القادمة لكل من الوزارة وصندوق تطوير وإقراض الهيئات المحلية والإتحاد الفلسطيني للهيئات المحلية وسائر الهيئات المحلية وللبرامج والمشاريع التي تستهدف رقمنة القطاع.

د. م. سامي حجاوي

وزير الحكم المحلي

دولة فلسطين State of Palestine وزارة الحكم المحلي Ministry of Local Government

الفهرس:

الاختصارات:

الاختصار	الوصف
الفريق	فريق اعداد استراتيجية الرقمنة في قطاع الحكم المحلي والمشكل بموجب قرار من معالي وزير الحكم المحلي رقم (1-2023-3254) بتاريخ 2023/5/10
MOLG	وزارة الحكم المحلي
APLA	الاتحاد الفلسطيني للهيئات المحلية
MDLF	صندوق تطوير واقراض الهيئات المحلية
MTIT	وزارة الاتصالات والاقتصاد الرقمي
PESTEL	تحليل البيئة الخارجية من النواحي السياسية والاقتصادية والاجتماعية والتكنولوجية والبيئية والقانونية
SWOT	التحليل الرباعي لنقاط القوة والضعف والفرص والتهديدات
INDIGO	مشروع الحكم الالكتروني في فلسطين
HCD	منهجية التصميم المتمحور حول الانسان

الملخص التنفيذي:

تُشكل استراتيجية الرقمنة للأعوام 2025 – 2030، أساسًا توجيهيًا وإرشاديًا للهيئات المحلية الفلسطينية ولسائر الشركاء في قطاع الحكم المحلي، لتحقيق الرقمنة في القطاع وتعزيز وتطوير الخدمات العامة المقدمة للمواطنين. وتعتمد في فحواها على عدد من العناصر الرئيسية الساعية إلى إرساء قاعدة لقطاع حكم محلي رقمي فعّال وشامل يعزز قدرة هيئات الحكم المحلي على الاستجابة لاحتياجات المواطنين المختلفة وتعزيز صمودهم، ويحفز التنمية المستدامة في فلسطين، بما يتواءم مع رؤية الحكومة الوطنية للتحول الرقمي ويُسهم في تعزيز دور قطاع الحكم المحلي في تحقيق هذه الرؤية.

وتتضمن هذه الاستراتيجية عدة أهداف رئيسية تشمل تعزيز البنية التحتية الرقمية والأدوات التكنولوجية، وبناء القدرات وتعزيز إدارة التغيير من خلال العمل على تعزيز ثقافة الرقمنة وتوعية الهيئات المحلية بكامل طواقمها إلى جانب توعية المجتمعات المحلية، سعيًا لتعزيز الصمود الرقمي وضمان استمرارية الخدمات الأساسية دون انقطاع لا سيما في حالات الطوارئ. وتعدّ هذه الأهداف الأساس التوجيهي للتنفيذ بفعالية؛ حيث أنها ارتكزت على تحليل الوضع القائم لقطاع الحكم المحلي في مجال التحول الرقمي، بالتركيز على دراسة نقاط القوة والضعف والتحديات والفرص.

تشمل الاستراتيجية أيضًا المبادئ والركائز الرئيسية كأساس يسهم في استمرارية التحول الرقمي، إضافة إلى القيم والمبادئ التي توجه عمليات التحول الرقمي، والمتمثلة بالشفافية والشمول والاستدامة المرتكزة على نهج التصميم المتمحور حول الإنسان، بهدف تحقيق نتائج فعّالة وطويلة الأمد.

وتشير استراتيجية الرقمنة في قطاع الحكم المحلي إلى التدابير والإجراءات والتدخلات الواجب تنفيذها لتحقيق التحول بشكل فعّال، عبر وضع إطار عمل مفصل يوضح كيف يُمكن بلوغ الأهداف المرجوة وتحويل كافة التحديات إلى فرص من أجل تحقيق رؤيتنا الطموحة لقطاع حكم محلي رقمي فعّال وشامل. ويتضمن هذا الإطار التخطيط، وتخصيص الموارد، وتدريب الكوادر، وتنفيذ التقنيات الرقمية الأمثل، وتحديد المحاور الرئيسية لتنفيذ الاستراتيجية ووضع جدول زمني لتحقيق الأهداف بفعالية. كما وتغطي الاستراتيجية عمليات المتابعة والتقييم باستخدام آليات فعّالة لمتابعة عملية تنفيذ وتقييم الأداء بانتظام لضمان تحقيق النتائج المرجوة وتحسين العملية بشكل مستمر.

المقدمة:

أولت الحكومات الفلسطينية المتعاقبة اهتمامًا كبيرًا برفاهية المواطن الفلسطيني وتحسين جودة حياته، وتُعدُّ التكنولوجيا أداةً جوهريةً في هذا المسعى. ومن هذا المنطلق، يتزايد الاهتمام الحكومي الفلسطيني بدفع عجلة التحول الرقمي على المستويين الوطني والمحلي، من أجل تطوير الخدمات الحكومية وجعلها أكثر كفاءة وفعالية، ممّا يُتيح للمواطنين الوصول إليها بسهولة ويسر.

تتبوّأ وزارة الحكم المحلي بصفتها التوجيهية والإشرافية على قطاع الحكم المحلي، مكانةً ريادية في قيادة مسيرة التحول الرقمي في القطاع. ومنذ نشأتها، حرصت وزارة الحكم المحلي على تحقيق الاستخدام الأمثل لتكنولوجيا المعلومات لتحسين الخدمات المُقدمة للمواطنين، وتجسّد ذلك في مجموعةٍ من الخطوات الملموسة، شملت؛ تجنيد الأموال، وتوجيه الشركاء، ووضع السياسات والاستراتيجيات، وتنفيذ المشاريع التي تحرز تقدمًا في مسار التحول الرقمي في الهيئات المحلية الفلسطينية.

وبالتنسيق والتعاون مع مختلف الجهات الفاعلة، أطلقت وزارة الحكم المحلي مبادرةً استراتيجيةً تمثّلت في وضع إطارٍ استراتيجيٍ شاملٍ للتحول إلى بلدياتٍ إلكترونية يُغطّي الفترة 2019 – 2023، وقد تم اعتماده رسميًا من قبل الوزارة، وصندوق تطوير وإقراض الهيئات المحلية، والاتحاد الفلسطيني للهيئات المحلية والعديد من الجهات المانحة في قضايا التحول الرقمي.

تتوافق جهود الوزارة في مجال التحول الرقمي مع الرؤية الوطنية وتتزامن مع إطلاق الحكومة الفلسطينية لأجندة فلسطين الرقمية 2030، واعتماد استراتيجية الحكومة الرقمية وخارطة الطريق المنبثقة عنها للأعوام (2024-2029) وإعداد السياسة الوطنية للنفاذية الرقمية. تأتي هذه الجهود في إطار شراكة مثمرة مع مختلف الجهات الفاعلة في قطاع الحكم المحلي وصندوق تطوير وإقراض الهيئات المحلية على وجه التحديد، وهو ما أسهم في تحقيق إنجازات ملموسة بدءًا من تطوير البنى التحتية للبيانات المكانية (SDI) ونظام جيومولج (Geomolg)، وتطوير العديد من الأنظمة في الهيئات المحلية مثل أنظمة الإدارة المالية المتكاملة، ووصولًا لمراكز خدمات الجمهور وما يرتبط بها من أدوات تكنولوجية.

وفي ظل التطور التكنولوجي المتسارع عالميًا ووطنيًا، ومع اقتراب انتهاء الإطار الاستراتيجي للتحول الى بلديات الكترونية بنهاية العام 2023، ارتأت الوزارة والشركاء في القطاع أهمية تطوير استراتيجية لرقمنة قطاع الحكم المحلي تتماشى مع الأجندات والسياسات الوطنية في مجال الرقمنة وتلبي متطلبات التحول الرقمي على المستوى المحلي للفترة (2025 – 2030). ومن هنا تقرر تشكيل فريق متخصص يُكلّف بإعداد استراتيجية الرقمنة في قطاع الحكم المحلي، ويتكون من ممثلين عن مختلف الجهات ذات العلاقة، أهمها:

1. وزارة الحكم المحلي
2. وزارة الاتصالات والاقتصاد الرقمي
3. الأمانة العامة لمجلس الوزراء
4. الاتحاد الفلسطيني للهيئات المحلية

5. صندوق تطوير وإقراض الهيئات المحلية الفلسطينية
6. القطاع الأكاديمي في قطاع غزة / الكلية الجامعية للعلوم التطبيقية
7. جامعة بيرزيت
8. جامعة النجاح الوطنية
9. اتحاد شركات أنظمة المعلومات الفلسطينية
10. نقابة العلوم المعلوماتية التكنولوجية الفلسطينية
11. مشروع الحكم الإلكتروني (INDIGO) المُمول من مؤسسة GIZ
12. بلدية نابلس
13. بلدية الخليل
14. بلدية بيتونيا

منهجية عمل الفريق:

- عقد اجتماعات دورية لاستعراض الخطوات ومتابعة التقدُم.
- دراسة الوثائق ذات العلاقة بالتحول الرقمي على كافة المستويات المحلية والإقليمية والعالمية.
- تقييم الواقع الحالي لتكنولوجيا المعلومات في قطاع الحكم المحلي.
- تشكيل مجموعات بؤرية خلال مراحل عمل الفريق.
- صياغة مسودة الاستراتيجية ومراجعتها وتنقيحها بشكل دقيق.
- الحصول على التغذية الراجعة وإجراء التعديلات اللازمة على مسودة الاستراتيجية.
- اعتماد الاستراتيجية من قبل الفريق والتنسيب لمعالي وزير الحكم المحلي للمصادقة النهائية.

التعريفات والمفاهيم:

جودة حياه المواطن من منظور الحكم المحلي:

تمكين المواطن من الحصول على خدمات قطاع الحكم المحلي بسهولة وسرعة الاستجابة بكفاءة عالية وبتكلفة أقل

المواطن من منظور استراتيجية الرقمنة في قطاع الحكم المحلي:

هو كل مكلف أو متلقي خدمة من قطاع الحكم المحلي بغض النظر عن الجنس، العمر، مكان السكن، أو حالة الإعاقة

البلدية الإلكترونية:

نظام قائم على إحداث تحول في الطريقة التي تعمل بها الهيئة المحلية (بما يشمل البلديات والمجالس القروية) ومجالس الخدمات المشتركة من خلال الاستخدام الأمثل والفعال لتكنولوجيا المعلومات والاتصالات بهدف تحسين إدارة الخدمات وتوفيرها بشكل أفضل للمواطنين لتعزيز تحقيق مفاهيم الحكم الرشيد

التصميم المتمحور حول الإنسان:

هو توجه مبتكر في التغلب على التحديات التي تضع احتياجات المواطنين وتجاربهم ومتطلباتهم وتطلعاتهم في صميم عملية حل المشكلات، استنادًا إلى أساليب" التعلم بالتجربة": التجريبية والإبداعية والتشاركية والتكرارية، لتوفير أساليب فعالة لضمان تلبية الحلول المبتكرة لاحتياجات أولئك التي صُممت من أجلهم.

الرقمنة:

عملية تحويل المعلومات والبيانات من صيغة تناسبية للإنسان إلى صيغة رقمية قابلة للتخزين والمعالجة باستخدام الأرقام (الأرقام الثنائية أو العشرية). يتضمن ذلك؛ تحويل الصور، والصوت، والنصوص، والفيديو، وغيرها من أشكال البيانات إلى صيغ قابلة للفهم والمعالجة من قبل الأنظمة الرقمية. وتعتبر الرقمنة طريقة لتطوير الأعمال من خلال استخدام الحلول الرقمية.

البلدية الرقمية:

هي بلدية إلكترونية تستخدم التكنولوجيا على نطاق واسع وشامل على كافة أعمال وخدمات البلدية مما يسهم في زيادة تحسين جودة الحياة للمواطنين.

التحول الرقمي على المستوى الوطني:

منذ فجر تأسيس السلطة الوطنية الفلسطينية، سعت دولة فلسطين جاهدةً لبناء مؤسسات تواكب أفضل الممارسات العالمية، فاهتمت بحوسبة عملياتها. ومع ظهور مفهوم الحكومة الإلكترونية، تبنت الحكومات الفلسطينية المتعاقبة منذ أكثر من خمسة عشر عامًا فكرة التحول إلى حكومة إلكترونية إدراكًا بتأثير ذلك على تقديم خدمات أفضل للمواطنين الفلسطينيين وتحسين كفاءة العمل الحكومي، فوضعت ونفذت العديد من الخطط وبرامج بناء القدرات وأوراق السياسات والاستراتيجيات والمشاريع التي تخدم عملية التحول وتسهم في تحقيق أهدافها، وعلى سبيل التدليل لا الحصر؛ فقد تم تنفيذ مشروع الشبكة الحكومية، وناقل البيانات الوطني، ومشروع زنار، ومنظومة الخدمات الإلكترونية الحكومية "حكومتي"، وقانون المعاملات الإلكترونية، وقانون منظومة الخدمات الحكومية الإلكترونية، وقانون الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

إيمانًا بأهمية التحول الرقمي ودوره في تحقيق التنمية المستدامة في فلسطين، واستمرارًا للجهود المبذولة في تعزيز الحوكمة الإلكترونية، وضعت دولة فلسطين أجندة فلسطين الرقمية 2030، وأطلقت مجموعة من المبادرات الاستراتيجية لتسريع وتيرة التحول الرقمي على المستوى الوطني، فقد تم اعتماد استراتيجية الحكومة الرقمية 2024-2029، وتم تعميمها على جميع الدوائر الحكومية للبدء في تنفيذ خارطة الطريق المنبثقة عنها، إضافة إلى السياسة الوطنية للنفاذية الرقمية.

الوثائق التالية تُشكل المراجع الرئيسية على المستوى الوطني لعملية التحول الرقمي الفلسطيني:

1. قرار بقانون 11 لسنة 2023 بشأن منظومة الخدمات الحكومية الإلكترونية.
2. قرار بقانون رقم 15 لسنة 2017 بشأن المعاملات الالكترونية.
3. أجندة فلسطين الرقمية 2030 / قرار مجلس الوزراء رقم (13) لسنة 2023.
4. استراتيجية الحكومة الرقمية وخارطة الطريق المنبثقة عنها للأعوام 2024-2029/ قرار مجلس الوزراء رقم (18/249/11/م. و/م. أ) لعام 2024.
5. إدارة أمن المعلومات / قرار مجلس الوزراء رقم (12) لسنة 2023 / بتعديل قرار مجلس الوزراء رقم (6) لسنة 2020.
6. استضافة المؤسسات على الحوسبة السحابية والربط على ناقل البيانات الوطني / قرار مجلس الوزراء رقم (18/151/06/م. و/م. أ) لعام 2022.
7. وثيقة حوكمة الخدمات الحكومية الإلكترونية والسياسة المالية للدفع الالكتروني / قرار مجلس الوزراء رقم 18/127/03/م. و/م. أ لعام 2021.
8. سياسة أمن المعلومات المعدلة / قرار مجلس الوزراء رقم 18/122/09/م. و/م. أ لعام 2021.
9. السياسة الوطنية للتحول الرقمي / قرار مجلس الوزراء رقم 18/105/17/م. و/م. أ.لعام 2021.
10. الإطار الاستراتيجي للتحول على بلديات الكترونية (2019-2023) / وزارة الحكم المحلي – تشرين الثاني/2018.
11. دليل إعداد سياسات تكنولوجيا المعلومات في الهيئات المحلية (2022 – 2023) / وزارة الحكم المحلي.

الرؤية - الأهداف:

الرؤية:

قطاع حكم محلي رقمي فعّال وشامل يُعزّز رفاهية المستفيدين ويُحفّز التنمية المستدامة في فلسطين.

الغاية العامة:

الارتقاء بجودة الخدمات المقدمة للمواطنين في قطاع الحكم المحلي من خلال تبني منهجية شاملة للرقمنة تُركّز على احتياجات المواطنين وتُساهم في تحقيق الشفافية والمساءلة والشمول الرقمي وسرعة الاستجابة.

الأهداف الاستراتيجية:

1. **تعزيز البنية التحتية الرقمية والأدوات التكنولوجية:**

توفير بيئة تكنولوجية آمنة وموثوقة وقادرة على توفير الخدمات الرقمية وضمان استمراريتها من خلال بناء وتحسين البنية التحتية التكنولوجية وما يرتبط بها من أدوات وأنظمة لدى جميع الشركاء في قطاع الحكم المحلي، واستخدام الأدوات الرقمية والأتمتة لتحسين العمليات الإدارية.

2. **بناء القدرات وتعزيز إدارة التغيير:**

تطوير المهارات والقدرات الرقمية اللازمة لدى جميع العاملين في قطاع الحكم المحلي، وتطبيق أفضل الممارسات في إدارة التغيير بما يخدم التحول الرقمي.

3. **تعزيز الثقافة والمجتمع الرقمي:**

العمل على نشر ثقافة الرقمنة وتوعية المجتمعات المحلية والكوادر العاملة في قطاع الحكم المحلي حول أهمية التحول الرقمي وسبل تحقيقه بما يسهم بتعزيز الثقة في الرقمنة وتحفيز المجتمع لتطبيقها واستخدامها.

4. **تعزيز الصمود الرقمي:**

تطبيق إدارة المخاطر وتوفير الخطط والأدوات للاستعادة والتعافي من الكوارث، وتطوير استراتيجيات المرونة والخطط البديلة لضمان تقديم الخدمات الأساسية دون انقطاع أثناء حالات الطوارئ، والاستفادة من المنصات الرقمية وحلول العمل عن بُعد للحفاظ على استمرارية الأعمال.

