https://doi.org/10.31272/ijes.v24.1555

المجلة العراقية للعلوم الاقتصادية
Iraqi Journal For
Economic Sciences

PISSN : 1812-8742 EISSE : 2791-092X Arcif : 0.375

Assessment of the Possibility of Implementing an Information Security Management System According to the International Standard (ISO/IEC 27001:2022)

تقييم أمكانية تطبيق نظام أمن المعلومات على وفق المواصفة الدولية ISO/IEC 27001:2022

حارث زيد مهدي جعفر
Harith Zaid Mahdi Jaafar
Harmsj2018@gmail.com
وزارة النفط

أ.م.د مكية كريدي بنيان كريم
Makkiyah Kraidi Bunyan Alkabi
dr.makkiyah71@uomustansiriyah.edu.iq
كلية الإدارة والاقتصاد/ جامعة المستنصرية

Abstract

The research aims to assess the extent of compliance of the General Company for Gas Filling and Services with the requirements of the international standard ISO/IEC 27001:2022, through a case study methodology using a standardized checklist and field study. The results showed that the overall implementation level reached 86.73%, with a gap of 13.27%. The analysis revealed that the gaps were centered on weaknesses in security documentation, risk management, and security awareness. The study concluded that there is a regulatory foundation capable of development, alongside existing gaps that require addressing. It recommended developing a comprehensive security policy, enhancing documentation, establishing an effective risk management framework, and implementing intensive training programs.

Keywords: Information Security, ISO/IEC 27001:2022, Information Security Management System.

المستخلص

يهدف البحث إلى تقييم مدى امتثال الشركة العامة لتعبئة وخدمات الغاز لمتطلبات المواصفة الدولية ISO/IEC 27001:2022، وذلك من خلال منهج دراسة الحالة باستخدام قائمة فحص معيارية ودراسة ميدانية. أظهرت النتائج أن مستوى التطبيق الكلي بلغ 86.73%، مع وجود فجوة نسبتها 13.27% . بيّن التحليل أن الفجوات تركزت في ضعف التوثيق الأمني وإدارة المخاطر والوعي الأمني. خلصت الدراسة إلى وجود قاعدة تنظيمية قابلة للتطوير مع وجود ثغرات تحتاج إلى معالجة. أوصت بتطوير سياسة أمنية شاملة وتعزيز التوثيق وبناء إطار فعال لإدارة المخاطر وبرامج تدريبية مكثفة.

الكلمات الرئيسية: أمن المعلومات، ISO/IEC 27001:2022، نظام أدارة أمن المعلومات.

1. المقدمة

يشهد العالم تطوراً كبيراً ونوعياً في مجال إدارة تكنولوجيا المعلومات والاتصالات، مما جعل أمن المعلومات ركيزة أساسية لضمان حماية الأصول الرقمية والحفاظ على استمرارية الأعمال في

المؤسسات العامة والخاصة. وتمثل المواصفة الدولية ISO/IEC 27001 إطاراً معيارياً عالمياً يقدم منهجية لإدارة أمن المعلومات عبر تحديد المخاطر ووضع الضوابط وضمان التحسين المستمر. لذا تهدف هذه الدراسة إلى تقييم إمكانية تطبيق هذه المواصفة في الشركة العامة لتعبئة وخدمات الغاز، من خلال تحليل واقع أمن المعلومات وقياس مدى الالتزام بمتطلباتها. وتتضمن الدراسة، المواصفة ومكوناتها. والتشخيص العملي لواقع أمن المعلومات في الشركة، وعرض الاستنتاجات والتوصيات العملية لتعزيز الامتثال للمعايير الدولية.