تحليل الواقع الحالي لقطاع الحكم المحلي في مجال التحول الرقمي:

أُجري مسحٌ شامل لتقييم واقع تكنولوجيا المعلومات في قطاع الحكم المحلي خلال النصف الأول من العام 2023، وقد شمل المسح جميع مكونات القطاع، بما في ذلك: الهيئات المحلية، وزارة الحكم المحلي، صندوق تطوير واقراض الهيئات المحلية، الاتحاد الفلسطيني للهيئات المحلية، ويدرج الملحق رقم (1) من هذه الوثيقة الاستراتيجية تحليلًا تفصيليًا للواقع الحالي لقطاع الحكم المحلي في مجال التحول الرقمي. وكان ملخص النتائج كما يلي:

أولا: تقييم واقع تكنولوجيا المعلومات في الهيئات المحلية:

1) البنية التحتية الرقمية والأنظمة المحوسبة:

يوجد بنية تحتية رقمية وأنظمة محوسبة وما يرتبط بها من أدوات تكنولوجيا المعلومات وتتوفر جزئيًا خدمات داخلية رقمية واستضافة داخلية للأنظمة. حيث أظهر المسح أن 55.8% من الهيئات المحلية لديها بنية تحتية رقمية وأنظمة محوسبة بدرجة متوسطة، كما أن 44 % من الهيئات المحلية لديها خدمات الانترنت واستضافة داخلية للأنظمة، مع عدم وجود مراكز استعادة من الكوارث.

2) الخدمات الرقمية: أظهر المسح أن 79 % من الهيئات المحلية تفتقر إلى وجود خدمات رقمية أو أن لديها خدمات رقمية بمستوى ضعيف، كما أن 15 % من الهيئات المحلية لديها خدمات رقمية بمستوى متوسط. أما بخصوص المواقع الإلكترونية فإن 44 % من الهيئات المحلية لديها مواقع إلكترونية رسمية، و15 % من الهيئات المحلية ليس لديها أية صفحة إلكترونية رسمية.

3) خصوصية البيانات وأمن المعلومات:

47.7% من الهيئات المحلية تراعي وتهتم بالمحافظة على خصوصية البيانات ولديها أنظمة أمن المعلومات، بينما 37.2% من الهيئات المحلية ليس لديها هذه الأنظمة أو أنها موجودة بأشكال بدائية. أما فيما يخص تقييم المخاطر، أظهر المسح أن 50% من الهيئات المحلية لم تقم بأي شكل من أشكال تقييم المخاطر من قبل طرف ثالث.

4) التخطيط والتطوير وكادر تكنولوجيا المعلومات:

يعاني مجال التخطيط والتطوير وكادر تكنولوجيا المعلومات من نقص بنسبة 58.1%، لعدة أسباب من أهمها عدم تخصيص الموازنات المطلوبة. هنالك أيضًا نقص في مشاركة المواطنين في معظم الهيئات المحلية في وضع استراتيجيات

التحول الرقمي. ويتمتع فقط 37.2% من هذه الهيئات باستراتيجيات نشطة وميزانية محددة وكوادر في مجال تكنولوجيا المعلومات.

5) التعاون والمشاركة: يظهر وجود قصور في التعاون في مجال الابتكار الرباعي (القطاع الخاص، القطاع الأكاديمي، المجتمعات المحلية، المؤسسات الإقليمية والدولية)، والذي قد يعيق تنفيذ الاستراتيجية الوطنية الرقمية على مستوى الحكم المحلي. يشير المسح إلى أن 42% من الهيئات المحلية لا يوجد لديها أي تعاون مع القطاع الخاص و22 % منها لديها القليل من التعاون، ولا يوجد تعاون مع القطاع الأكاديمي بنسبة 81%، ولا يوجد تعاون مع المجتمعات المحلية بنسبة 83%، بينما وصلت نسبة عدم وجود تعاون بين الهيئات المحلية والهيئات الإقليمية أو الدولية الى 86%.

6) التدريب وتقييم الأداء: تبين أن 86% من الهيئات المحلية لا تمتلك أية آليات للتدريب وتقييم الأداء، حيث تشير الدراسة إلى أن 54.7% منها ليس لديها أية آليات، و31.4% لديها آليات ولكن تصنف بأنها ضعيفة للغاية. وأظهرت الدراسة أيضًا أن 2.3% فقط من الهيئات المحلية تمتلك آليات فعّالة للتدريب وتقييم الأداء.

تحليل النتائج:

تم تحليل العلاقات بين المتغيرات المختلفة بهدف الحصول على مزيد من الملاحظات والنتائج، حيث عولجت المتغيرات المعلوماتية العامة المتعلقة بالمحافظات وتصنيفات الهيئات المحلية وعدد موظفيها وكذلك وضع الرقمنة فيها باستخدام معالج التقارير crosstab. يظهر الملحق رقم (1) من هذه الدراسة تفاصيل هذا التحليل.

انعكاس و أثر نتائج التحليل الخاص بالهيئات المحلية على استراتيجية الرقمنة في قطاع الحكم المحلي

- على الرغم من وجود أنظمة محوسبة وملحقات جيدة، واتصال إنترنت جيد في الهيئات المحلية، إلا أن هناك نقصًا في الأسس الضرورية مثل مراكز البيانات ومراكز استرجاعها لتتناسب مع الخدمات الإلكترونية التي يتم طرحها للمواطنين، وتحسين عمل الهيئات المحلية. ولذا، يُفضل إنشاء هذه المراكز للبيانات والاستفادة من المراكز الموجودة كبديل مساعد أو كمراكز لاسترجاع البيانات.
- الخدمات الإلكترونية ضعيفة أو معدومة في جميع التصنيفات، رغم أن توفيرها للمواطنين يجب أن يكون سلسًا وغير منقطع ومتاحًا بشكل فوري. كما يجب أن تكون هذه الخدمات متصلة بالحكومة المركزية لتسهيل الوصول إليها والتعامل معها، وهذا يجب أن يكون جزءًا من البنية الأساسية في خطط الهيئات المحلية السنوية.
- هذا وبيّن المسح أن 63 من البلديات تعاني من ضعف في كوادر التخطيط والتطوير وتكنولوجيا المعلومات أيضًا في التصنيفات الأربعة كلها. ولذلك، يجب النظر في هذا الموضوع بجدية في الخطط السنوية لتسريع عملية الرقمنة في كافة الهيئات المحلية.

- تضعف أيضًا آليات المشاركة والتعاون والتدريب وأنظمة تقييم الأداء في جميع تصنيفات الهيئات المحلية. وهذا يستدعي التزامًا جادًا من قبل وزارة الحكم المحلي وصندوق تطوير وإقراض الهيئات المحلية والاتحاد الفلسطيني للهيئات المحلية لتقوم كل من هذه الأطراف بدورها في مواجهة هذه المشاكل ورعاية مشروع التحول الرقمي كجزء من التخطيط المُنهج والعمل نحو توفير خدمات إلكترونية بشكل سلس للمواطنين وموظفي الهيئات المحلية.

ثانيا: تقييم واقع تكنولوجيا المعلومات على المستوى الوطني للقطاع:

(وزارة الحكم المحلي، صندوق تطويرو إقراض الهيئات المحلية، الاتحاد الفلسطيني للهيئات المحلية)

بناءً على استقراء واقع الوزارة والصندوق والاتحاد ومن خلال الإجابة على أسئلة محددة تتعلق بجوانب البنى التحتية والشبكة والاتصالات وأمن المعلومات وإدارة البيانات والخدمات والصيانة والكوادر، فقد تبين ما يلي (التفاصيل في الملحق رقم (1) من هذه الوثيقة):

البنية التحتية لتكنولوجيا المعلومات:

تعتبر البنية التحتية لتكنولوجيا المعلومات في كل من المؤسسات الثلاث (الوزارة، الاتحاد، الصندوق) قادرة على تلبية احتياجات المؤسسات في المرحلة الحالية، مع التأكيد على الحاجة للتحسين والتطوير المستمر في البنية التحتية، خاصة في مجال أمن المعلومات، واستخدام الحوسبة السحابية والنسخ الاحتياطي ومواقع الاستعادة من الكوارث.

الشبكة والاتصالات:

تعتبر الشبكة والاتصالات في المؤسسات الثلاث هي الركيزة الأساسية للتواصل داخل المؤسسة بطواقمها وخدماتها، ويعتبر تطوير الشبكة والاتصالات بشكل مستمر حاجة ملحة لمواكبة التطور السريع في التكنولوجيا، حيث أنها تعتبر ركيزة أساسية لعمل المؤسسات.

أمن المعلومات:

تولي المؤسسات الثلاث اهتمامًا كبيرًا بقضايا أمن المعلومات لحماية معلوماتها من التهديدات الأمنية حيث يلزم خطط دورية فاعلة لضمان حماية الأنظمة والبيانات ووجود مصادر خارجية تضمن استعادتها بشكل فاعل، وهناك حاجة لدورات توعوية أمنية لتلك المؤسسات بشكل دائم تراعي التطور في المجال الأمني.

إدارة البيانات:

تتم إدارة معظم البيانات في المؤسسات الثلاث من خلال أنظمة معلومات خاصة بها مرتبطة بقواعد بيانات أو أنظمة ملفات، وتظهر الدراسة بأن معظم الأنظمة المستخدمة لإدارة البيانات على درجة عالية من الكفاءة والموثوقية وتراعي الأسس المطلوبة في إدارة البيانات، خاصة فيما يتعلق بصلاحيات الوصول للبيانات وسلامتها وكذلك النسخ الاحتياطي.

إدارة الخدمات والصيانة:

يتم توفير الخدمات والصيانة المطلوبة في مجال تكنولوجيا المعلومات سواء المتعلقة بالبنية التحتية أو الأنظمة والبرامج من خلال موظفي تكنولوجيا المعلومات في المؤسسات الثلاث وكذلك من خلال المزودين الخارجيين لخدمات الدعم والصيانة بحسب نوع الخدمة وطبيعة الصيانة المطلوبة.

طو اقم تكنولوجيا المعلومات:

توفر وزارة الحكم المحلي إدارة عامة لتكنولوجيا المعلومات، مع توفر طاقم دائم من 7 مختصين في مركز الوزارة يقومون حاليًا بتغطية الخدمات على مستوى الوزارة والمديريات، فيما يوفر الصندوق موظفين، ويوفر اتحاد الهيئات المحلية موظفًا واحدًا بدوام جزئي. وهنا تظهر الحاجة الى استكمال التعيينات الوظيفية في المؤسسات الثلاث، والعناية بتدريبهم وبناء قدراتهم.

التحليل الرباعي (SWOT):

تم القيام بتحليل رباعي للبيئة الداخلية والخارجية لقطاع الحكم المحلي على مستوى وزارة الحكم المحلي وصندوق تطوير واقراض الهيئات المحلية واتحاد الهيئات المحلية، والذي أظهر وجود تطور نوعي في استخدام تكنولوجيا المعلومات مع وجود فجوات مختلفة لكل مؤسسة على حدة يمكن تلخيصها كما يظهر في الجدول أدناه:

نقاط القوة (Strengths)	نقاط الضعف (Weaknesses)
وزارة الحكم المحلي	وزارة الحكم المحلي
1. وجود الخوادم والبنية التحتية داخل مقر الوزارة يمنح السيطرة الكاملة على الأنظمة والبيانات، مما يزيد من الأمان والتحكم. 2. استخدام تقنيات حديثة: استخدام خوادم من نوع Blade Server ونظام VMware يسمح بتقسيم الموارد بكفاءة وفعالية. 3. استخدام جدران نارية وبرامج مكافحة الفيروسات وأنظمة حماية البيانات يساهم في تعزيز أمان البيانات. 4. توزيع الحمل وتجميع البيانات: استخدام تقنيات التجميع على الخوادم وتوزيع الحمل يضمن استدامة وكفاءة الأنظمة. 5. الأنواع البيانية: القدرة على استخدام وإدارة مجموعة متنوعة من أنواع البيانات تعزز من مرونة الوزارة في معالجة المعلومات. 6. نظم إدارة البيانات: استخدام نظم إدارة البيانات يساعد على ضمان جودة البيانات وتنظيمها بشكل فعال. 7. عمليات النسخ الاحتياطي: تنفيذ عمليات النسخ الاحتياطي الدورية واستعادة البيانات يسهم في تحقيق استدامة البيانات وضمان عدم فقدانها.	1. نقص التوعية الأمنية: عدم وجود دورات تدريبية أو ورش عمل لتعزيز الوعي الأمني بين الموظفين يمكن أن يترك الوزارة عرضة للتهديدات الأمنية. 2. عدم وجود أنظمة اكتشاف التسلل: عدم وجود أنظمة اكتشاف التسلل يمكن أن يترك الوزارة عرضة لهجمات غير مكتشفة. 3. عدم وجود خطط طوارئ: عدم وجود خطط طوارئ لمواجهة انقطاع الخدمات أو الهجمات السيبرانية يمكن أن يزيد من تأثيرها السلبي. 4. إدارة الصيانة اليدوية: الاعتماد على إدارة وصيانة الأجهزة والبرمجيات بشكل يدوي يمكن أن يكون غير فعال ويزيد من فرص الأخطاء البشرية. 5. عدم وجود سياسات تحديث محددة: عدم وجود سياسات محددة لعمليات التحديث والصيانة يمكن أن يؤدي إلى تأخير في تحسين البنية التحتية.

الاتحاد الفلسطيني للهيئات المحلية	الاتحاد الفلسطيني للهيئات المحلية
1. التخزين السحابي: الاعتماد على التخزين السحابي يمنح الاتحاد مرونة وقدرة على توسيع سعة التخزين بسرعة وكفاءة. 2. تطبيق صلاحيات دقيقة للوصول إلى البيانات يقلل من مخاطر التسريب والوصول غير المصرح به. 3. استخدام وسائل حماية فعالة داخل الاتحاد مثل صلاحيات الدخول الى الخوادم. 4. استخدام صارم لصلاحيات الوصول للبيانات للموظفين. 5. استخدام نسخ احتياطي فعال للبيانات داخلي وخارجي. 6. عمليات مراقبة الشبكة فعال ودوري. 7. مراقبة جودة البيانات والتحقق من سلامتها. 8. فحص دوري للنسخ الاحتياطية. 9. دورات دورية لزيادة التوعية بأمن المعلومات للموظفين. 10. استخدام نظام هجين للخدمات والبيانات.	1. وجود عدد قليل من الخوادم في مقر الاتحاد والاعتماد بشكل كبير على التخزين السحابي. 2. استعمال نظام الملفات لتخزين البيانات (File System) بشكل كبير مع استعمال بسيط لأنظمة ادارة البيانات مثل (MySQL & Oracle). 3. عدم وجود أنظمة لإدارة ملفات الصيانة وتحديث البرمجيات يمكن أن يؤدي إلى تفويت الصيانة الدورية وتحديث الأنظمة. 4. وجود موظف تكنولوجيا المعلومات بدوام جزئي يمكن أن يزيد من التأخر في التعامل مع المشاكل التقنية.. 5. لا يوجد خطط وسياسات محددة معنية بادارة البنية التحتية لتكنولوجيا المعلومات والتحديث المستمر. 6. عدم وجود آلية لفحص النسخ الاحتياطية المأخوذة من السحابة الالكترونية. 7. اخذ نسخ احتياطية من البيانات فقط، دون البرمجيات الموجودة داخل الاتحاد.
صندوق تطوير و اقراض الهيئات المحلية	**صندوق تطوير و اقراض الهيئات المحلية**
1. استخدام السحابة الالكترونية حيث توفر المرونة وامكانية الوصول الى البيانات من اي مكان وفي اي وقت. 2. بنية تحتية هجينة تجمع بين الخوادم المحلية والسحابة الإلكترونية توفر مرونة واستدامة عند تحميل البيانات وفي حالات الطوارئ. 3. استخدام نظام تشغيل متطور وأنظمة تجزئة (VMware) يزيد من كفاءة الخوادم والاستفادة من الموارد . 4. الاستفادة من تقنيات التوزيع وتجميع البيانات والتحميل التلقائي للنسخ الاحتياطية تسهم في تعزيز الأمان واستمرارية العمل. 5. تشفير البيانات وتطبيق نظام الصلاحيات يعززان أمان البيانات ومنع الوصول غير المصرح به. 6. استخدام نظام الكشف والاستجابة الموسعة (XDR) للكشف عن التهديدات الأمنية يعزز من قدرة الصندوق على التصدي للتهديدات السيبرانية. 7. تحديث مستمر للبنية التحتية : القدرة على تحديث البنية التحتية واستخدام تكنولوجيا المعلومات تزيد من كفاءة العمل وامان البيانات. 8. استخدام أنظمة أمان: استخدام الجدار الناري وانظمة الامان المختلفة يعزز امن المعلومات والكشف عن الانشطة الغير الآمنة المرتبطة بالبيانات والشبكة الداخلية.	1. عدم توجيه التدريب للموظفين: عدم تقديم دورات توعية امنية للموظفين يزيد من مخاطر الهجمات الالكترونية. 2. عدم وجود نظام موحد لإدارة وصيانة الأجهزة يمكن أن يؤدي إلى فقدان البيانات أو انقطاع الخدمة في حالة عدم التنسيق الجيد. 3. عدم وجود سياسات محددة لإدارة التحديثات وتوقيتها: حيث يتم الاعتماد بشكل كامل على التحديثات من شركة مايكروسوفت فقط .

الفرص (Opportunities)	التهديدات (Threats)
وزارة الحكم المحلي	**وزارة الحكم المحلي**
1. تحسين التوعية الأمنية: إمكانية تقديم دورات تدريبية وورش عمل للموظفين لتعزيز الوعي الأمني وتعزيز مهاراتهم في مجال أمن المعلومات. 2. تطوير أنظمة اكتشاف التسلل: إمكانية تحسين بنية الأمان عبر تنفيذ أنظمة اكتشاف التسلل لرصد واستجابة الهجمات السيبرانية. 3. استخدام برمجيات اكتشاف التسلل مثل : Cisco NGIPS , Fidelis Network. 4. استخدام اجهزة كشف التسلل مثل : FireEye Intrusion Prevention System, Hillstone S-series 5. تخزين البيانات في السحابة: زيادة استخدام التخزين في السحابة مع تشفير البيانات يمكن أن يعزز من تأمين البيانات والاستجابة للاحتياجات المتغيرة. 6. تحسين الصيانة والتحديث: إمكانية تنظيم عمليات الصيانة والتحديث لتحسين أداء البنية التحتية. 7. تنظيم العمليات: فرصة لتنظيم وتوجيه إدارة العمليات من خلال تطبيق الأنظمة المناسبة . 8. تطوير القدرات: توفير دورات تدريبية لموظفي تكنولوجيا المعلومات يمكن أن يساعد في تطوير مهاراتهم وزيادة وعيهم بأمان المعلومات. 9. الاستفادة من الخدمات التي تقدمها وزارة الاتصالات والاقتصاد الرقمي بناء على قرار مجلس الوزراء رقم 18/151/06 لعام 2022.	1. هجمات DDoS :هي هجمات يمكن أن تؤثر سلباً على استقرار الخدمات، ويجب تطوير استراتيجيات لمنعها واستجابة فعالة لها. 2. نقص التخطيط للطوارئ: عدم وجود خطط طوارئ يمكن أن يترك الوزارة عرضة لتعطيل العمل وفقدان البيانات في حالة الأزمات. 3. الأمان الغير كافي : عدم استخدام أنظمة أمان متقدمة يمكن أن يجعل البنية التحتية عرضة للتهديدات الأمنية المتطورة مثل استعمال نظام WAF . 4. فرصة الأخطاء البشرية: الاعتماد على الإدارة اليدوية يتيح فرصًا للأخطاء البشرية والتأخير في الصيانة والتحديث. 5. فقدان البيانات: عدم وجود سياسات تحديث محددة يمكن أن يزيد من خطر فقدان البيانات . 6. عدم كفاية (Offline Backup) وفقا لأفضل الممارسات والأنظمة والمعدات الممكن استخدامها لتنفيذ استعادة البيانات . 7. نقص التنسيق: عدم وجود موظف تكنولوجيا معلومات في معظم المديريات التابعة للوزارة يمكن أن يؤثر على التنسيق بين الفرق وتوزيع المهام بشكل فعال.
الاتحاد الفلسطيني للهيئات المحلية	**الاتحاد الفلسطيني للهيئات المحلية**
1. استخدام برمجيات اكتشاف التسلل مثل : Cisco NGIPS , Fidelis Network. 2. استخدام اجهزة كشف التسلل مثل : FireEye Intrusion Prevention System, Hillstone S-series. 3. بخصوص صلاحيات الوصول للبيانات تتم تطويرها من خلال : تمكين مالكي البيانات من التحكم في حقوق الوصول إلى البيانات التي يمتلكونها للتأكد من أن جميع العمليات مصرح بها . 4. استخدام تقنيات التحقق المتعدد الخطوات مثل التحقق الثنائي (2FA) يمكن أن يحمي البيانات من الوصول غير المصرح به .	1. يتم تطبيق تدابير امنية اساسية فقط على مستوى الصلاحيات للوصول الى البيانات دون استخدام انظمة متطورة. 2. الاعتماد على موظف تكنولوجيا معلومات بدوام جزئي هذا يشكل خطرا في حال حدوث اختراق او تسريب. 3. الاعتماد على الشركة المزودة لتشفير البيانات واختيار الاماكن لتخزين البيانات. 4. عدم وجود تقييم لجميع الإجراءات والسياسات الأمنية المتبعة وتحسينها استنادًا إلى التهديدات والتطورات الأمنية الجديد. 5. استخدام نظام (Files System)بدلا من استخدام انظمة ادارة البيانات بشكل كامل.

5. يمكن تطبيق تقنيات تدفق البيانات للكشف عن تغييرات غير متوقعة في البيانات على مدار الزمن. إذا تم اكتشاف تغييرات كبيرة أو مفاجئة .	6. التبعية للطرف الثالث :في حالة اعتماد الجهة على الطرف الثالث بشكل كبير، قد يؤدي توقف الطرف الثالث عن تقديم الخدمات إلى تعطيل العمليات. عدم وجود تنظيم دقيق لعمليات التحديث والاستبدال يمكن أن يترك الأنظمة عرضة للهجمات أو التجاوز.
صندوق تطوير و اقراض الهيئات المحلية	**صندوق تطوير و اقراض الهيئات المحلية**
1. تحسين التوجيه والتدريب للموظفين: منح الموظفين التدريب في مجال امن المعلومات واستخدام الانظمة يقلل من مخاطر الهجمات الالكترونية. 2. تعزيز تنسيق العمل بين موظفي تكنولوجيا المعلومات يساعد في تحسين الاستجابة للمشكلات التكنولوجية. 3. تحسين إدارة البيانات والتنسيق بين موظفي تكنولوجيا المعلومات يمكن أن يزيد من كفاءة العمل والتنسيق بين المشاريع. 4. استخدام أدوات إدارة مشاريع تسهم في تتبع وصيانة الأجهزة بشكل أفضل.	1. عدم وجود سياسات معينة لإدارة التحديثات يمكن أن يؤدي إلى تأخر في تطبيق التكنولوجيا الجديدة. 2. يعتمد الصندوق بشكل كبير على عقود الصيانة مع الشركات الموردة للتكنولوجيا، مما يعرضه لمخاطر في حالة عدم توفر هذه الخدمات. 3. تحديثات غير منتظمة: عدم وجود سياسات محددة لإدارة التحديثات يمكن أن يجعل البنية التحتية عرضة للثغرات الأمنية.

التوصيات:

هذا وجاءت التوصيات لاستكمال النو اقص وسد الفجوات والبناء على نقاط القوة لكل مؤسسة كما يلي:

وزارة الحكم المحلي	الاتحاد الفلسطيني للهيئات المحلية	صندوق تطوير و اقراض الهيئات المحلية
• تنفيذ أنظمة حماية DoS متقدمة . • تطوير خطط استجابة للهجمات DDoS تشمل الكشف المبكر وعزل الانشطة المشبوهة. • تطوير وتنفيذ خطط طوارئ شاملة تشمل استرجاع البيانات وتوفير توجيهات واضحة للفرق في حالات الأزمات. • تنظيم تدريبات دورية للفرق على أساس الخطط الطارئة. • تقييم البنية التحتية للتكنولوجيا وتحديث أنظمة الأمان وفقًا لأحدث أفضل الممارسات. • تعزيز التوعية بأمان المعلومات بين الموظفين وتطوير سياسات استخدام آمن للأنظمة والبرمجيات. • اعتماد أنظمة إدارة أتمتة للصيانة والتحديث لتقليل الأخطاء البشرية. • تقديم تدريب مستمر للموظفين على مهام الصيانة والأمان. • وضع سياسات دورية لعمليات النسخ الاحتياطي واسترجاع البيانات. • تنفيذ حلول تشفير وتحكم في الوصول لحماية البيانات من الوصول غير المصرح به. • تنفيذ أنظمة متقدمة لاكتشاف التسلل لمراقبة النشاط غير المصرح به داخل البنية التحتية. • تطوير خطط طوارئ تشمل استجابة فورية لانقطاع الخدمات أو الهجمات السيبرانية واستعادة الأمان بسرعة. • اعتماد أنظمة إدارة أتمتة لصيانة الأجهزة والبرمجيات لتحسين الكفاءة وتقليل الأخطاء البشرية. • وضع سياسات وجداول زمنية محددة لعمليات التحديث والصيانة وتنفيذها بانتظام.	• تحسين وتوسيع تدابير الامان واعداد صلاحيات الوصول بما يتناسب مع التهديدات المحتملة , و التفكير في استخدام تقنيات متقدمة مثل تعدد العوامل للمصادقة (Multi-Factor Authentication). • وضع خطط محددة للتحديثات التكنولوجية والامنية بشكل دوري حيث يتضمن تحديث انظمة التشغيل والبرمجيات والتصحيحات الامنية. • الاستثمار في اختبارات الاختراق والتدقيق الامني بشكل دوري لتحديد الثغرات ونقاط الضعف وتصحيحها قبل استغلالها. • توظيف موظف تكنولوجيا معلومات بدوام كامل ليكون مسؤولا بشكل مباشر عن البنية التحتية لتكنولوجيا المعلومات والبيانات وامنها ومراقبة واستجابة لاي تهديدات امنية بشكل فعال. • التأكد من وجود اتفاقيات وعقود دقيقة تشمل جميع جوانب تزويد الخدمة مثل امور تشفير البيانات وحفظ البيانات بشكل مناسب. • اجراء تقييم دوري للسياسات والإجراءات الامنية المتبعة وتحسينها استنادا الى التهديدات والتطورات الامنية الجديدة. • استخدام انظمة ادارة البيانات المتقدمة لزيادة امان وتنظيم البيانات. • تنفيذ انظمة تتبع البريد الالكتروني ومحتوياته للكشف عن اي تهديدات محتملة قبل ان يصل البريد الى الموظفين. • وضع استراتيجية للتعامل مع الطرف الثالث لمزود خدمة السحابة الالكترونية تشمل مراجعة الامان والمتطلبات الامنية في العقود والاتفاقيات.	• تنظيم دورات توعية أمنية دورية لجميع الموظفين في الصندوق، بما في ذلك التحديثات المتعلقة بأمان المعلومات والسلوك السليم عبر الإنترنت. • إنشاء حملات توعية داخلية لتسليط الضوء على تهديدات الأمان الشائعة والتصرف الآمن عبر البريد الإلكتروني والموارد الرقمية الأخرى. • تعزيز توجيه الموارد: توجيه المزيد من الموارد لتقديم الدعم والأدوات اللازمة لموظفي تكنولوجيا المعلومات. • انشاء منهج وأدوات مشتركة لإدارة المشروع وتوثيق الأعمال الصيانة وإصلاح الأخطاء. • تطوير وتنفيذ نظام موحد لإدارة وصيانة الأجهزة وضمان توافقه مع سياسات الأمان. • انشاء سياسات محددة لإدارة التحديثات بما في ذلك الجداول الزمنية وإجراءات الاختبار. • تطوير سياسة تحديثات منتظمة واختبارات فحص دورية لضمان سلامة الأنظمة والتطبيقات. • إعداد خطة استجابة للتهديدات الأمنية تشمل إجراءات للتعامل مع هجمات محتملة. و توزيع هذه الخطة على جميع الموظفين وتحديثها بانتظام.

المبادئ والركائز الأساسية للتحول الرقمي في قطاع الحكم المحلي:

المبادئ

1. المواطن هو محور عملية التحول الرقمي.
2. الحوكمة، الموثوقية والشفافية.
3. خدمات الهيئات المحلية يتم الوصول اليها من منصة او منصات رقمية يتم تطويرها من خلال الشراكة بين الهيئات المحلية والشركاء والمواطنين ومزودي الخدمة.
4. المرونة والاستدامة والتحسين المستمر.
5. سهولة الاستخدام وتمكين المستفيدين وتعزيز ثقافة التحول الرقمي.
6. ضمان أمن البيانات وخصوصيتها.
7. إمكانية التوافق والتبادل البيني.
8. ضمان قابلية التوسع والاستمرارية.
9. المبادئ الأخلاقية والعدالة.
10. الواقعية وقابلية التطبيق.

الركائز الأساسية

1. الاستراتيجيات والسياسات الوطنية المتعلقة بالتحول الرقمي.
2. التصميم المتمحور حول الانسان.
3. التعاون وتظافر الجهود.
4. التطوير الإداري والتقني.
5. تراكم الخبرات والمهارات.
6. توفر المصادر ومتطلبات التحول الرقمي.
7. إدارة التغيير.
8. إدارة المخاطر.

منهجية التحول الرقمي في قطاع الحكم المحلي:

تُعد إستراتيجية الرقمنة في قطاع الحكم المحلي ذات أهمية قصوى في توفير أساس ومرجع يتم تطبيقه لتحقيق التحول نحو هيئات محلية رقمية، وتعتبر مكونات الإستراتيجية بما فيها من أهداف ومبادئ وأسس مُحددًا رئيسيًا للاعتماد عليه في عملية التطبيق وإيجاد الطرق وتطوير الحلول اللازمة لتحقيق التطور المطلوب. لقد كشف تحليل الواقع للهيئات المحلية في مجال التحول الرقمي عن وجود تباين واضح بين الهيئات المحلية على مستوى التحول، وهو ما يؤكد على ضرورة وجود هذه الإستراتيجية واعتمادها كعنصر أساسي لقياس مدى التقدم في التحول الرقمي للهيئات المحلية.

استنادًا إلى تحليل الوضع الحالي للهيئات المحلية، وأخذًا في الاعتبار التجارب المكتسبة من الآخرين والممارسات الفضلى المتبعة، تتضح الحاجة لاعتماد منهجية خاصة للتحول الرقمي في قطاع الحكم المحلي يمكن تسميتها بـ "منهجية المراحل والتدرج والتحسين المستمر" بحيث تشمل جميع المجالات الضرورية للتحول، ومن هذه المجالات:

1. التحول في الإجراءات والعمليات: ومن ملامح التحول في هذا المجال تبسيط واختصار الإجراءات والعمليات التي تقوم بها الهيئة المحلية لتحسين جودة حياة المواطنين.
2. التحول في دقة المعلومات والأدوات الإدارية لضبط المعلومات.
3. التحول في استخدام التكنولوجيا: ومن ملامح التحول في هذا المجال وجود استثمارات مستدامة في تكنولوجيا المعلومات والاتصالات لإيجاد بنية تحتية مرنة بمعماريات مفتوحة.
4. التحول في ثقافة الهيئة المحلية والأفراد: ومن ملامح التحول في هذا المجال إدراك المشارك بأهمية دوره في النظام الكلي سواءً كان المشارك فردًا أو دائرة، وحرصه على ربط أهدافه بالأهداف الكلية للهيئة المحلية.
5. التحول في وعي وثقافة المجتمع بأهمية الاستفادة من خدمات الهيئات المحلية الإلكترونية.

وبشكل عام، فإن عملية التحول الرقمي هي عملية طويلة الأمد وتدريجية؛ وتستطيع كل هيئة محلية التركيز على كل مرحلة بما يتماشى مع رؤيتها ورسالتها، وبما يضمن التناغم مع استراتيجيات التحول الرقمي العامة لقطاع الحكم المحلي والسياسات الوطنية المعمول بها.

محاور وخارطة التنفيذ:

لضمان تنفيذ استراتيجية الرقمنة تحول الرقمي في قطاع الحكم المحلي بفعالية، مع مراعاة أهدافها ومبادئها وركائزها، يُصبح من الضروري تحديد المحاور الرئيسية لخارطة التنفيذ للاستراتيجية والتي يُمكن إيجازها على النحو التالي:

1. **محور الأنظمة والبرامج:**

- توفير الأنظمة والبرامج المحوسبة الفاعلة والموائمة لكافة أعمال الهيئة المحلية
- توفير الأنظمة والبرامج المطلوبة للحماية
- تطبيق سياسات لتكنولوجيا المعلومات في الأنظمة والبرامج
- توفر بيانات دقيقة في الأنظمة والبرامج

2. **محور البنية التحتية التكنولوجية:**

- توفير الأجهزة والمعدات المطلوبة لعملية التحول الرقمي
- توفير الأجهزة والمعدات المطلوبة للحماية
- توفير خطوط وأجهزة الاتصال المطلوبة
- تطبيق سياسات لتكنولوجيا المعلومات فيما يتعلق بالأجهزة والمعدات

3. **محور الخدمات الإلكترونية:**

- تصميم وتطوير الخدمات الإلكترونية باتباع منهجية التصميم المتمحور حول الإنسان
- تحديث سنوي ودوري لكتيب الخدمات والإجراءات في الهيئة المحلية.
- تقييم دوري وتحسين مستمر لجودة الخدمات الإلكترونية

4. **محور الاستدامة:**

- توفير أنظمة ومعدات للتعافي من الكوارث
- وجود موازنة خاصة لضمان استمرارية صيانة وتطوير الأنظمة والأجهزة
- التقييم والتحديث الدوري للأنظمة والبرامج والأجهزة والمعدات
- وجود سياسات لتكنولوجيا المعلومات معتمدة من قبل الهيئة المحلية
- بناء قدرات من خلال التدريب لكوادر الهيئات المحلية

5. **محور الثقة والثقافة:**
   - برامج توعوية لكوادر الهيئة المحلية
   - برامج وحملات توعوية للمواطنين
   - اعتماد وتطبيق حوافز لاستخدام الخدمات الإلكترونية
   - تطبيق أفضل الممارسات والسياسات المتعلقة بحماية البيانات الشخصية
   - توفير آليات فاعلة لمتابعة ودعم تقديم الخدمات الإلكترونية

ولوضع خارطة التنفيذ لتطبيق الاستراتيجية، وضعنا مراحل محددة للتطبيق والتقدم في تحقيق الأهداف الاستراتيجية والعمل على المحاور الأساسية في عملية التحول الرقمي، وفيما يلي المراحل الأساسية لخارطة التنفيذ، مع الأخذ بعين الاعتبار أنه بالإمكان تنفيذ أكثر من مرحلة بالتزامن وفقا لواقع الهيئة المحلية:

1. **المرحلة الأولى: مرحلة تحسين أداء الخدمات الداخلية والربط بين الأنظمة المحوسبة.**

تتميز هذه المرحلة بإجراءات عمل داخلية محوسبة تحقق سرعة استجابة ودقة في المعلومات تمهيدًا لإطلاق خدمات إلكترونية فاعلة وموثوقة، وتطبيق تسجيل الدخول الموحد (Single Sign On)، بما يضمن أكبر قدر من الدقة، وآليات محسنة في نظام الشكاوى والخدمات، مع مراعاة أن تكون الإجراءات التي تتبعها الهيئات المحلية تستند إلى أدلة إجراءات وتدقيق ممنهج من أجل ضمان دقة المعلومات ليتم استخدامها بالمراحل التالية.