اولاً: مشكلة البحث: تتمحور مشكلة البحث الرئيسة حول قصور نظم المعلومات في الشركة العامة لتعبئة وخدمات الغاز في مجال حماية البيانات والمعلومات ، نتيجة لعدم تطبيق معايير عالمية معتمدة او نتيجة المخاطر التي تتعرض لها بيانات المستخدمين وبناءً على الواقع الاداري والتنظيمي والفني الحالي في الشركة العامة لتعبئة وخدمات الغاز ويمكن التعبير عن مشكلة البحث بالتساؤلات:

1. هل لدى الشركة العامة لتعبئة وخدمات الغاز نظام او اجراءات او ضوابط لإدارة أمن المعلومات ؟
2. مدى جاهزية البنية التحتية التقنية والتنظيمية لشركة لتطبيق متطلبات المواصفة ISO 27001؟
3. ما حجم الفجوة المحددة في الشركة وفق الواقع التطبيقي بين واقع الاداء الفعلي لنظام ادارة امن المعلومات ومتطلبات المواصفةISO\IEC 27001:2022؟
4. ماهي نقاط القوة والضعف لنظام امن المعلومات في الشركة ؟
5. كيف يمكن تعزيز أمن المعلومات في الشركة ؟

ثانياً : هدف البحث

1- التأكد من توافر نظام لإدارة أمن المعلومات في الشركة العامة لتعبئة وخدمات الغاز .
2- بيان واقع الشركة الفعلي لتطبيق نظام إدارة أمن المعلومات على وفق المواصفة الدولية ISO/IEC27001:2022.
3- قياس حجم الفجوة بين الواقع الفعلي لإدارة أمن المعلومات في الشركة وبين متطلبات نظام إدارة أمن المعلومات على وفق المواصفة الدولية ISO/IEC27001:2022.
4- تحديد نقاط القوة والضعف في متطلبات المواصفة الدولية ISO/IEC27001:2022 في الشركة.
5- اقتراح الية عملية لمعالجة الضعف وردم الفجوة لتطبيق المواصفة الدولية ISO/IEC27001:2022 داخل الشركة.

ثالثاً : اهمية البحث

1- مساعدة الشركة في تلبية متطلبات المواصفة ISO/IEC 27001/2022 من خلال تحديد الفجوة بين متطلبات المواصفة وواقع أمن المعلومات في الشركة.
2- يسهم البحث في بيان اهمية انظمة ادارة أمن المعلومات خاصة المواصفة ISO/IEC 27001/2022 لحماية المعلومات والحفاظ على سريتها وسلامتها وضمان استمرارية العمل وحماية البيانات الحساسة وتعزيز ثقة المتعاملين معها.
3- توجيه أنظار الادارة العليا والجهات المعنية بأهمية تطبيق المواصفة ISO/IEC 27001/2022 وما يوافره من مستوى عالٍ من الحماية من خلال عمليات التدقيق الداخلي والاجراءات التصحيحية
4- يوافر البحث بيانات ونتائج تسهم في دعم صناع القرار والادارة العليا في الشركة لإتخاذ خطوات
مدروسة لانشاء نظام أمن المعلومات لتقليل احتمالية التعرض للمخاطر.

5- يقدم البحث اضافة علمية تفيد الباحثين في مجال في مجال نظم ادارة أمن المعلومات كونه يُعد نموذجاً قابلاً للتطبيق أو تطويره لمنظمات أخرى.

المحور الاول : الجانب النظري المواصفة ISO/IEC 27001

1. **مفهوم مواصفة الـ ISO/IEC 27001:** اشارت الهيأة الدولية للتقييس (International Organization for Standardization [ISO], 2022) ان معيار ISO/IEC 27001 يحدد المتطلبات الواجب تحقيقها لانشاء نظام إدارة أمن المعلومات و يوافر المعيار إرشادات للشركات من جميع الأحجام وفي مختلف القطاعات حول كيفية إنشاء وتنفيذ وصيانة وتحسين نظام إدارة أمن المعلومات بشكل مستمر و الالتزام بـ ISO/IEC 27001 يعني أن المؤسسة أو الشركة قد وضعت نظامًا لإدارة المخاطر المتعلقة بأمن البيانات التي تملكها أو تتعامل معها، وأن هذا النظام يلتزم بجميع أفضل الممارسات والمبادئ التي ينص عليها هذا المعيار الدولي واشارت هيأة الضمان والجودة في منشورها (NQA, 2022:4)ان معيار ISO 27001 هو المعيار دولي معتمد لأنظمة إدارة أمن المعلومات لكونه يوفر إطار عمل متكامل لحماية المعلومات، لانه ملائم لجميع المؤسسات بمختلف انواعها وأحجامها ومع ازدياد مخاطر امن المعلومات في الفترة الاخيرة فإن العديد من المؤسسات تلجأ تطبيق نظام لإدارة أمن المعلومات يتماشى مع معيار ISO 27001 ، واشار (Yli-Karro, 2025: 5-6) الى تميز معيار ISO 27001 بهيكل مشابه لهيكل المعايير ISO الأخرى المتعلقة بأنظمة الإدارة و يُسمى هذا الهيكل Annex SL. يُحدد Annex SL هيكل المعايير وعنوانات بنودها، ويساعد على تيسيرها وتوحيد معاييرها. كما يُسهّل هذا تدقيق معايير متعددة في الوقت نفسه، ويساعد على تطبيق معايير ذات هياكل متشابهة. الهيكل المشترك لمعايير نظام الإدارة التي تستخدم Annex SL