2. **المرحلة الثانية: مرحلة بناء قدرات وتعزيز إدارة التغيير والصمود لضمان استمرارية الخدمات.**

تهدف هذه المرحلة لتعزيز إدارة التغيير داخل الهيئات المحلية وتدريب وتثقيف أعضاء مجالس الهيئات المحلية وموظفيها بأهمية الرقمنة لتحسين جودة حياة المواطنين. ويشمل ذلك دراسة نسبة جهوزية البنية التحتية التقنية والمعلوماتية للهيئات المحلية، وتحليل الفجوات وتحديد الاحتياجات وحجم العمل المطلوب. مع الأخذ بعين الاعتبار الأدوات والأنظمة المطلوبة للوصول إلى تعزيز الصمود الرقمي في حالة الكوارث والأحداث المناخية؛ حيث يتم احتساب نسبة دقة المعلومات التقنية للهيئات المحلية بناءً على تحليل مؤسسي يجب القيام به، ووجود خطة عمل مع تحديد المسؤوليات والإطار الزمني الخاص بتنفيذ كل خطة ومنهجية متابعة التنفيذ والتقييم ونذكر من تلك الخطط إنشاء سياسات تكنولوجيا المعلومات للهيئات المحلية وخطة دعم الصمود.

3. **المرحلة الثالثة: مرحلة تحسين الخدمات الإلكترونية الخارجية وتحسين الأدوات الرقمية للمواطنين.**

تعتبر مشاركة المواطنين وذوي العلاقة في تصميم الخدمات الرقمية عاملًا أساسيًا في نجاح إطلاق خدمات مُرقمنة من خلال أدوات موثوقة تعزز الثقة بها وتسهل استخدامها وتمكن المواطن من التعامل مع كافة معاملات الهيئة المحلية الخدماتية والمالية، مع التعزيز لتطبيق فكرة تسجيل الدخول الموحد للهيئات المحليات على المدى المتوسط والبعيد وبما يتوافق مع المستوى الوطني في فكرة تسجيل الدخول الموحد.

4. **المرحلة الرابعة: مرحلة تعزيز ثقافة المجتمع من أجل الوصول إلى مجتمع رقمي صامد.**

تهدف هذه المرحلة لتعزيز ثقافة المجتمع بحيث يتخللها لقاءات وإجراء استطلاعات رأي الجمهور واعتماد الشفافية في الإجراءات، حيث أن هناك أهمية قصوى لنشر الميزانية وإشراك المجتمع المحلي من خلال أنشطة توعوية رقمية وورشات عمل تعاونية موجهة للجمهور، بما يشمل عقد دورات تدريبية إدارية متخصصة للعاملين في الهيئة المحلية ذات العلاقة خاصة أولئك العاملين في مجال تكنولوجيا المعلومات والاتصالات للاستخدام الأمثل للتكنولوجيا الحديثة.

العلاقة بين الأهداف ومحاور ومراحل التنفيذ:

المرحلة	المحور/ المحاور	الهدف / الأهداف الاستراتيجية
المرحلة الأولى: مرحلة تحسين أداء الخدمات الداخلية والربط بين الأنظمة المحوسبة	الأنظمة والبرامج البنية التحتية التكنولوجية	تعزيز البنية التحتية الرقمية والأدوات التكنولوجية
المرحلة الثانية: مرحلة بناء قدرات وتعزيز إدارة التغيير والصمود لضمان استمرارية الخدمات	الاستدامة الثقة والثقافة	بناء القدرات وتعزيز إدارة التغيير تعزيز الثقافة والمجتمع الرقمي
المرحلة الثالثة: مرحلة تحسين الخدمات الإلكترونية الخارجية وتحسين الأدوات الرقمية للمواطنين	الخدمات الإلكترونية	تعزيز البنية التحتية الرقمية والأدوات التكنولوجية
المرحلة الرابعة: مرحلة تعزيز الثقافة المجتمع من أجل الوصول إلى مجتمع رقمي صامد	الاستدامة الثقة والثقافة	بناء القدرات وتعزيز إدارة التغيير تعزيز الثقافة والمجتمع الرقمي تعزيز الصمود الرقمي

جدول مؤشرات قياس تحقق الاستراتيجية:

الهدف الاستراتيجي	مؤشر الأداء/ المعيار	الفترة
تحسين خدمات قطاع الحكم المحلي (المرحلة الاولى)	الخدمات المحسنة بإجراءاتها وتفصيلاتها يتم تحديثها سنويًا على كتيب الإجراءات المعتمد من المجلس البلدي.	خلال أول سنتين
	وجود مركز أرشيف إلكتروني فعّال خاص بالخدمات المقدمة والمرفقات.	
	مقدار التحسينات في سرعة أداء الخدمات التي اعتمدها المجلس البلدي تتجاوز 20%.	
	عدد طلبات الخدمات المنجزة بالبلدية ضمن الوقت المخصص لها بنسبة تتجاوز 60%	
	عدد الطلبات العالقة بالبلدية لا تتجاوز 10%	
	نظام مركز خدمات جمهور يعمل ضمن إجراءات دليل الخدمة بالبلدية	
	وجود نظام شكاوى فعّال وتصنيفات الشكاوى واضحة	
	توحيد معلومات ملف المكلفين	
تعزيز البنية التحتية الرقمية والأدوات التكنولوجية (المرحلة الثانية)	وجود موازنة البلدية التكنولوجية بالموازنة المعتمدة للهيئة المحلية. تدعمها القرارات والأنشطة التي يتبناها مجلس الهيئة المحلية الداعمة للتحول إلى بلدية رقمية.	
	وجود خطط عمل مع تحديد المسؤوليات والإطار الزمني الخاص بتنفيذ كل خطة ومنهجية متابعة التنفيذ والتقييم بناءً على الموازنة.	
	نسبة جهوزية البنية التحتية التقنية والمعلوماتية للهيئات المحلية للتحول إلى بلديات مرقمنة بمقدار 70%.	
	تقييم تكنولوجي سنوي وتحديد الاحتياج التقني بما يتناسب مع موازنة البلدية التكنولوجية.	
	نسبة دقة المعلومات التقنية للهيئات المحلية للتحول إلى بلديات مرقمنة تتجاوز 80%	
	وجود أنظمة محوسبة مترابطة بأنظمة البلدية الأساسية (مركز الخدمات، النظام المالي، ونظام الشكاوى، ونظام الارشفة)	
	وجود تراخيص حماية وتطبيق سياسات تكنولوجيا المعلومات في الهيئات المحلية	
بناء القدرات وتعزيز إدارة التغيير (المرحلة الثالثة)	دورات تدريبية للعاملين في مجال الإدارة والخدمات والأدوات الرقمية	خلال 3 سنوات
	عدد السياسات/ الإجراءات/ التعليمات التي تُحفز الهيئات المحلية والمواطنين نحو استخدام الخدمات الإلكترونية	
	عدد التشريعات/ القوانين/ الأنظمة / اللوائح الداعمة لخدمات الرقمنة	
	نسبة زيادة الحسابات الإلكترونية النشطة من العدد الكلي للمكلفين	
	نسبة زيادة المعاملات الإلكترونية التي تم تنفيذها سنويًا من إجمالي المعاملات	

تعزيز الثقافة والمجتمع الرقمي (المرحلة الرابعة)	لقاءات واستطلاعات رأي جماهيرية	خلال 4 سنوات
	نشر موازنة المواطن لتحقيق الشفافية	
	نشاطات توعوية رقمية موجهة للجمهور	
	ورشات عمل أو دورات تدريبية إدارية متخصصة للعاملين	
	دورات تدريبية للعاملين في مجال تكنولوجيا المعلومات والاتصالات على الاستخدام الأمثل والتكنولوجيا الحديثة	
تعزيز الصمود الرقمي (المرحلة الرابعة)	وجود خطة صمود تشمل الصمود المعلوماتي والرقمي	
	عدد آليات العمل التنسيقية التي يتم تطبيقها بالمشاريع والتي تعزز من الصمود	
	نسبة تنفيذ خطة الصمود بالهيئة المحلية	

المتابعة والتقييم:

1. تطبيق الاستراتيجية هو مسؤولية الهيئات المحلية بشكل أساسي بالتعاون مع الشركاء ذوي العلاقة.
2. متابعة تطبيق الاستراتيجية تكون مسؤولية وزارة الحكم المحلي بشكل أساسي.
3. يتم تشكيل لجنة لمتابعة تطبيق الاستراتيجية؛ تكون اللجنة برئاسة وزارة الحكم المحلي وعضوية كل من الصندوق والاتحاد الفلسطيني للهيئات المحلية وأيه جهات أخرى تراها الوزارة مناسبة.
4. تكون مهام لجنة متابعة تطبيق الاستراتيجية كما يلي:

1) تقوم اللجنة بعقد اجتماعات دورية كل ثلاثة أشهر.
2) وضع النماذج والأدوات المطلوبة لمتابعة تحقيق الأهداف الاستراتيجية ومتابعة التنفيذ وفقًا لأسلوب ومؤشرات الأداء التي يمكن مراجعتها وتحسينها وفقا لتطورات الاستراتيجية وباتباع العملية التجريبية.
3) إجراء عمليات تقييم دورية لواقع الهيئات المحلية في مجال الرقمنة، تقوم اللجنة بالاستعانة بالاستشاريين لإجراء عملية التقييم بحسب الحاجة، مع مراعاة تحقيق الشفافية من خلال نشر نتائج التقييم.
4) وضع المقترحات لاستحداث برامج ومشاريع للمساعدة في تحقيق أهداف الاستراتيجية، والمشاركة في متابعة البرامج القائمة وتعزيز انسجامها مع الاستراتيجية.
5) إعداد تقارير دورية سنوية ورفعها لمعالي وزير الحكم المحلي بحيث تشمل كحد أدنى: نتائج تقييم واقع الهيئات المحلية، التحديات، الدروس المستفادة، والتوصيات.

ملحق رقم (1): تحليل الواقع الحالي لقطاع الحكم المحلي في مجال التحول الرقمي

تحليل الو اقع الحالي للهيئات المحلية:

(1) دراسة مسحية لتقييم و اقع تكنولوجيا المعلومات في الهيئات المحلية

قسّمت هذه الدراسة إلى سبعة أجزاء للإلمام بالوضع العام المتعلق بالرقمنة في الهيئات المحلية:

الجزء الأول: معلومات عامة.

الجزء الثاني: البنية التحتية الرقمية والأنظمة المحوسبة.

الجزء الثالث: الخدمات الرقمية

الجزء الرابع: خصوصية البيانات وأمن المعلومات

الجزء الخامس: كوادر التخطيط والتطوير وتكنولوجيا المعلومات

الجزء السادس: التعاون والمشاركة

الجزء السابع: التدريب وتقييم الأداء

وفيما يلي تفاصيل الاستمارة وجزئياتها:

استمارة تقييم و اقع تكنولوجيا المعلومات في الهيئات المحلية

الجزء الأول: المعلومات العامة:

اسم الهيئة المحلية	
عدد سكان الهيئة المحلية	
عدد موظفي الهيئة المحلية	
المحافظة	
تصنيف الهيئة المحلية	** ضع دائرة: (بلدية أ، بلدية ب، بلدية ج، مجلس قروي)
عدد موظفي تكنولوجيا المعلومات في الهيئة المحلية	
معلومات الاتصال للشخص الذي قام بتعبئة الاستمارة	الاسم:
	المسمى الوظيفي:
	رقم الجوال:
تاريخ تعبئة الاستمارة	

الجزء الثاني: البنية التحتية الرقمية والأنظمة المحوسبة:

	الفقرة	لا يوجد	ضعيفة	متوسطة	جيدة
2.1	وجود شبكة حاسوب وملحقاتها (جدار ناري، سويتشات، شبكات افتراضية، أجهزة توجيه) في الهيئة المحلية				
2.2	وجود غرفة خاصة للخوادم وإدارة شبكات الاتصال				
2.3	وجود أجهزة حاسوب وملحقاتها				
2.4	وجود خدمة انترنت				
2.5	وجود نسخ احتياطي واستعادة بيانات – داخل مبنى الهيئة				
2.6	وجود نسخ احتياطي واستعادة بيانات – خارج مبنى الهيئة				
2.7	القدرة التخزينية الاجمالية				
2.8	توفر خدمات سحابية				
2.9	يوجد لدى الهيئة المحلية مركز استعادة من الكوارث				
2.10	مدى أتمتة إجراءات العمل الداخلية				
2.11	مدى توفر واستخدام أنظمة المعلومات الجغرافية (GIS)				

الجزء الثالث: الخدمات الرقمية:

	الفقرة	لا يوجد	ضعيفة	متوسطة	جيدة
3.1	توفر موقع الكتروني رسمي للهيئة المحلية				
3.2	توفر تطبيقات (ويب / محمولة) لاستخدام المواطنين للوصول الى معلومات الهيئة المحلية				
3.3	توفر تطبيقات (ويب / محمولة) لاستخدام المواطنين للوصول الى الخدمات المقدمة من الهيئة المحلية				
3.4	توفر خدمات الكترونية لدفع الفواتير مثل فواتير الكهرباء والمياه.				
3.5	توفر خدمات إلكترونية للمعاملات في الهيئة المحلية مثل معاملات التراخيص				
3.6	مدى مراعاة بناء الخدمات الإلكترونية المقدمة لذوي الإعاقة				
3.7	مدى مشاركة المواطنين في تصميم وبناء الخدمات الإلكترونية				

الجزء الرابع: خصوصية البيانات وامن المعلومات:

	الفقرة	لا يوجد	ضعيفة	متوسطة	جيدة
4.1	توفر إجراءات امنية لحماية بيانات الهيئة المحلية والمواطنين				
4.2	مدى تطبيق سياسات امن المعلومات للأنظمة الالكترونية في الهيئة المحلية				
4.3	تطبيق سياسات استعادة البيانات وعدم وقوعها في المكان الخطأ				
4.5	تطبيق إجراءات خصوصية البيانات للمواطنين في الهيئة المحلية				
4.6	مدى تنفيذ تقييمات أمنية من قبل جهات خارجية				

الجزء الخامس: التخطيط والتطوير وكادر تكنولوجيا المعلومات:

	الفقرة	لا يوجد	ضعيفة	متوسطة	جيدة
5.1	وجود استراتيجيات تحول الهيئة المحلية الى النظام الرقمي				
5.2	وجود خطة لتحسين البنية التحتية الرقمية والتحول الرقمي				
5.3	وجود ميزانية محددة وكافية لدعم التحول الرقمي في الهيئة المحلية				
5.4	وجود مشاركة للمواطنين في وضع استراتيجيات التحول الرقمي للهيئة المحلية				
5.5	مدى كفاية كادر تكنولوجيا المعلومات في الهيئة المحلية – من ناحية العدد				
5.6	مدى كفاية كادر تكنولوجيا المعلومات في الهيئة المحلية – من ناحية القدرة والخبرات المطلوبة				
5.7	مدى توفر كادر متخصص ببناء تطبيقات الويب والتطبيقات المحمولة				
5.8	مدى توفر شخص متخصص بأمن المعلومات				
5.9	مدى توفر شخص متخصص بمجال أنظمة المعلومات الجغرافية				

الجزء السادس: التعاون والمشاركة:

	الفقرة	لا يوجد	ضعيفة	متوسطة	جيدة
6.1	وجود تعاون وتعاقدات مع القطاع الخاص للاستفادة من الخبرات في التحول الرقمي للهيئة المحلية				
6.2	وجود تعاون مع المؤسسات الاكاديمية للاستفادة من الخبرات في التحول الرقمي للهيئة المحلية				
6.3	وجود شراكات مع الجهات المجتمعية المحلية لتعزيز التحول الرقمي				
6.4	وجود شراكات مع جهات إقليمية أو دولية في مجال التحول الرقمي				

الجزء السابع: التدريب وتقييم الأداء:

	الفقرة	لا يوجد	ضعيفة	متوسطة	جيدة
7.1	توفر برامج تدريب وتوعية رقمية للموظفين لتحسين مهاراتهم الرقمية				
7.2	توفر حملات تدريب وتوعية للمواطنين لزيادة وعيهم التقني والرقمي				
7.3	وجود تقييمات دورية لفحص جاهزية التحول الرقمي وقياس تقدم الهيئة المحلية				
7.4	وجود تقييمات دورية لفحص تقبل ورضى المواطنين للخدمات الالكترونية المقدمة				
7.5	توفر تحليل لنتائج التقييمات الدورية وبرامج التدريب والتوعية				

الجزء الثامن: العقبات والتحديات:

أسئلة مفتوحة: يرجى التكرم والاجابة عن الأسئلة التالية:

السؤال الأول: ما هي العقبات والتحديات الرئيسية التي تواجه الهيئة المحلية في تحقيق التحول الرقمي؟

السؤال الثاني: ما هي المقترحات لتحسين مستوى التحول الرقمي في الهيئة المحلية؟

---

(2) المنهجية

تم نشر استمارة الدراسة المسحية باستخدام نماذج جوجل ، وتم تحديد موعد انتهاء تعبئة الاستمارة بتاريخ 2023/8/31. قام الفريق بدوره بالمتابعة لزيادة عدد الردود من خلال المكالمات الهاتفية والبريد الالكتروني. وكان إجمالي عدد الإجابات التي تم استقبالها بحلول تاريخ الانتهاء هو (86) ست وثمانون إجابة .

تم الاتفاق على اتباع آلية تجميع للاستمارات بهدف التحليل بحيث تكون كما يلي : (بلديات أ، بلديات ب، بلديات ج ، المجالس القروية) .

تمت تصفية ومعالجة البيانات الواردة في الاستمارات ، وتم تشفير الأسئلة بمعرِّفات مميزة باستخدام معايير البيانات المفتوحة ، علاوة على ذلك أُعطي اهتمام خاص لخصوصية البيانات وذلك بإزالة أية معلومات شخصية وبالتحديد بيانات الاتصال.

طبق مقياس ليكرت ذو الأربع نقاط لتحويل البيانات من نوعي إلى كمي لتسهيل عملية التفسير والتحليل الإحصائي لها . حيث اعتمد نظام تقييمي يستخدم مقياس نقطي يبدأ ب 1 وينتهي ب 4. حيث يكافئ 1 لا شيء ، 2 تعني ضعيف ،3 متوسط و 4 جيد. بعض الإجابات أعطت أكثر من نقطة تقييمية ولذلك تم أخذ أدناها بعين الاعتبار بهدف دقة الدراسة.

عولجت متغيرات أعداد السكان وأعداد موظفي الهيئات المحلية بشكل خاص من خلال اتباع أسلوب الفترات الاحصائية ، بهدف تسهيل عملية التحليل الإحصائي وللسماح بمعالج التقارير الجدولي بالتعرف على الروابط و التقاطعات بين البيانات

تم أيضاً تجميع البيانات من الجزء 2 وحتى الجزء 7 ضمن موضوعات معينة لتيسير عملية التحليل وفقا للمحافظات ولتصنيف الهيئات المحلية .

(3) نتائج عامة

أ. الجزء الثاني: البنية التحتية الرقمية والأنظمة المحوسبة

يوجد بنية تحتية رقمية و أنظمة محوسبة وما يرتبط بها من أدوات تكنولوجيا المعلومات و توفير خدمات داخلية رقمية واستضافة داخلية للأنظمة . حيث أظهرت الدراسة أن 55.8% من الهيئات المحلية لديها بنية تحتية رقمية وأنظمة محوسبة بدرجة متوسطة ، كما أظهرت الدراسة أن 44 % من الهيئات المحلية لديها خدمات الانترنت واستضافة داخلية للأنظمة . تظهر الدراسة أيضا عدم وجود مراكز استعادة من الكوارث.

ب. الجزء الثالث : الخدمات الرقمية

أظهرت الدراسة أن 79 % من الهيئات المحليه تفتقر الى وجود خدمات رقمية أو أن لديها خدمات رقمية بمستوى ضعيف ، كما أظهرت أن 15 % من الهيئات المحلية لديها خدمات رقمية بمستوى متوسط .

بخصوص المواقع الالكترونية أظهرت الدراسة أن 44 % من الهيئات المحلية لديها مواقع الكترونية رسمية ، و كذلك أظهرت أن 15 % من الهيئات المحلية ليس لديها اية صفحة الكترونية رسمية .

ج.الجزء الرابع: خصوصية البيانات وأمن المعلومات.

47.7% من الهيئات المحلية تراعي وتهتم بالمحافظة على خصوصية البيانات ولديها أنظمة لأمن المعلومات، بينما 37.2% من الهيئات المحلية ليس لديها هذه الأنظمة أو أنها موجودة بأشكال بدائية.

فيما يخص تقييم المخاطر، أظهر المسح أن 50% من الهيئات المحلية لم تقم بأي شكل من اشكال تقييم المخاطر من قبل طرف ثالث.

د. الجزء الخامس: التخطيط والتطوير وكادر تكنولوجيا المعلومات.

يعاني مجال التخطيط والتطوير و كادر تكنولوجيا المعلومات من نقص بنسبة 58.1%، لعدة أسباب من أهمها عدم تخصيص الموازنات المطلوبة . هنالك أيضًا نقص في مشاركة المواطنين في معظم الهيئات المحلية في وضع استراتيجيات التحول الرقمي. يتمتع فقط 37.2% من هذه الهيئات باستراتيجيات نشطة وميزانية محددة وكوادر في مجال تكنولوجيا المعلومات.

هـ. الجزء السادس: التعاون والمشاركة.

يظهر وجود قصور في التعاون في مجال الابتكار الرباعي (القطاع الخاص، القطاع الأكاديمي، المجتمعات المحلية، المؤسسات الإقليمية والدولية)، والذي قد يعيق تنفيذ الاستراتيجية الوطنية الرقمية على مستوى الحكم المحلي. يشير المسح إلى أن 42% من الهيئات المحلية لا يوجد لديها أي تعاون مع القطاع الخاص و22 % منها لديها القليل من التعاون ، و لا يوجد تعاون مع القطاع الأكاديمي بنسبة 81%، و لا يوجد تعاون مع المجتمعات المحلية بنسبة 83%، بينما وصلت نسبة عدم وجود تعاون بين الهيئات المحلية والهيئات الإقليمية أو الدولية الى 86% .

و. الجزء السابع: التدريب وتقييم الأداء.

تبين أن 86% من الهيئات المحلية لا تمتلك أية آليات للتدريب وتقييم الأداء، حيث تشير الدراسة الى أن 54.7% منها ليس لديها أية آليات ، و31.4% لديها آليات ولكن تصنف بأنها ضعيفة للغاية.

أظهرت الدراسة أيضا أن 2.3% فقط من الهيئات المحلية تمتلك آليات فعّالة للتدريب و تقييم الأداء.

(4) العلاقات بين المتغيرات المختلفة

تم تحليل العلاقات بين المتغيرات المختلفة بهدف الحصول على مزيد من الملاحظات والنتائج ، حيث عولجت المتغيرات المعلوماتية العامة المتعلقة بالمحافظات وتصنيفات الهيئات المحلية وعدد موظفيها وكذلك وضع الرقمنة فيها باستخدام معالج التقارير crosstab ، حيث تم ربطها وتحليلها مع المجالات الست الواردة في الدراسة ، وكانت كما يلي :

أ. المحافظات :

تفوقت الهيئات المحلية في قطاع غزة على تلك في الضفة الغربية في جميع التصنيفات الستة. وصلت محافظتا رام الله وخان يونس إلى مكانة متقدمة بفضل امتلاكهما أنظمة فعّالة في جميع التصنيفات الستة. على الجانب الآخر، أشارت جميع المحافظات عدم امتلاك بعض الهيئات المحلية للخدمات الإلكترونية، وكثير منها أشار عن وجود أنظمة لحماية خصوصية البيانات وأمان المعلومات تعمل بشكل متوسط. وفي سياق آخر، يظهر نقص في كوادر التخطيط والتطوير وتكنولوجيا المعلومات في نصف المحافظات، بالإضافة إلى نقص في التعاون والمشاركة، وانعدام أو ضعف في الأنظمة المتخصصة في التدريب وتقييم الأداء في جميع المحافظات.

ب. تصنيفات الهيئات المحلية وعدد الموظفين :

فيما يتعلق بالتصنيفات وعدد الموظفين، تظهر أن الهيئات المحلية في المجالس القروية تحتوي على أقل من عشرة موظفين. وفي بلديات منطقة ج، يتراوح عدد الموظفين بين 10 و49 موظفًا في 29 هيئة محلية، حيث أفادت اثنتان منها بوجود 400 أو 500 موظف، وكلاهما في قطاع غزة، ويتراوح التعداد السكاني لكل منهما بين 230,000 و470,879. أما بلديات منطقة ب، فتمتلك عددًا أكبر من الموظفين يتراوح بين 10 ويصل إلى أكثر من 1000 موظف. ومعظمها يحتوي على موظفين بعدد يتراوح بين 25 و49 موظفًا، واثنتان في منطقة أ يمتلكان من 50 إلى 74 موظفًا، أما الباقي فيتجاوز إجمالي عددهم المئة.

ج. تصنيفات الهيئات المحلية ووضع الرقمنة فيها :

تظهر معظم الهيئات المحلية، بغض النظر عن تصنيفاتها، وجود أسس رقمية حالية بجودة متوسطة. تبين أن الخدمات الإلكترونية فيها معدومة أو ضعيفة في جميع الأقسام، وأن البلديات في منطقة ج تعاني من أعلى نسبة نقص في هذه الخدمات، على الرغم من توفر خصوصية البيانات وأمان المعلومات بشكل جيد. أما كوادر التخطيط والتطوير وتكنولوجيا المعلومات، فإما أن تعاني من ضعف أو تكون بجودة متوسطة في جميع الثلاث والستين بلدية وفي جميع التصنيفات الأربع. وأخيرًا، يظهر أن التعاون والمشاركة والتدريب وتقييم الأداء في جميع الهيئات المحلية ضعيفة أو غير موجودة على الإطلاق.

د. عدد الموظفين و وضع الرقمنة :

بغض النظر عن حجم الهيئات المحلية، يظهر أن معظمها يتمتع بالبنية الأساسية للرقمنة. ومع ذلك، تبين أن الخدمات الإلكترونية ضعيفة أو معدومة في التصنيفات بجميع الأحجام باستثناء تلك التي تمتلك أكثر من 1000 موظف. وجميع الهيئات تمتلك خصوصية جيدة للبيانات وأمان جيد للمعلومات، باستثناء تلك التي تمتلك موظفين في نطاق من 10 إلى 24 موظفًا. ويظهر أن هناك ثلاث مجموعات فقط تتمتع بكوادر جيدة في التخطيط والتطوير وتكنولوجيا المعلومات، وتظهر مستوى جيد في التعاون والمشاركة أيضًا. ومع ذلك، يعاني البقية من ضعف أو انعدام في كل من التعاون والمشاركة. وجميع المجموعات أكدت على ضعف أو انعدام وجود برامج للتدريب وتقييم الأداء.

انعكاس و أثر *نتائج* التحليل الخاص بالهيئات المحلية على استراتيجية الرقمنة في قطاع الحكم المحلي

على الرغم من وجود أنظمة محوسبة وملحقات جيدة، واتصال إنترنت جيد في الهيئات المحلية، إلا أن هناك نقصًا في الأسس الضرورية مثل مراكز البيانات ومراكز استرجاعها لتتناسب مع الخدمات الإلكترونية التي يتم طرحها للمواطنين، وتحسين عمل الهيئات المحلية. ولذا، يُفضل إنشاء هذه المراكز للبيانات والاستفادة من المراكز الموجودة كبديل مساعد أو كمراكز لاسترجاع البيانات. الخدمات الإلكترونية ضعيفة أو معدومة في جميع التصنيفات، رغم أن توفيرها للمواطنين يجب أن يكون سلسًا وغير منقطع ومتاحًا بشكل فوري . كما يجب أن تكون هذه الخدمات متصلة بالحكومة المركزية لتسهيل الوصول إليها والتعامل معها، وهذا يجب أن يكون جزءًا من البنية الأساسية في خطط الهيئات المحلية السنوية.

هذا وبين المسح ان 63 من البلديات تعاني من ضعف في كوادر التخطيط والتطوير وتكنولوجيا المعلومات أيضًا وفي التصنيفات الأربعة كلها. ولذلك، يجب النظر في هذا الموضوع بجدية في الخطط السنوية لتسريع عملية الرقمنة في كافة الهيئات المحلية. تضعف أيضًا آليات المشاركة والتعاون والتدريب وأنظمة تقييم الأداء في جميع تصنيفات الهيئات المحلية. وهذا يستدعي التزامًا جادًا من قبل وزارة الحكم المحلي وصندوق الإقراض والتطوير والاتحاد الفلسطيني للهيئات المحلية لتقوم كل من هذه الأطراف بدورها في مواجهة هذه المشاكل ورعاية مشروع التحول الرقمي كجزء من التخطيط المنهج والعمل نحو توفير خدمات إلكترونية بشكل سلس للمواطنين وموظفي الهيئات المحلية.

التحليل الرباعي (SWOT) لو اقع تكنولوجيا المعلومات في الهيئات المحلية :

نقاط القوة (Strengths)	نقاط الضعف (Weaknesses)
بنية تحتية رقمية متوسطة الدرجة : وجود بنية تحتية رقمية وأنظمة محوسبة في أكثر من نصف الهيئات المحلية يعكس استعدادها للاستفادة من التكنولوجيا الرقمية لتعزيز الأداء وتحسين الخدمات.	نقص الخدمات الإلكترونية : تفتقر غالبية الهيئات المحلية إلى تقديم خدمات إلكترونية فعّالة، مما يعيق قدرتها على تلبية احتياجات المواطنين بشكل فعال وتعزيز التفاعل بين الحكومة المحلية والمجتمع.
أنظمة أمان المعلومات وحماية البيانات : وجود أنظمة لأمان المعلومات بدرجة مقبولة لدى عدد جيد من الهيئات المحلية وخاصة البلديات يوضح الاهتمام بحماية البيانات والمعلومات الحساسة، مما يخلق ثقة أكبر للمواطنين والمستفيدين من الخدمات الحكومية.	نقص كوادر التخطيط والتطوير وتكنولوجيا المعلومات : يعيق نقص الكوادر المؤهلة في هذا المجال قدرة الهيئات المحلية على تطوير وتحسين البنية التحتية الرقمية وتقديم خدمات أفضل.
وجود مواقع إلكترونية رسمية لدى بعض الهيئات المحلية: يمثل وجود مواقع إلكترونية رسمية لدى الهيئات المحلية فرصة لتعزيز التواصل مع المواطنين وتقديم الخدمات بشكل أفضل وأكثر شمولاً.	ضعف التعاون في مجال الابتكار المرتبط بالتحول الرقمي مع القطاع الخاص والقطاع الأكاديمي والمجتمعات المحلية والهيئات الإقليمية
	عدم وجود مراكز استعادة من الكوارث
	عدم تقييم المخاطر بشكل كافٍ : قد يؤدي عدم تقييم المخاطر بشكل كافٍ إلى تعرض الهيئات المحلية لمخاطر محتملة تهدد استمرارية العمل وجودته.
	محدودية البرامج التدريبية والحملات التوعوية في مجال الرقمنة
الفرص (Opportunities)	**التهديدات (Threats)**

الاهتمام الحكومي على المستوى الوطني في مجال التحول الرقمي والعمل على توفير متطلبات التحول من النواحي القانونية والإدارية والمالية والفنية	التحديات المالية والميزانية المحدودة : يمكن أن تحد من القدرة على الاستثمار في تحسين البنية التحتية الرقمية وتقديم الخدمات الإلكترونية بشكل كامل وشامل.
التطور المتسارع في مجال تكنولوجيا المعلومات مما يتيح إمكانية توفير خدمات رقمية بجودة عالية	التعرض لهجمات سبرانية في ظل عدم وجود إجراءات أمنية كافية (تقييمات أمنية من جهات خارجية ، مراكز استعادة من الكوارث)
تعزيز التعاون مع القطاع الخاص والقطاع الأكاديمي والمجتمعات المحلية والهيئات الإقليمية : فرصة لتبادل المعرفة والخبرات وتطوير الحلول التكنولوجية بشكل مشترك، مما يسهم في تعزيز القدرات وتطوير الخدمات.	عدم استقرار الوضع الأمني والسياسي

لذا، ينبغي على الهيئات المحلية تبني استراتيجيات شاملة تستفيد من القوى وتعمل على تحسين الضعف والاستفادة من الفرص المتاحة، بينما تتخذ إجراءات للتصدي للتهديدات المحتملة.