2. **متطلبات المواصفة 27001:** تتكون المواصفة ISO 27001 من عشرة بنود البنود الثلاثة الأولى هي (النطاق، المراجع المعيارية، والمصطلحات والتعريف) وتعد بنود تمهيدية و البنود السبعة الاخرى تعد بنود ملزمة للمنظمة التي تسعى للحصول على الشهادة.

الشكل (1) بنود المواصفة ISO/IEC27001:2022المصدر(Voicu, 2022:9)

لكي تدّعي أي منظمة المطابقة لمعيار ISO 27001 عليها تنفيذ متطلبات سبعة بنود رئيسة مُحددة في البنود من 4 إلى 10والتي سنتناولها في ادناه بالتفصيل :

البند الرابع : سياق المنظمة: يتضمن هذا البند أربع نقاط أساسية وهي فهم المنظمة وسياقها وفهم احتياجات وتوقعات الأطراف المعنية وتحديد نطاق نظام إدارة أمن المعلومات (ISMS) ونظام إدارة أمن المعلومات نفسه. حيث يلزم هذا البند المنظمة على تحديد القضايا الخارجية والداخلية ذات الصلة بغرضها والمؤثرة على قدرتها في تحقيق النتائج المرجوة من نظام إدارة أمن المعلومات الخاص بها وكذلك يجب في المنظمة تحديد الاطراف ذات الصلة بادارة النظام وتحديد المتطلبات التي سيعالجها النظام وتحديد حدود وقابلية النظام لتحديد

وتوثيق النطاق والتزام المنظمة إنشاء وتنفيذ وصيانة نظام إدارة أمن المعلومات وضمان استمرارية تحسين النظام والعمليات اللازمة المرتبطة به وتفاعلاتها على وفاقاً لمتطلبات هذه الوثيقة. المصدر المواصفة 27001

البند الخامس (القيادة) : يُركز هذا البند على مسؤوليات الإدارة العليا من خلال الزامها (الادارة العليا) بإظهار القيادة والالتزام تجاه نظام إدارة أمن المعلومات وذلك من خلال ضمان تحقيق النظام لنتائجه المطلوبة والعمل على توافر الموارد اللازمة لغرض تعزيز عملية التحسين المستمر والتزام الادارة بتوجيه الأفراد ودعمهم للمشاركة في فاعلية النظام كما يُلزم هذا البند الإدارة العليا بوضع سياسة لأمن المعلومات، وضمان توزيع المسؤوليات والصلاحيات المتعلقة بالأدوار ذات الصلة بأمن المعلومات داخل المؤسسة، والتواصل بشأنها.

البند السادس (التخطيط) : يختص هذا البند بمرحلة التخطيط لنظام إدارة أمن المعلومات (ISMS) حيث يجب على المؤسسة دراسة القضايا والمتطلبات وتحديد المخاطر والفرص التي يجب معالجتها لضمان تحقيق النظام للنتائج المطلوبة ومنع الآثار غير المرغوبة أو تقليلها وينبغي على المؤسسة ان تُحدد معايير مخاطر أمن المعلومات وتُحافظ عليها من خلال تحديد وتطبيق عملية تقييم مخاطر أمن المعلومات وضمان ان تؤدي الحصول على نتائج متسقة وصحيحة وقابلة للمقارنة من خلال تكرار عملية التقييم ويجب ان تقوم المؤسسة بتحديد وتطبيق عملية معالجة مخاطر أمن المعلومات ووضع الخطط اللازمة لكيفية تحقيق أهداف أمن المعلومات مع مراعاة ان اي تغيير في نظام إدارة أمن المعلومات يجب ان تكون على وفق تخطيط مسبق.

البند السابع (الدعم) : بموجب هذا البند على المنظمة ان تلتزم بتحديد الموارد اللازمة لإنشاء نظام إدارة أمن المعلومات وتوفيرها لتطبيق النظام وصيانته وضمان التحسين المستمر يركز هذا البند على ضمان توافر الكفاءة اللازمة في المؤسسة و أن يكون الأشخاص الذين يعملون تحت سيطرة المؤسسة على دراية ووعي بسياسة أمن المعلومات لضمان مساهمتهم الفاعلة لنظام إدارة أمن المعلومات.

البند الثامن (التشغيل): على المنظمة ان تخطط للعمليات اللازمة لتلبية وتنفيذ المتطلبات والتحكم بها وتنفيذ إجراءات خاصة بوضع معايير للعمليات والتحكم بها على وفاقاً لهذه المعايير وتحتاج المنظمة كذلك إلى إجراء تقييمات لمخاطر أمن المعلومات على فترات مخطط لها مسبقا أو عند اقتراح حدوث تغييرات جوهرية كما سيتعين على المنظمة تنفيذ خطة معالجة مخاطر أمن المعلومات

البند التاسع (تقييم الأداء) : على المنظمة تحديد ما يجب مراقبته وقياسه وطرائق الرصد والقياس والتحليل والتقييم، ومتى يجب إجراء الرصد والقياس، ومن سيتولى الرصد والقياس، ومتى يجب تحليل النتائج وتقييمها، ومن يجب عليه تحليلها وتقييمها.

البند العاشر(التحسين المستمر) : يجب إجراء عمليات التدقيق الداخلي بشكل دوري مخطط له للتأكد من توافق نظام إدارة أمن المعلومات مع متطلبات المنظمة ومتطلبات ISO 27001 والتحقق من فاعلية تنفيذ النظام وصيانته و يتعين على المنظمة التخطيط لبرنامج تدقيق و وتنفيذه والحفاظ عليه. (Pejic, 2023: 24–27)

الجدول (1)متطلبات المواصفةISO27001

رقم البند	العنوان	التفرعات	الوصف
4	سياق المنظمة	1- فهم المنظمة وسياقها. 2- فهم احتياجات وتوقعات الأطراف المعنية. 3- تحديد نطاق نظام إدارة أمن المعلومات .	يتناول فهم العوامل المؤثرة في أمن المعلومات داخليًا وخارجيًا، وفهم متطلبات الأطراف المعنية، وتحديد النطاق الكامل لنظام إدارة أمن المعلومات.

		4- نظام إدارة أمن المعلومات.	
5	القيادة	1- القيادة والالتزام . 2- سياسة أمن المعلومات. 3- الأدوار والمسؤوليات والسلطات التنظيمية.	يركز على التزام الإدارة العليا، وتحديد السياسة العامة لأمن المعلومات، وتوزيع الأدوار والسلطات.
6	التخطيط	1- إجراءات لمعالجة المخاطر والفرص. 2- أهداف أمن المعلومات والتخطيط لتحقيقها. 3- التخطيط لتغيرات.	يشمل تقييم المخاطر والفرص المتعلقة بأمن المعلومات، وتحديد الأهداف الاستراتيجية وكيفية تحقيقها.
7	الدعم	1- الموارد. 2- الكفاءة. 3- الوعي . 4- الاتصال . 5- المعلومات الموثقة.	يتناول توفير الموارد والكفاءات والتوعية، وضمان التواصل وتوثيق المعلومات بشكل سليم.
8	التشغيل	1- التخطيط والتحكم التشغيل. 2- تقييم مخاطر أمن المعلومات. 3- معالجة مخاطر أمن المعلومات.	تنفيذ العمليات ذات العلاقة بأمن المعلومات ومتابعة معالجة المخاطر بشكل فاعل.
9	تقييم الأداء	1- المراقبة والقياس والتحليل والتقييم. 2- التدقيق الداخلي . 3- مراجعة الإدارة.	يركز على مراقبة أداء نظام أمن المعلومات من خلال التدقيق والمراجعة المستمرة من قبل الإدارة.
10	التحسين	1- عدم المطابقة والإجراءات التصحيحية. 2- التحسين المستمر.	يتناول الإجراءات الواجب اتباعها عند حدوث انحرافات، وكيفية تعزيز النظام باستمرار.