تقيم و اقع تكنولوجيا المعلومات في كل من:
(وزارة الحكم المحلي, صندوق تطوير و اقراض الهيئات المحلية, الاتحاد الفلسطيني للهيئات المحلية)

الأسئلة التي تم اعتمادها كأساس في عملية تقييم المؤسسات ذات العلاقة بالهيئات المحلية:

البنية التحتية لتكنولوجيا المعلومات:

1. ما هو نوع البنية التحتية المستخدمة في المؤسسة (محلية، سحابية، هجينة)
2. ما هو الغرض الأساسي لكل خادم (خادم البريد الإلكتروني، قواعد البيانات، خادم الويب)
3. مواصفات الأجهزة لكل خادم مثل سعة الذاكرة والمعالج
4. نظام التشغيل الذي يعمل على كل خادم
5. هل الخوادم موزعة في موقع واحد ام توجد في أماكن مختلفة
6. هل يتم استخدام تقنيات التجميع على الخوادم (clustering) او توازن الحمولة (load balancing)
7. ما هي إجراءات الأمان المتبعة على مستوى الخوادم مثل أنظمة الحماية من الهجمات والجدران النارية؟
8. هل يوجد سياسة لاستبدال الخوادم القديمة بأحدث التقنيات
9. هل يتم استخدام أنظمة افتراضية مثل الخوادم الافتراضية؟ تفاصيل حول استخدامها وادارتها
10. ما هي التقنيات المستخدمة لضمان استدامة وتوفر البنية التحتية
11. هل يتم استخدام أجهزة شبكية مثل جدران الحماية و routers وfirewallsوماهي تكوينها؟

الشبكة والاتصالات:

1. يرجى وصف الشبكة المستخدمة في المؤسسة (سلكية او لاسلكية) ونوع التكنولوجيا المستخدمة (Ethernet cat 5 or 6, Wi-Fi or Wi-Fi 6)
2. يرجى وصف توبو لوجيا الشبكة (الشبكة النجمية، الحلقية، الشبكة الشجرية)
3. هل يتم استخدام تقنية توزيع الاحمال (load balancing) لتحسين أداء الشبكة؟
4. هل يتم استخدام أنظمة تجميع البيانات (aggregation Switches) لربط الشبكات الفرعية؟
5. ما هي التقنيات المستخدمة لتأمين الشبكة من الهجمات الالكترونية واختراق البيانات
6. هل يتم استخدام أنظمة اكتشاف التسلل (Intrusion Detection Systems) لمراقبة وكشف أنشطة غير مرغوبة على الشبكة؟
7. كيف يتم تأمين ومراقبة الاتصالات مع الشبكات الخارجية
8. هل يتم استخدام خوادم IPو DHCPوكيف تتم إدارة توزيع العناوين؟
9. كيف يتم الاتصال بشكل آمن عن بعد؟ هل يتم استخدام شبكات افتراضية خاصة (VPN)
10. كيف تتم إدارة ورصد الشبكة؟ هل يتم استخدام أدوات خاصة لرصد أداء الشبكة وصيانتها

امن المعلومات:

1. ما هي التدابير الأمنية التي تتخذونها لحماية بيانات المؤسسة والمعلومات الأخرى
2. ما هي التهديدات الأمنية التي تتعرض لها المؤسسة والبيانات، مثل الهجمات الإلكترونية أو التسريبات؟

3. هل تستخدم المؤسسة أنظمة اكتشاف التسلل (Intrusion Detection Systems) للكشف عن أنشطة غير مصرح بها؟
4. كيف يتم مراقبة أنشطة الأمان والتحقق من سلامة الأنظمة بشكل منتظم؟
5. هل لديكم خطط طوارئ للتعامل مع انقطاع الخدمات أو الهجمات السيبرانية؟
6. كيف تضمنون استعادة البيانات واستئناف الأعمال بسرعة في حالة حدوث خلل أمني أو توقف؟
7. هل تستخدموا أنظمة تشفير للبيانات عند النقل والتخزين
8. كيف تتم إدارة تصاريح الوصول الى البيانات والموارد في المؤسسة
9. هل يتم تطبيق مبدأ الحد الأدنى من الامتيازات (Least Privilege) للموظفين؟
10. كيف تعززون التوعية الأمنية بين الموظفين والمستخدمين؟ هل تقومون بتقديم دورات تدريبية حول أمن المعلومات والسلوك الآمن.

إدارة البيانات

1. ما هو نوع البيانات التي تتعاملوا معها في المؤسسة؟
2. كيف يتم تخزين وإدارة البيانات في المؤسسة؟ هل تستخدموا أنظمة قواعد البيانات؟
3. كيف يتم تخزين البيانات في المؤسسة؟ هل تستخدمون أنظمة تخزين محلية أو سحابية؟
4. هل تستخدمون نماذج محددة لتخزين وتنظيم البيانات، مثل نموذج العلاقات أو نموذج الوثائق؟
5. ما هي الهياكل والترتيبات التي تستخدمونها لتنظيم البيانات داخل قواعد البيانات؟
6. كيف تضمنون جودة البيانات؟ هل تستخدمون إجراءات للتحقق من دقة واكتمال البيانات المخزنة؟
7. هل تدمجون بيانات من مصادر مختلفة، مثل التطبيقات الخارجية أو البيانات من فروع فرعية؟
8. كيف تتعاملون مع أمان البيانات؟ هل هناك إجراءات لمنح صلاحيات الوصول إلى البيانات بناءً على دور المستخدم؟
9. ا هي الإجراءات المتبعة لحماية البيانات الحساسة من الوصول غير المصرح به؟
10. ما هي إجراءات النسخ الاحتياطي للبيانات التي تستدمونها لضمان توفر البيانات في حال حدوث خلل
11. هل هناك اختبارات دورية لاستعادة البيانات من النسخ الاحتياطية للتأكد من فعالية عمليات الاستعادة؟
12. في حالة عمل نسخ احتياطية خارج المؤسسة اين يتم تخزين هذه البيانات (الدولة، المدينة)؟
13. ما هي أنظمة إدارة النسخ الاحتياطية المستخدمة في المؤسسة؟
14. التكنولوجيا المستخدمة في اخذ النسخ الاحتياطية للبيانات؟
15. آلية النسخ الاحتياطي (يدوي، تلقائي) والفترة الزمنية بين كل نسخة من البيانات؟

إدارة الخدمات والصيانة:

1. كيف يتم إدارة وصيانة الأجهزة والبرمجيات في المؤسسة؟ هل تستخدموا نظم إدارة الخدمات؟
2. كيف يتم تتبع وتوثيق الأعطال والمشاكل التي يمكن ان تحدث في الأنظمة والبنية التحتية
3. هل لديكم خطط صيانة دورية للأجهزة والبرمجيات؟
4. كيف يتم إدارة عمليات التحديث والترقية للبرمجيات
5. ماهي السياسة المعتمدة لإدارة تحديثات الأمان؟
6. هل توجد إجراءات تحديث دورية للبرمجيات وتطبيقات الأمان للبيانات؟

طو اقم تكنولوجيا المعلومات:

1. كم عدد افراد تكنولوجيا المعلومات في المؤسسة؟ وما هي التخصصات والوظائف التي يشملها الفريق
2. كيف يتم تخطيط وتنسيق اعمال تكنولوجيا المعلومات لضمان تقديم الدعم والخدمات بشكل فعال؟
3. كيف يتم توزيع المهام وإدارة الأولويات؟
4. هل تستخدموا أدوات إدارة المشاريع لمراقبة وتنسيق اعمال الفريق؟
5. كيف تقومون بتطوير مهارات أعضاء الفريق؟
6. ما هي الجهود المبذولة لمواكبة التطورات التكنولوجية؟
7. كيف يتعامل الفريق مع الازمات التكنولوجية؟

(أ) تحليل الو اقع الحالي لوزارة الحكم المحلي:

المشاهدات وملخص الإجابات على الأسئلة:

البنية التحتية لتكنولوجيا المعلومات:

1. البنية التحتية لتكنولوجيا المعلومات في وزارة الحكم المحلي تعتمد بشكل اساسي على خوادم موجودة في مقر الوزارة حيث يوجد العديد من الخوادم مثل (خادم نظام الارشفة الالكترونية ، نظام شؤون الموظفين، نظام بوابة الموازنات) وجميع هذه الخوادم موجودة بشكل كامل داخل مقر الوزارة ، بينما يتم استخدام خوادم لأنظمة أخرى لدى مركز الحاسوب الحكومي التابع لوزارة الاتصالات وتكنولوجيا المعلومات .
2. تستخدم الوزارة خوادم من نوع (Blade Server) ويتم تقسم موارد هذه الخوادم بإستخدام (VMware) وتستخدم فيها انظمة تشغيل (Windows Server 2018, Windows Server 2016 & Linux) بإستثناء خادم نظام الجيو مولج (Geo-MOLG) موجود على خوادم الحاسوب الحكومي الموجود في وزارة الاتصالات وتكنولوجيا المعلومات, وبخصوص البريد الالكتروني تستخدم الوزارة البريد الالكتروني الحكومي الموحد والموجود ايضا في مقر وزارة الاتصالات وتكنولوجيا المعلومات.
3. الخوادم الموجودة داخل مقر الوزارة تستعمل نظام التجميع على الخوادم (Clustering) ونظام (Load Balancing) بدرجات متفاوتة على كل خادم او (VM).
4. يتم حماية هذه السيرفرات الموجودة في مقر الوزارة من خلال ابواب امان بإستخدام الرقم السري مع وجود الرقم السري مع عدد محدود من موظفي تكنولوجيا المعلومات في الوزارة فقط ، وبخصوص بيانات هذه الخوادم تتم حمايتها بإستخدام (Fortinet Gate Firewall) وايضا نظام (Endpoint Antivirus) .
5. بخصوص سياسات استبدال الاجهزة او البنية التحتية فإنها موجودة ولكن مدى تنفيذها مرتبط بالعامل المادي وتوفره في الوزارة .
6. يستخدم نظام (VEEM) لانشاء انظمة افتراضية وانشاء خوادم افتراضية ، حيث ان نظام (VEEM) يحوى الكثير من الميزات والادوات لضمان استدامة البيانات ويتم الربط ما بين هذه السيرفرات من خلال (V-Lan) لضمان تبادل البيانات وجودة النقل ما بينها.

الشبكة والاتصالات:

1. تستعمل الوزارة شبكة انترنت سلكية باستخدام كوابل (CAT7) وايضا شبكة لاسلكية باستخدام نظام (WIFI 6) والشبكتين خاضعتين لنفس القواعد (Rules) لضمان نقل آمن للبيانات ولا يوجد فصل ما بينهما من حيث نوعية الاجهزة المرتبطة بها . تستخدم كل من الشبكتين نظام توزيع الاحمال (Load Balancing) حيث ان لكل طابق في مقر الوزارة شبكة موزعة ويتم ربطها مع الشبكة الرئيسية ،

وبخصوص المديريات لكل مديرية شبكتها الخاصة ونظام عناوين مختلفة عن الشبكة الام ولكن يتم ربطها من خلال خادم موجود في كل مديرية ، من خلال الشبكات الفرعية والشبكة الرئيسية يتم استعمال (Aggregation Switches) لربطها مع بعض لضمان ارسال واستقبال البيانات حيث يستعمل داخل مقر الوزارة (floor Switches) و (Core Switches).

2. يتم تأمين الشبكة من خلال استخدام (Fortinet Gate Firewall, Endpoint Antivirus) لضمان عدم وجود اختراق او تسريب للبيانات وايضا يتم مراقبة الاتصالات الخارجية مع المديريات او الحاسوب الحكومي بإستخدام (VPN) ، كمان ان الوزارة تفتقر لانظمة اكتشاف التسلل (Intrusion Detection System).
3. يتم توزيع العناوين (IPs) من خلال خادم (DHCP) من خلال استخدام تقنية (V-Lans) واعطاء العناوين لكل جهاز جديد بناء على توزيع الطوابق (floor) ومن خلال هذه التقنية تتم ادارة العناوين القديمة او الجديدة.

امن المعلومات:

1. تم حماية البيانات الموجودة على الخوادم وخصوصا ان هذه الخوادم موجودة داخل مقر الوزارة بطريقتين الطريقة الاولى وجود انظمة حماية وكاميرات مراقبة لمنع الوصول بشكل مباشر لهذه البيانات, وبخصوص الوصول الالكتروني يتم حمايتها من خلال الجدار الناري و مضاد الفيروسات, كما يتم حمايتها بأخذ نسخة احتياطية محلية لهذه البيانات.
2. اكثر انواع التهديدات الالكترونية التي تتعرض لها تهديد منع الوصول للخدمة ((Denial-of-Service (DoS) ولكن مع وجود هذا التهديد لا ان الوزارة تستخدم اداوت اساسية وليس متقدمة لمنع هذه التهديديات ولا تستخدم انظمة اكتشاف التسلل (Intrusion Detection System) لحماية بيانات الوزارة. يتم مراقبة انظمة الامان من انها تعمل بشكل سليم من خلال اخذ التحديثات للانظمة التشغيل وايضا تحديثات مضاد الفيروسات, مع العلم انه لا توجد لدى الوزارة اي خطط طوارئ لتعامل مع انفطاع الخدمات او الهجمات السيبرانية.
3. في حال حدوث اي مشاكل متعلقة بالبيانات يتم استعادة البيانات من خلال النسخ الاحتياطية المحلية وبخصوص البيانات الموجودة على السحابة الالكترونية ايضا تعتبر محلية اذ انها موجودة في الحاسوب الحكومي الموجود تقريبا في نفس البقعة الجغرافية,وان البيانات الموجودة على السحابة الالكترونية لا يتم تشفيرها من قبل الوزارة وانما يعتمد على الحاسوب الحكومي في عملية تشفير البيانات.
4. تمم ادارة وصول المستخدمين للبيانات الموجودة على الانظمة من خلال استخدام (User Authentication Login) وايضا نظام صلاحيات للمستخدمين للوصول الى الملفات من خلال الجدار الناري (Users Rule).
5. لا توجد اي دورات او ورشات تقنية او فنية للموظفين لتعزيز الوعي الامني للبيانات او الهجمات الالكترونية التي من الممكن ان تتعرض لها الوزارة وطرق الوقاية منها او دورات بخصوص السلوك الامني للمعلومات.

ادارة البيانات:

1. تستخدم الوزارة تقريبا جميع الانواع من البيانات (بيانات كتابية ، بيانات جغرافية ، ملفات مرئية ومسموعة) ويتم تخزين هذه البيانات وفق النظام التابع لها فعلا سبيل المثال يتم تخزين بيانات الجغرافية من خلال نظام (Geo-MOLG) وبيانات الموظفين من خلال نظام شؤون الموظفين (HR System) ونظام الارشفة الالكترونية ، حيث ان جميع هذه الانظمة تستخدم انظمة ادارة البيانات (MySQL, Oracle) بإستثناء ادارة ملفات الموظفين لا تستخدم اي نظام ولكن تستعمل طريقة تنظيم حسب المجلدات كالنظام المتبع في نظام تشغيل (Windows) ويتم اخذ نسخ احتياطية محلية للبيانات واخذ نسخ احتياطية للبيانات فقط على السحابة الالكترونية.
2. يتم التحقق من جودة البيانات بإستخدام انظمة ادارة البيانات (MySQL) لضمان جودة وتطابق البيانات مع البيانات الموجودة في الوزارة واستكمال اخذ نسخ احتياطية لهذه البيانات, وكما انه يوجد دمج لبعض البيانات من مصادر خارجية مثل بيانات الموازنات الموجودة في الهيئات المحلية ، وكما ان وصول المستخدمين لهذه البيانات يتم على مستوى النظام وعلى مستوى الجدار الناري (User Rules).

3. يتم اخذ نسخ احتياطية بشكل تلقائي مجدول وتتم حفظ هذه النسخ محليا (داخل مقر الوزارة) وعلى السحابة الالكترونية (الحاسوب الحكومي)ويتم فحص هذه البيانات بشكل دوري لضمان سلامتها من اي ملفات ضارة ، وايضا عمليات اختبار استعادة هذه البيانات بشكل دوري لضمان استعادتها بشكل سريع وسليم ، تستخدم الوزارة نظام (VEEM) لادارة عمليات النسخ الاحتياطي للبيانات واستعادتها.

ادارة الخدمات والصيانة:

1. تتم ادارة وصيانة الاجهزة والبرمجيات وتوثيق الاعطال بشكل يدوي.
2. يوجد خطط لعمل الصيانة الدورية للاجهزة وتحديث الانظمة ولكن هذه الخطط في العادة لا تتم بشكل دوري ولكن تتم في اغلب الاحيان بناءا على حصول اي مشكلات تنتج, وكما ان عمليات التحديث للبرمجيات تتم حسب الحاجة وتحديث او تطوير البنية التحتية تتم في حالة توفر العامل المادي لتنفيذها.
3. لا يوجد سياسات محددة لعمل التحديثات للاجهزة والبرمجيات او تحديثات دورية الا من خلال الحاجة تتم عمليات التحديث والتطوير.

طو اقم تكنولوجيا المعلومات:

1. يوجد 7 موظفين تكنولوجيا المعلومات في الوزارة مع عدم وجود اي موظف تكنولوجيا معلومات في المديريات وبالتالي موظفي تكنولوجيا المعلومات في الوزارة يقوموا بالعمل داخل المقر الرئيسي وفي المديريات في نفس الوقت.
2. يتواجد في مقر الوزارة دائرتين رئيسيتين متخصصة بتكنولوجيا المعلومات تقوم بالتنسيق الكبير في ما بينهم في حالة الاعطال, التحديثات للبرمجيات والبينية التحتية وتوزيع الاحمال ما بينهم, ويتم توزيع الاحمال ما بين موظفي تكنولوجيا المعلومات بناءا على تخصص كل موظف, كما انه لا توجد نظام ادارة مشاريع مراقبة وتنسيق توزيع المهام على الموظفين.
3. لا يوجد اي دورات تدريبية متخصصة لموظفي تكنولوجيا المعلومات حيث ان عملية تطوير القدرات التكنولوجية تتم بمجهود فردي دون وجود اي خطط لعقد دورات تدريبية متخصصة بتكنولوجيا المعلومات في الوزارة.

التحليل الرباعي (SWOT) :

نقاط القوة (Strengths)	نقاط الضعف (Weaknesses)
1. وجود الخوادم والبنية التحتية داخل مقر الوزارة يمنح السيطرة الكاملة على الأنظمة والبيانات، مما يزيد من الأمان والتحكم. 2. استخدام تقنيات حديثة: استخدام خوادم من نوع Blade Serverونظام VMware يسمح بتقسيم الموارد بكفاءة وفعالية. 3. استخدام جدران نارية وبرامج مكافحة الفيروسات وأنظمة حماية البيانات يساهم في تعزيز أمان البيانات. 4. توزيع الحمل وتجميع البيانات: استخدام تقنيات التجميع على الخوادم وتوزيع الحمل يضمن استدامة وكفاءة الأنظمة. 5. الأنواع البيانية: القدرة على استخدام وإدارة مجموعة متنوعة من أنواع البيانات تعزز من مرونة الوزارة في معالجة المعلومات.	1. نقص التوعية الأمنية: عدم وجود دورات تدريبية أو ورش عمل لتعزيز الوعي الأمني بين الموظفين يمكن أن يترك الوزارة عرضة للتهديدات الأمنية. 2. عدم وجود أنظمة اكتشاف التسلل: عدم وجود أنظمة اكتشاف التسلل يمكن أن يترك الوزارة عرضة لهجمات غير مكتشفة. 3. عدم وجود خطط طوارئ: عدم وجود خطط طوارئ لمواجهة انفطاع الخدمات أو الهجمات السيبرانية يمكن أن يزيد من تأثيرها السلبي. 4. إدارة الصيانة اليدوية: الاعتماد على إدارة وصيانة الأجهزة والبرمجيات بشكل يدوي يمكن أن يكون غير فعال ويزيد من فرص الأخطاء البشرية.

6. نظم إدارة البيانات: استخدام نظم إدارة البيانات يساعد على ضمان جودة البيانات وتنظيمها بشكل فعال. 7. عمليات النسخ الاحتياطي: تنفيذ عمليات النسخ الاحتياطي الدورية واستعادة البيانات يسهم في تحقيق استدامة البيانات وضمان عدم فقدانها.	5. عدم وجود سياسات تحديث محددة: عدم وجود سياسات محددة لعمليات التحديث والصيانة يمكن أن يؤدي إلى تأخير في تحسين البنية التحتية.
الفرص (Opportunity)	**التهديدات (Threats)**
1. تحسين التوعية الأمنية: إمكانية تقديم دورات تدريبية وورش عمل للموظفين لتعزيز الوعي الأمني وتعزيز مهاراتهم في مجال أمن المعلومات. 2. تطوير أنظمة اكتشاف التسلل: إمكانية تحسين بنية الأمان عبر تنفيذ أنظمة اكتشاف التسلل لرصد واستجابة الهجمات السيبرانية. 3. استخدام برمجيات اكتشاف التسلل مثل : Cisco NGIPS , Fidelis Network. 4. استخدام اجهزة كشف التسلل مثل : FireEye Intrusion Prevention System, Hillstone S-series 5. تخزين البيانات في السحابة: زيادة استخدام التخزين في السحابة مع تشفير البيانات يمكن أن يعزز من تأمين البيانات والاستجابة للاحتياجات المتغيرة. 6. تحسين الصيانة والتحديث: إمكانية تنظيم عمليات الصيانة والتحديث لتحسين أداء البنية التحتية. 7. تنظيم العمليات: فرصة لتنظيم وتوجيه إدارة العمليات من خلال تطبيق الأنظمة المناسبة . 8. تطوير القدرات: توفير دورات تدريبية لموظفي تكنولوجيا المعلومات يمكن أن يساعد في تطوير مهاراتهم وزيادة وعيهم بأمان المعلومات. 9. الاستفادة من الخدمات التي تقدمها وزارة الاتصالات والاقتصاد الرقمي بناء على قرار مجلس الوزراء رقم 18/151/06 لعام 2022.	1. هجمات DDoS :هي هجمات يمكن أن تؤثر سلباً على استقرار الخدمات، ويجب تطوير استراتيجيات لمنعها واستجابة فعالة لها. 2. نقص التخطيط للطوارئ: عدم وجود خطط طوارئ يمكن أن يترك الوزارة عرضة لتعطيل العمل وفقدان البيانات في حالة الأزمات. 3. الأمان الغير كافي : عدم استخدام أنظمة أمان متقدمة يمكن أن يجعل البنية التحتية عرضة للتهديدات الأمنية المتطورة مثل استعمال نظام WAF . 4. فرصة الأخطاء البشرية: الاعتماد على الإدارة اليدوية يتيح فرصًا للأخطاء البشرية والتأخير في الصيانة والتحديث. 5. فقدان البيانات: عدم وجود سياسات تحديث محددة يمكن أن يزيد من خطر فقدان البيانات . 6. عدم كفاية (Offline Backup) وفقا لأفضل الممارسات والأنظمة والمعدات الممكن استخدامها لتنفيذ استعادة البيانات . 7. نقص التنسيق: عدم وجود موظف تكنولوجيا معلومات في معظم المديريات التابعة للوزارة يمكن أن يؤثر على التنسيق بين الفرق وتوزيع المهام بشكل فعال.

التوصيات:

1. تنفيذ أنظمة حماية DoS متقدمة .
2. تطوير خطط استجابة للهجمات DDoS تشمل الكشف المبكر وعزل الانشطة المشبوهة.
3. تطوير وتنفيذ خطط طوارئ شاملة تشمل استرجاع البيانات وتوفير توجيهات واضحة للفرق في حالات الأزمات.

4. تنظيم تدريبات دورية للفرق على أساس الخطط الطارئة.
5. تقييم البنية التحتية للتكنولوجيا وتحديث أنظمة الأمان وفقًا لأحدث أفضل الممارسات.
6. تعزيز التوعية بأمان المعلومات بين الموظفين وتطوير سياسات استخدام آمن للأنظمة والبرمجيات.
7. اعتماد أنظمة إدارة أتمتة للصيانة والتحديث لتقليل الأخطاء البشرية.
8. تقديم تدريب مستمر للموظفين على مهام الصيانة والأمان.
9. وضع سياسات دورية لعمليات النسخ الاحتياطي واسترجاع البيانات.
10. تنفيذ حلول تشفير وتحكم في الوصول لحماية البيانات من الوصول غير المصرح به.
11. تنفيذ أنظمة متقدمة لاكتشاف التسلل لمراقبة النشاط غير المصرح به داخل البنية التحتية.
12. تطوير خطط طوارئ تشمل استجابة فورية لانقطاع الخدمات أو الهجمات السيبرانية واستعادة الأمان بسرعة.
13. اعتماد أنظمة إدارة أتمتة لصيانة الأجهزة والبرمجيات لتحسين الكفاءة وتقليل الأخطاء البشرية.
14. وضع سياسات وجداول زمنية محددة لعمليات التحديث والصيانة وتنفيذها بانتظام.

(ب) تحليل الو اقع الحالي للاتحاد الفلسطيني للهيئات المحلية :

المشاهدات وملخص الإجابات على الأسئلة:

من خلال زيارة مقر الاتحاد الفلسطيني للهيئات المحلية كانت الاجابات على الاسئلة المعدة لكل قسم كالتالي :

البنية التحتية لتكنلوجيا المعلومات:

1. يعتمد الاتحاد بشكل أساسي على خادم نظام الارشفة الالكترونية لتخزين وارشفة البيانات، وخادم لادارة ومراقبة والتحكم بالشبكة الداخلية ، كما يستعمل نظام (VMware) لتقسيم الموارد الموجودة ويستخدم انظمة تشغيل مثل (Windows Server 2019) ويستخدم التخزين السحابي فقط لاخذ نسخ احتياطية لبيانات الاتحاد.
2. جميع الخوادم الموجودة في الاتحاد في مكان واحد داخل المؤسسة ، حيث ان هذه الخوادم تتم حمايتها بشكل مباشر من خلال بصمة الدخول اليها بشكل اساسي ولا يتم الدخول اليها الا من خلال مسؤول الاتحاد وموظف تكنولوجيا المعلومات ، كما تتوفر كاميرات امنية لمراقبة الخوادم الموجودة ، وايضا يوفر الاتحاد تأمين لهذه الخوادم.
3. لايستعمل الاتحاد اي من تقنيات (clustering) او (load balancing)للخوادم الموجودة بسبب عدم وجود ضغط في البيانات المرسلة او المستقبلة من الاتحاد.
4. لا يوجد سياسات معينة باستبدال او تحديث الخوادم الموجودة ولكن يتم التحديث حسب احتياجات العمل وتكون التوصيات من خلال موظف تكنولوجيا المعلومات في الاتحاد.

الشبكة والاتصالات:

1. وجود شبكتين داخل الاتحاد احداهما تستعمل فقط لاجهزة الكمبيوتر والشبكة الاخرى تستعمل للهواتف الذكية او اجهزة أخرى ، وهي مفصولة عن الشبكة الرئيسية ، وتستعمل شبكة سلكية (Cat6a) وشبكة لاسلكية.
2. وبخصوص عمليات توزيع الاحمال (Load Balancing) لا يوجد اي من هذه الانظمة وذلك بسبب الضغط على الشبكة او الخوادم الموجودة داخل الاتحاد ، وبخصوص عمليات تجميع البيانات من الشبكتين (aggregation switches) لا يوجد حيث ان الشبكتين المذكورتين غير متصلات مع بعض بشكل مباشر.
3. يستعمل الاتحاد تقنيات الجدار الناري (FortiGate Firewall) لحماية الشبكة من الهجمات الالكترونية وكما أن خادم البريد الالكتروني يحتوي على حماية من خلال نظام التشغيل ، وتتم مراقبة الشبكة وابلاغ المسؤولين بوجود هجوم او اي عملية دخول غير مصرح به للشبكة.
4. يستخدم الاتحاد خطوط خاصة (VPN) في عمليات الاتصال خارج الاتحاد وخصوصا مع البيانات المخزنة في السحابة.

امن المعلومات:

1. في حالة حدوث اي عملية او محاولة اختراق للشبكة يتم اغلاق الشبكة بشكل كامل, وحيث ان الاتحاد لم يتعرض لاي تهديدات سابقة على مستوى الاتحاد, كما ان الاتحاد يستخدم انظمة اكتشاف التسلل (Intrusion Detection Systems) , ويتم فحص الشبكة والبيانات داخل الاتحاد مرتان بالاسبوع من خلال موظف تكنولوجيا المعلومات.

2. بخصوص خطط الطوارئ داخل الاتحاد يوجد خادم احتياطي وايضا وجود اتفاق مع المزود الخارجي بالتزويد بالبيانات في حال فقدانها او تلفها, اما بخصوص البيانات المخزنة على السحابة فيوجد اتفاق مع الشركة المزودة للخدمة السحابية للاتحاد لتشفير البيانات وحفظها في مكان مناسب ومراقبتها وتفادي اي هجوم الكتروني او تسريب لهذه البيانات.
3. كما يوجد نظام صلاحيات للموظفين للوصول الى المعلومات ويتم تقسيم هذه الصلاحيات وفق موقع الموظف وماهي مدى ارتطابه بهذه العملومات والوصول اليها ويتم منح هذه الصلاحيات وفق سياسة يتم الاتفاق عليها ما بين رئيس الاتحاد وموظف تكنولوجيا المعلومات, حيث من خلال نظام الصلاحيات يتم تطبيق الحد الادنى من الصلاحيات (Least Privilege) لضمان امن المعلومات من التسريب او الاطلاع الغير مصرح به.
4. يتم تعزيز التوعية الامنية للموظفين واهميتها من خلال دورات دورية للموظفين واطلاعهم على اخر التحديثات بوسائل حماية البيانات.

إدارة البيانات:

1. يتعامل الاتحاد مع عدد من الانواع من البيانات (ملفات فيديو, ملفات كتابية) وانواع اخرى, حيث ان هذه البيانات يتم تخزينها داخلي وخارجي (التخزين السحابي) وجزء من هذه البيانات يتم تخزينها من خلال انظمة (MySQL & Oracle) , والجزء الاكبر من البيانات تتم تخزينها من خلال نظام الوثائق (File system) والتي تتم من خلال تصنيفها من خلال مجلدات او ملفات موجودة على الخوادم, ويتم اخذ نسخ احتياطية على السحابة الالكترونية.
2. وبخصوص جودة البيانات لا يستقبل الاتحاد البيانات الا من جهات رسمية وايضا يتم التحقق من هذه البيانات قبل ايصالها الى الموظفين من خلال الجدار الناري او مضاد الفايروسات.
3. ولا يتم الوصول الى البيانات الا من خلال صلاحيات محددة مسبقا للموظفين لضمان عدم تسريب او اطلاع غير مصرح به.
4. بخصوص عمليات اخذ نسخ احتياطية للبيانات الموجودة داخل الاتحاد يتم اخذها بشكل تلقائي (اسبوعي ويومي), اما بخصوص البيانات المخزنة على السحابة الالكترونية فالمزود هو من يقوم بعمليات اخذ النسخ الاحتياطية من هذه البيانات حيث ان هذه البيانات مخزنة في موقع في رام لله وموقع (التشيك او الولايات المتحدة) لم يتم تحدد المكان بدقة.
5. كما يتم بشكل دوري عملية فحص البيانات وتطابقها وسلامتها من خلال اخذ جزء من النسخ الاحتياطية ومقارنتها وفحص جودتها.
6. بخصوص البيانات المخزنة داخل الاتحاد يتم استعمال انظمة (VEEM) لعمل نسخ احتياطية بشكل اتوماتيكي ومتزامن.

الخدمات والصيانة:

1. لا يوجد انظمة لادارة ملفات الصيانة وتحديث البرمجيات اذ ان هذه الخطوة تتم من خلال موظف تكنولوجيا معلومات بدوام جزئي وبخصوص البيانات الموجودة على السحابة تتم من خلال الشركة المزودة للخدمة السحابية.
2. يوجد الية عمل يدوية لتوثيق الاعطال والصيانة للاجهزة الموجودة داخل الاتحاد.
3. وجود خطط لعملية التحديث وترقية الخوادم الموجودة داخل الاتحاد, حيث ان هذه الخطط يتم وضعها بشكل سنوي.

طو اقم تكنولوجيا المعلومات:

1. لا يوجد موظفي تكنولوجيا معلومات بدوام كامل ولكن يوجد موظف بدوام جزئي في الاتحاد.

التحليل الرباعي (SWOT) :

نقاط القوة (Strengths)	نقاط الضعف (Weaknesses)
1. التخزين السحابي: الاعتماد على التخزين السحابي يمنح الاتحاد مرونة وقدرة على توسيع سعة التخزين بسرعة وكفاءة. 2. تطبيق صلاحيات دقيقة للوصول إلى البيانات يقلل من مخاطر التسريب والوصول غير المصرح به. 3. استخدام وسائل حماية فعالة داخل الاتحاد مثل صلاحيات الدخول الى الخوادم. 4. استخدام صارم لصلاحيات الوصول للبيانات للموظفين. 5. استخدام نسخ احتياطي فعال للبيانات داخلي وخارجي. 6. عمليات مراقبة الشبكة فعال ودوري. 7. مراقبة جودة البيانات والتحقق من سلامتها. 8. فحص دوري للنسخ الاحتياطية. 9. دورات دورية لزيادة التوعية بأمن المعلومات للموظفين. 10. استخدام نظام هجين للخدمات والبيانات.	1. وجود عدد قليل من الخوادم في مقر الاتحاد والاعتماد بشكل كبير على التخزين السحابي. 2. استعمال نظام الملفات لتخزين البيانات (File System) بشكل كبير مع استعمال بسيط لانظمة ادارة البيانات مثل (MySQL & Oracle). 3. عدم وجود أنظمة لإدارة ملفات الصيانة وتحديث البرمجيات يمكن أن يؤدي إلى تفويت الصيانة الدورية وتحديث الأنظمة 4. وجود موظف تكنولوجيا المعلومات بدوام جزئي يمكن أن يزيد من التأخر في التعامل مع المشاكل التقنية. 5. لا يوجد خطط وسياسات محددة معنية بادارة البنية التحتية لتكنولوجيا المعلومات والتحديث المستمر. 6. عدم وجود آلية لفحص النسخ الاحتياطية المأخوذة من السحابة الالكترونية. 7. اخذ نسخ احتياطية من البيانات فقط ، دون البرمجيات الموجودة داخل الاتحاد.
الفرص (Opportunity)	**التهديدات (Threats)**
1. استخدام برمجيات اكتشاف التسلل مثل : Cisco NGIPS , Fidelis Network. 2. استخدام اجهزة كشف التسلل مثل : FireEye Intrusion Prevention System, Hillstone S-series. 3. بخصوص صلاحيات الوصول للبيانات تتم تطويرها من خلال : تمكين مالكي البيانات من التحكم في حقوق الوصول إلى البيانات التي يمتلكونها للتأكد من أن جميع العمليات مصرح بها . 4. استخدام تقنيات التحقق المتعدد الخطوات مثل التحقق الثنائي (2FA) يمكن أن يحمي البيانات من الوصول غير المصرح به . 5. يمكن تطبيق تقنيات تدفق البيانات للكشف عن تغييرات غير متوقعة في البيانات على مدار الزمن. إذا تم اكتشاف تغييرات كبيرة أو مفاجئة .	7. يتم تطبيق تدابير امنية اساسية فقط على مستوى الصلاحيات للوصول الى البيانات دون استخدام انظمة متطورة. 8. الاعتماد على موظف تكنولوجيا معلومات بدوام جزئي هذا يشكل خطرا في حال حدوث اختراق او تسريب. 9. الاعتماد على الشركة المزودة لتشفير البيانات واختيار الاماكن لتخزين البيانات. 10. عدم وجود تقييم لجميع الإجراءات والسياسات الأمنية المتبعة وتحسينها استنادًا إلى التهديدات والتطورات الأمنية الجديد. 11. استخدام نظام (Files System)بدلا من استخدام انظمة ادارة البيانات بشكل كامل. 12. التبعية للطرف الثالث :في حالة اعتماد الجهة على الطرف الثالث بشكل كبير، قد يؤدي توقف الطرف الثالث عن تقديم الخدمات إلى تعطيل العمليات. 13. عدم وجود تنظيم دقيق لعمليات التحديث والاستبدال يمكن أن يترك الأنظمة عرضة للهجمات أو التجاوز.