اعداد الباحث بالاعتماد على المواصفة ISO 27001/2022

المحور الثاني: الجانب التطبيقي

5.تطبيق وتحليل نظام إدارة أمن المعلومات على وفق المواصفة الدولية ISO/IEC 27001:2022 في الشركة العامة لتعبئة وخدمات الغاز:

يُعَدّ أمن المعلومات أحد المرتكزات الأساسية في استمرارية الأعمال وحماية البيانات الحساسة داخل المؤسسات الصناعية والخدمية، سيما تلك التي تتعامل مع موارد حيوية مثل الغاز ومشتقاته. وانطلاقاً من أهمية هذا المجال، تسعى الشركة العامة لتعبئة وخدمات الغاز إلى تبني نهج إداري متكامل في إدارة أمن المعلومات، بما يتوافق مع متطلبات المواصفة القياسية الدولية ISO/IEC 27001:2022 ، التي تُعد الإطار الأكثر اعتماداً عالمياً في بناء أنظمة إدارة أمن المعلومات وتقييمها وتطويرها بصورة مستمرة. ويهدف هذا الجزء من البحث إلى تقييم مدى التزام الشركة العامة لتعبئة وخدمات الغاز بمعايير ISO/IEC 27001:2022 وذلك عبر تطبيق قائمة الفحص الخاصة بنشاط إدارة أمن المعلومات وتحليل نتائجها على أرض الواقع ويشمل التحليل مقارنة تفصيلية بين الإجراءات والسياسات المطبقة داخل الشركة والمتطلبات المنصوص عليها في المواصفة الدولية، لتحديد درجة التطابق أو الانحراف بينهما. ولتحقيق دقة في القياس سيتم الاعتماد على المقياس السباعي لتقدير مستوى الالتزام بكل بند من بنود المواصفة، مما يسهم في الحصول على مؤشرات كمية يمكن تحليلها علمياً لتحديد مدى نضج نظام إدارة أمن المعلومات في الشركة. تحليل الفجوات وأوجه التحسين بعد تنفيذ قائمة الفحص، سيتم إجراء تحليل شامل للفجوات التي قد تظهر بين الوضع القائم في الشركة ومتطلبات المواصفة الدولية و يشمل ذلك مراجعة عناصر الحوكمة الأمنية، وآليات إدارة المخاطر، وسياسات حماية المعلومات، وضوابط الوصول إلى البيانات، فضلاً عن تقييم كفاءة برامج التوعية الأمنية للعاملين، ويُتوقع أن يُظهر التحليل مدى حاجة الشركة إلى تطوير بعض الإجراءات التشغيلية أو التقنية من أجل تحقيق التوافق التام مع بنود المواصفة ISO/IEC 27001:2022 ، بما يضمن رفع جاهزيتها في مواجهة التهديدات السيبرانية والمخاطر التقنية المحتملة.

1.5 البند الرابع : سياق المنظمة

الجدول (2) سياق المنظمة

متطلبات المواصفة 4. سياق المنظمة	مطبق كليا موثق كليا	مطبق كليا موثق جزئيا	مطبق كليا غير موثق	مطبق جزئيا موثق كليا	مطبق جزئيا موثق جزئيا	مطبق جزئيا غير موثق	غير مطبق غير موثق
	6	5	4	3	2	1	0
4.1فهم المنظمة وسياقها							
1- تحدد ادارة الشركة القضايا الداخلية والخارجية المرتبطة بالشركة و	□						

المؤثرة في نتائج النظام.							
4.2فهم احتياجات وتوقعات الأطراف المعنية							
2- تقوم ادارة الشركة بتحديد :							
أ- الأطراف المعنية المرتبطة بنظام ادارة امن المعلومات ومتطلباتها.	□						
ب- المتطلبات التي سيتم معالجتها.		□					
4.3 تحديد مجال نظام ادارة امن المعلومات							
3- تقوم ادارة الشركة بتعيين حدود النظام وقابلية تطبيقه لتحديد النطاق.	□						
4- تقوم ادارة الشركة بتحديد نطاق نظام ادارة امن المعلومات وتراعي مايأتي :							
أ- القضايا الداخلية والخارجية		□					
ب- متطلبات الاطراف المعنية		□					
ج- التبعيات وواجهات الربط وطرائق تبادل المعلومات بين أنشطة الشركة و الجهات الخارجية ذات العلاقة			□				
5- توثيق المجال واتاحته كمعلومة ضمن وثائق النظام .		□					
4.4 نظام إدارة أمن المعلومات							
6- إنشاء وتنفيذ نظام ادارة امن المعلومات على وفاقاً لمتطلبات المواصفة (ISO/IEC27001:2022)		□					
7- وضع آليات مناسبة لصيانة وتحسين نظام ادارة امن المعلومات بشكل مستمر		□					
التكرارات	3	6	1	0	0	0	0
النتيجة	18	30	4	0	0	0	0
الوسط الحسابي المرجح	5.2						
النسبة المئوية للمطابقة	86.66%						
حجم الفجوة %	13.34%						

المصدر: من اعداد الباحث استناداً الى بنود المواصفة القياسية الدولية (ISO/IEC 27001:2022).

1- أظهر تقييم البند الرابع "سياق المنظمة" في الشركة العامة لتعبئة وخدمات الغاز نسبة مطابقة عالية بلغت 86.66%، مع فجوة قياسية محدودة بنسبة 13.34%، مما يشير إلى التزام فعلي بمتطلبات المواصفة.ISO/IEC 27001:2022

2- تميز الأداء بوعي مؤسسي واضح بالقضايا الداخلية والخارجية، وتحديد دقيق للأطراف المعنية واحتياجاتهم، مع وضوح في نطاق النظام وحدوده، والتزام عملي بتطبيق متطلبات المواصفة.

3- رصد التقييم ضعفاً في توثيق بعض الإجراءات المطبقة، مما يحد من إثبات الالتزام خلال عمليات التدقيق. كما لوحظ غموض في إدارة متطلبات الأطراف المعنية وتصنيف أولوياتها، وضعف في توثيق حدود النظام وتفاعلاته الخارجية.

4- يعتمد النظام حالياً على المعرفة الضمنية للموظفين أكثر من الإجراءات الموثقة، مما يهدد استدامته على المدى الطويل. ويوصى بتحسين شمولية التوثيق وتعزيز التكامل بين مخرجات البنود الفرعية.

5- بشكل عام، يُعد تطبيق البند ناضجاً وفاعلاً، ويعكس أساساً قوياً وقابلاً للتطوير، مع وجود فرص واضحة للتحسين المستمر لضمان الاستدامة والامتثال الكامل.

2.5 البند الخامس (القيادة)