التوصيات :

1. تحسين وتوسيع تدابير الامان واعداد صلاحيات الوصول بما يتناسب مع التهديدات المحتملة , و التفكير في استخدام تقنيات متقدمة مثل تعدد العوامل للمصادقة (Multi-Factor Authentication).
2. وضع خطط محددة للتحديثات التكنولوجية والامنية بشكل دوري حيث يتضمن تحديث انظمة التشغيل والبرمجيات والتصحيحات الامنية.
3. الاستثمار في اختبارات الاختراق والتدقيق الامني بشكل دوري لتحديد الثغرات ونقاط الضعف وتصحيحها قبل استغلالها.
4. توظيف موظف تكنولوجيا معلومات بدوام كامل ليكون مسؤولا بشكل مباشر عن البنية التحتية لكتولوجيا المعلومات والبيانات وامنها ومراقبة واستجابة لاي تهديدات امنية بشكل فعال.
5. التأكد من وجود اتفاقيات وعقود دقيقة تشمل جميع جوانب تزويد الخدمة مثل امور تشفير البيانات وحفظ البيانات بشكل مناسب.
6. اجراء تقييم دوري للسياسات والاجرائات الامنية المتبعة وتحسينها استنادا الى التهديدات والتطورات الامنية الجديدة.
7. استخدام انظمة ادارة البيانات المتقدمة لزيادة امان وتنظيم البيانات.
8. تنفيذ انظمة تتبع البريد الالكتروني ومحتوياته للكشف عن اي تهديدات محتملة قبل ان يصل البريد الى الموظفين.
9. وضع استراتيجية للتعامل مع الطرف الثالث لمزود خدمة السحابة الالكترونية تشمل مراجعة الامان والمتطلبات الامنية في العقود والاتفاقيات.

(ت) تحليل الو اقع الحالي لصندوق تطويرو اقراض الهيئات المحلية :

المشاهدات وملخص الإجابات على الأسئلة:

من خلال زيارة صندوق تطوير واقراض الهيئات المحلية كانت الاجابات على الاسئلة المعدة لكل قسم كالتالي :

البنية التحتية لتكنولوجيا المعلومات:

1. يستخدم الصندوق بنية تحتية هجينة ما بين الخوادم في مقر الصندوق والسحابة الالكترونية ، حيث ان جميع البيانات يتم تحميلها بشكل كامل على السحابة الالكترونية وكما يستخدم السحابة الالكترونية ايضا في حال الطوارئ لضمان سير العمل داخل الصندوق من حيث تدفق البيانات والانظمة العاملة داخل الصندوق.
2. يوجد في مقر الصندوق العديد من الخوادم التي تستخدم لكل من : أرشفة الملفات المالية ، الموقع الالكتروني حيث يستخدم الصندوق نظام (VMware) لتقسيم الخوادم وفق اغراض متعددة في نفس الوقت.
3. الصندوق يقوم بتحديث مواصفات هذه الخوادم وفق المتطلبات العملية وايضا ادخال التحديثات بناء على نوع التكنولوجيا الحديثة ، حيث يستخدم نظام تشغيل (Windows Server 2019) كأساس للخوادم ، واستخدام نظام (Linux) في تفعيل نظام (VMware) ، وجميع الخوادم موجودة في مقر الصندوق ويتم تأمين غرفة الخوادم لمنع الوصول لاي شخص ليس لديه الصلاحيات من خلال باب امان ذو مواصفات امان مثل وجود رقم سري للدخول اليها ، معزولة بشكل كامل عن المحيط مزودة بخطي كهرباء وايضا خط (UPS) .
4. يستعمل لزيادة فعالية الخوادم انظمة (Clustering) لتجميع موارد الخوادم لعمل اكثر فعالية وايضا يستعمل نظام (Load Balancing) لتوزيع الاحمال على الخوادم في حالة الضغط وكما يستعمل في نفس الوقت هذه الانظمة بالتزامن مع السحابة الالكترونية.
5. يستعمل انظمة امان لحماية البيانات على هذه الخوادم حيث يستخدم الجدار الناري (Firewall) ونظام (WAF) لعمل عزل لهذه الخوادم عن العالم الخارجي لحمايتها من التهديدات الامنية.
6. كما ذكر سابقا يتم تقسيم موارد الخوادم واستخدامها بشكل فعال من خلال استخدام (VMware) ، ومن خلال استخدام هذا النظام يتم اخذ نسخ احتياطية تلقائية (يومي ، شهري ، سنوي) على مستوى(VMware) وايضا اخذ نسخ احتياطية على مستوى البيانات.

الشبكة والاتصالات:

1. وجود شبكة سلكية (Cat6a) و شبكة لاسلكية (Wi-Fi 6) و شبكة (VOIP) ولكل نظام من هذه الشبكات محددات وقواعد خاصة بها من حيث الوصول الى المعلومات او الخدمات المتوفرة.
2. يستخدم نظام توزيع الاحمال (Load Balancing) على الشبكة لتسهيل الوصول الى المعلومات من الخوادم ، و السحابة الالكترونية واجهزة الموظفين داخل الصندوق ، ويتم ايضا استخدام نظام تجميع البيانات (Aggregation Switches) لتجميع البيانات من جميع اقسام الشبكة الرئيسية منها والفرعية .
3. يتم حماية الشبكة داخل الصندوق من خلال استخدام (Physical Firewall IPS) و نظام (WAF software) , وايضا يمنع استخدام (USB) بشكل مباشر على الاجهزة الا بعد فحصها وضمان خلوها من اي ملفات مصابة ، كما ايضا يستخدم (WAF software) كنظام اكتشاف التسلل للانظمة (Intrusion Detection System).
4. يتم تأمين الاتصالات الخارجية مع الشبكة و وصول الموظفين للبيانات داخل الصندوق من خلال استخدام (Microsoft Domain Authentication) لتحدد هوية المستخدم صلاحيات الوصول الى الشبكة الداخلية او البيانات الداخلية.
5. يوجد خوادم لتوزيع عناوين الاجهزة (DHCP Server) حسب الشبكة المتصلة مع الجهاز .

6. بخصوص الاتصال البعيد الامن يستخدم نظام (s-VPN) ما بين الضفة وغزة وتتم هذه الطريقة باستخدام اعطاء الصلاحيات لجهاز محدد من خلال (Real IP) فقط واعطائه صلاحيات محددة للوصول للبيانات او الخوادم.
7. ان رصد ومراقبة الشبكة يتم من خلال نظام تنبيهات تصدر من (Antivirus admin Control tools) لتنبيه مسؤول النظام في حال حدوث اي تسلل او هجوم الكتروني.

امن المعلومات:

1. يستعمل الصندوق نظام الكشف والاستجابة الموسعة (Extended detection and response XDR) للكشف وحماية المعلومات من التهديدات الامنية الالكترونية.
2. لم يتعرض الصندوق لتهديدات امنية الكترونية تذكر ولكن كان هجوم الكتروني وحيد على موقع الصندوق , حيث ان استخدام انظمة (Intrusion Detection System) مثل نظام (Fortinet Antivirus , IPS) ساهم بشكل كبير في الحد من التهديدات الامنية الالكترونية وحماية البيانات الموجودة داخل الصندوق.
3. يتم التحقق من الانشطة على البيانات من خلال نظام التنبيهات (Notification) الموجود على نظام (WAF System) وتحديد الانشطة الامنة من غيرها من الانشطة.
4. خطط دورية غير موجودة ولكن يتم تحديث الاجهزة والبرمجيات المتعلقة بأمن المعلومات بشكل دوري وايضا اتسخدام النسخ الاحتياطي المحلي (Offline data Backup) لضمان وجود نسخة محلية لا يتم الوصول اليها الا من خلال موظف تكنولوجيا المعلومات, كما انه يتم الاستعانة بمصارد خارجية (Third party source)لحفظ البيانات واستعادتها بشكل فعال وسريع.
5. يتم تشفير بيانات الصندوق من خلال استخدام نظام التشفير الخاص بشركة (Microsoft) بحيث تكون البيانات مشفرة وايضا وسيلة الاتصال ايضا تكون مشفرة بحيث يصعب الوصول الى هذه البيانات, وايضا بخصوص الوصول للبيانات من خلال الموظفين تتم من خلال نظام الصلاحيات وتطبيق الحد الادنى من الصلاحيات لضمان عدم تسريب او اطلاع اي من الموظفين على بيانات معينة.
6. لا يتم تطبيق دورات توعية امنية للموظفين داخل الصندوق بخصوص انظمة الامان او التهديدات الالكترونية والتي يمكن ان تحدث و اداوات الحماية ولكن يتم اعطاء دورات في امن المعلومات لموظف تكنولوجيا المعلومات فقط.

ادارة البيانات:

1. يتعامل الصندوق تقريبا مع عدد كبير من انواع البيانات مثل (بيانات مالية, بيانات الموقع الالكتروني) وتتم ادارة هذه الملفات او البيانات من خلال نظامين (Oracle, MySQL) ويتم استخدام هذه الانظمة ادخل الخوادم الموجودة في الصندوق وايضا استخدامها في السحابة الالكترونية ويتم عمل تزامن ما بين البيانات الموجودة داخل الصندوق والبيانات الموجودة على السحابة الالكترونية.
2. تتم التحقق من جودة البيانات من حيث سلامة البيانات من اي ملفات ضارة من خلال النظام التلقائي (Firewall, WAF, Forty Antivirus) وايضا من خلال مسؤول الانظمة في الصندوق, ومن حيث دقة البيانات تتم بشكل هرمي.
3. يتم التعامل مع امان البيانات والوصول اليها من خلال الدور الوظيفي للمستخدم ومنه الصلاحيات الادنى للوصول اليها وفي بعض الحالات يتم اعطاء الصلاحيات بناءا على توصيات من المدير المباشر وان تكون هذه الصلاحيات مؤقتة, كما انه يستخدم انظمة (Microsoft user rules) و (VM) لتحديد صلاحيات الوصول لهذه البيانات.
4. يتم اخذ نسخ احتياطية بشكل اتوماتيكي (Automatic backup) وايضا من خلال (VEEM) وايضا وجود نسخة احتياطية محلية (Offline Data Backup) ونسخة احتياطية موجودة على السحابة الالكترونية مع العلم ان النسخة الاحتياطية على السحابة

الالكترونية غير معروف اين يتم تخزينها وانما يتم ادارتها من خلال الشركة المزودة لهذه الخدمة, ويتم عمل اختبارات لتحقق من مدى سلامة هذه النسخ من البيانات كل 3 اشهر وسرعة الاستعادة لهذه البيانات.

ادارة الخدمات والصيانة:

1. لا يوجد انظمة معينة لادارة وصيانة الاجهزة , حيث تتم عمليات الادارة او توثيق الاعطال في الانظمة والاجهزة بشكل يدوي.
2. يوجد خطط مستقبلية لتحديث وصيانة الاجهزة والبرمجيات المستخدمة داخل الصندوق, حيث ان عمليات التحديث تتم من خلال دراسة الحاجات المتزايدة على خدمات معينة او وجود تكنولوجيا جديدة توفر فعالية افضل, وتتم عمليات التحديث بناءا على المتطلبات بدون وجود سياسات معينة لادارة هذه التحديثات.

طو اقم تكنولوجيا المعلومات:

1. يوجد موظف تكنولوجيا معلومات بدوام كامل يعمل داخل الصندوق , وموظف لمتابعة المشاريع المتعلقة بالبنية التحتية لتكنولوجيا العملومات خارج الصندوق, اذ انه كل موظف يقوم بعمل مختلف من حيث طبيعة العمل والمسؤوليات المنوطة به, ولا يوجد انظمة لادارة مشاريع التخطيط والتطوير البنية التحتية داخل الصندوق.
2. عدم وجود او ندرة الدوات المتعلقة بكنولوجيا المعلومات التي يتم اعطائها لموظفي تكنولوجيا المعلومات في الصندوق حيث يتم الاعتماد بشكل كبير على عقود الصيانة مع الشركات المزودة لمواكبة التطورات التكنولوجية وايضا التعامل مع الازمات التكنولوجية.

التحليل الرباعي (SWOT) :

نقاط القوة (Strengths)	نقاط الضعف (Weaknesses)
9. استخدام السحابة الالكترونية حيث توفر المرونة وامكانية الوصول الى البيانات من اي مكان وفي اي وقت. 10. بنية تحتية هجينة تجمع بين الخوادم المحلية والسحابة الإلكترونية توفر مرونة واستدامة عند تحميل البيانات وفي حالات الطوارئ. 11. استخدام نظام تشغيل متطور وأنظمة تجزئة (VMware) يزيد من كفاءة الخوادم والاستفادة من الموارد . 12. الاستفادة من تقنيات التوزيع وتجميع البيانات والتحميل التلقائي للنسخ الاحتياطية تسهم في تعزيز الأمان واستمرارية العمل. 13. تشفير البيانات وتطبيق نظام الصلاحيات يعززان أمان البيانات ومنع الوصول غير المصرح به.	1. عدم توجيه التدريب للموظفين: عدم تقديم دورات توعية امنية للموظفين يزيد من مخاطر الهجمات الالكترونية. 2. عدم وجود نظام موحد لإدارة وصيانة الأجهزة يمكن أن يؤدي إلى فقدان البيانات أو انقطاع الخدمة في حالة عدم التنسيق الجيد. 3. عدم وجود سياسات محددة لإدارة التحديثات وتوقيتها: حيث يتم الاعتماد بشكل كامل على التحديثات من شركة مايكروسوفت فقط .

14. استخدام نظام الكشف والاستجابة الموسعة (XDR) للكشف عن التهديدات الأمنية يعزز من قدرة الصندوق على التصدي للتهديدات السيبرانية. 15. تحديث مستمر للبنية التحتية : القدرة على تحديث البنية التحتية واستخدام تكنولوجيا المعلومات تزيد من كفاءة العمل وامان البيانات. 16. استخدام أنظمة أمان: استخدام الجدار الناري وانظمة الامان المختلفة يعزز امن المعلومات والكشف عن الانشطة الغير الآمنة المرتبطة بالبيانات والشبكة الداخلية.	
الفرص (Opportunity)	**التهديدات (Threats)**
1. تحسين التوجيه والتدريب للموظفين: منح الموظفين التدريب في مجال امن المعلومات واستخدام الانظمة يقلل من مخاطر الهجمات الالكترونية. 2. تعزيز تنسيق العمل بين موظفي تكنولوجيا المعلومات يساعد في تحسين الاستجابة للمشكلات التكنولوجية. 3. تحسين إدارة البيانات والتنسيق بين موظفي تكنولوجيا المعلومات يمكن أن يزيد من كفاءة العمل والتنسيق بين المشاريع. 4. استخدام أدوات إدارة مشاريع تسهم في تتبع وصيانة الأجهزة بشكل أفضل.	1. عدم وجود سياسات معينة لإدارة التحديثات يمكن أن يؤدي إلى تأخر في تطبيق التكنولوجيا الجديدة. 2. يعتمد الصندوق بشكل كبير على عقود الصيانة مع الشركات الموردة للتكنولوجيا، مما يعرضه لمخاطر في حالة عدم توفر هذه الخدمات. 3. تحديثات غير منتظمة: عدم وجود سياسات محددة لإدارة التحديثات يمكن أن يجعل البنية التحتية عرضة للثغرات الأمنية.

التوصيات :

1. تنظيم دورات توعية أمنية دورية لجميع الموظفين في الصندوق، بما في ذلك التحديثات المتعلقة بأمان المعلومات والسلوك السليم عبر الإنترنت.
2. إنشاء حملات توعية داخلية لتسليط الضوء على تهديدات الأمان الشائعة والتصرف الآمن عبر البريد الإلكتروني والموارد الرقمية الأخرى.
3. تعزيز توجيه الموارد: توجيه المزيد من الموارد لتقديم الدعم والأدوات اللازمة لموظفي تكنولوجيا المعلومات.
4. انشاء منهج وأدوات مشتركة لإدارة المشروع وتوثيق الأعمال الصيانة وإصلاح الأخطاء.
5. تطوير وتنفيذ نظام موحد لإدارة وصيانة الأجهزة وضمان توافقه مع سياسات الأمان.
6. انشاء سياسات محددة لإدارة التحديثات بما في ذلك الجداول الزمنية وإجراءات الاختبار.
7. تطوير سياسة تحديثات منتظمة واختبارات فحص دورية لضمان سلامة الأنظمة والتطبيقات.
8. إعداد خطة استجابة للتهديدات الأمنية تشمل إجراءات للتعامل مع هجمات محتملة. و توزيع هذه الخطة على جميع الموظفين وتحديثها بانتظام.

تم إنجاز هذا العمل بالتعاون مع برنامج "الحكم الإلكتروني (INDIGO)"
التابع لمؤسسة GIZ وبتفويض من الوزارة الإتحادية للتعاون الاقتصادي
والتنمية الألمانية (BMZ)