الجدول (3) القيادة تحليل بند (5) القيادة على وفق متطلبات ISO/IEC 27001:2022

متطلبات المواصفة 5. القيادة	مطبق كليا موثق كليا	مطبق كليا موثق جزئيا	مطبق كليا غير موثق	مطبق جزئيا موثق كليا	مطبق جزئيا موثق جزئيا	مطبق جزئيا غير موثق	غير مطبق غير موثق
	6	5	4	3	2	1	0
1.5القيادة والالتزام							
1- تقوم الادارة العليا للشركة باظهار القيادة والالتزام فيما يتعلق بنظام ادارة امن المعلومات من خلال :							
أ- وضع سياسة وتحديد أهداف لأمن المعلومات تتوافق مع التوجه الاستراتيجي للشركة.			ü				
ب- تكامل متطلبات نظام ادارة أمن المعلومات مع عمليات الشركة.			ü				
ج- توفير الموارد اللازمة لتطبيق وتنفيذ نظام ادارة امن المعلومات في الشركة.	ü						
د- التوعية بأهمية الادارة الفاعلة لأمن المعلومات والامتثال لمتطلبات نظام ادارة امن المعلومات في الشركة.	ü						
ه- ضمان تحقيق نظام ادارة امن المعلومات لديها للنتائج المطلوبة منه.						ü	
و- العمل على دعم وتوجيه الأفراد للمساهمة في فاعلية نظام ادارة امن المعلومات لديها.		ü					
ز- التشجيع على التحسين المستمر لمدخلات وعمليات ومخرجات نظام ادارة امن المعلومات		ü					
ح- تدعم الادارة العليا الأدوار الإدارية الأخرى المتعلقة باظهار القيادة في مجال مسؤولياتهم.	ü						
2.5 سياسة أمن المعلومات							
2- تضع الادارة العليا للشركة سياسة لامن المعلومات على ان تكون :							
أ- ملائمة لغرض الشركة .			ü				
ب- تتضمن اهداف امن المعلومات او توافر اطاراً لتحديد الاهداف .			ü				
ج- تتضمن الالتزام بتلبية المتطلبات المتعلقة بأمن المعلومات .			ü				

3- يتعين ان تكون سياسة امن المعلومات :							
أ- متاحة كمعلومة موثقة.			ü				
ب- متداولة ويتم التواصل بشأنها.			ü				
ج- مُتاحة للأطراف المعنية (بحسب الحاجة).			ü				
3.5 الأدوار والمسؤوليات والصلاحيات							
4- تتأكد الادارة العليا من تعيين المسؤوليات والصلاحيات المتعلقة بأمن المعلومات وابلاغها داخل المنظمة.	ü						
5- تحدد الادارة العليا للشركة المسؤوليات والصلاحيات الخاصة المطلوبة من اجل :							
أ- ضمان توافق نظام ادارة امن المعلومات مع متطلبات المواصفة ISO 27001/2022 .	ü						
ب- تقديم تقارير للادارة العليا حول اداء نظام ادارة امن المعلومات.			ü				
التكرارات	5	2	6	3	0	1	0
النتيجة	30	10	24	9	0	1	0
الوسط الحسابي المرجح	4.35						
النسبة المئوية للمطابقة	%72.50						
حجم الفجوة %	%27.50						

المصدر: من اعداد الباحث استناداً الى بنود المواصفة القياسية الدولية (ISO/IEC 27001:2022).

1- أظهر تقييم البند الخامس (القيادة) نسبة مطابقة بلغت 72.5% مع فجوة قياسية وصلت إلى 27.5%، مما يشير إلى دعم إداري واضح لنظام أمن المعلومات مع حاجة ملحة لتعزيز التوثيق ووضوح الأدوار.

2- تميز الأداء بتوفير الموارد اللازمة ونشر الوعي بأهمية أمن المعلومات، مع تحديد هيكل واضح للمسؤوليات ووجود سياسة أمنية معلنة.

3- كشف التقييم عن ضعف في إتاحة السياسة الأمنية وتكامل النظام مع العمليات التشغيلية، بالإضافة إلى نقص التوثيق الرسمي لممارسات القيادة وغياب آليات قياس الأداء المنتظمة.

4- يتميز الواقع التطبيقي بوجود التزام إداري جزئي، إلا أنه لا يزال يعتمد على الجهود الفردية أكثر من المنهجية المؤسسية الموثقة.

5- بشكل عام، يُظهر البند مستوى مقبولاً من الفاعلية، لكنه يحتاج إلى تحويل الدعم الإداري إلى ممارسات عملية موثقة وقا**بلة للقياس لضمان استدامة النظام وتحسينه المستمر.**

3.5 البند السادس (التخطيط)

الجدول (4) تحليل بند (6) التخطيط على وفق متطلبات ISO/IEC 27001:2022

متطلبات المواصفة	مطبق كليا موثق كليا	مطبق كليا موثق جزئيا	مطبق كليا غير موثق	مطبق جزئيا موثق كليا	مطبق جزئيا موثق جزئيا	مطبق جزئيا غير موثق	غير مطبق غير موثق
6.التخطيط	6	5	4	3	2	1	0
1.6إجراءات معالجة المخاطر والفرص							
1.1.6 عام							
1- تقوم ادارة الشركة بالتخطيط لنظام ادارة امن المعلومات وتراعي القضايا والخارجية ومتطلبات الأطراف لضمان التحسين المستمر.			ü				
2- تخطط ادارة الشركة الإجراءات اللازمة لمعالجة المخاطر والفرص وكيفية الاجراءات وتنفيذها وتقييم فاعليتها.			ü				
2.1.6 تقييم المخاطر والفرص							
3- تحدد ادارة الشركة وتطبق عملية لتقييم المخاطر التي تشمل تحديد معايير المخاطر فضلا عن تحديد معايير قبول المخاطر.		ü					
4- ضمان ان تكون نتائج تقييم المخاطر المتكررة صحيحة وقابلة للمقارنة.		ü					
5- تحديد مخاطر امن المعلومات المرتبطة بفقدان السرية والسلامة والتوافر نطاق ادارة امن المعلومات وتحدد الجهات المسؤولة عن المخاطر.		ü					
6- تحليل المخاطر من خلال تقييم احتمالية حدوثها والاثر المترتب في وقوع							
7- تقييم المخاطر من خلال مقارنة النتائج بالمعايير المحددة وتحديد اولويات التي تم تحليلها.							
8- توثيق عملية معالجة المخاطر والاحتفاظ بها كمعلومة موثقة ضمن وثائق							
3.1.6معالجة مخاطر أمن المعلومات							
9- تقوم ادارة الشركة بتطبيق وتحديد عملية معالجة مخاطر امن المعلومات من اجل :							
أ- تحديد خيارات المعالجة المناسبة لمخاطر امن المعلومات مع مراعاة نتائج المخاطر.							
ب- تحديد الضوابط اللازمة لتنفيذ خيارات معالجة مخاطر أمن المعلومات.		ü					
ج- مقارنة الضوابط التي يتم تحديدها في الفقرة (ب) في اعلاه مع الضوابط في الملحق أ من المواصفة ISO27001/2022 .		ü					
د- إعداد بيان تطبيق مخاطر امن المعلومات يتضمن الضوابط المطلوبة ومبرر ادراجها واستبعادها وما اذا كانت لازمة التنفيذ اولا.			ü				
ه- صياغة خطة لمعالجة مخاطر امن المعلومات .							
و- استحصال موافقة الجهات المعنية على خطة معالجة مخاطر امن المعلومات المخاطر المتبقية لأمن المعلومات .							
2.6أهداف أمن المعلومات والتخطيط لتحقيقها							
10 -ينبغي ان تقوم ادارة الشركة بوضع اهداف أمن المعلومات على مستوى ا والمستويات ذات الصلة		ü					
11- يجب ان تكون الاهداف:							

أ- قابلة للقياس .					i		
ب- تراعي ادارة الشركة بالحسبان عند تحديد الاهداف متطلبات امن المعلوم ومعالجة المخاطر .					i		
ج- خاضعة للمراقبة .				ü			
د- قابلة للتحديث بحسب الحاجة.				ü			
ه- توثيق الاهداف والاحتفاظ بها ضمن وثائق النظام وجعلها متاحة.							
12-تقوم الشركة عند التخطيط لتحقيق الاهداف بتحديد مايأتي:							
أ- ما الذي يجب فعله؟					i		
ب- ما الموارد المطلوبة ؟					i		
ج- من المسؤول عن تحقيق الاهداف؟					i		
د- متى يتم الانتهاء من تحقيق الاهداف؟					i		
ه- كيف سيتم تقييم النتائج؟					i		
3.6 تخطيط التغييرات							
13- تحديد الية او خطة لتنفيذ التغييرات مع مراعاة التغييرات التي ستطرأ ع امن المعلومات مستقبلا.				ü			
التكرارات	7	13	6	0	0	0	0
النتيجة	2	65	24	0	0	0	0
الوسط الحسابي المرجح	5.03						
النسبة المئوية للمطابقة	%83.83						
حجم الفجوة %	%16.17						

المصدر: من اعداد الباحث استناداً الى بنود المواصفة القياسية الدولية (ISO/IEC 27001:2022).

1- أظهر تقييم البند السادس (التخطيط) نسبة مطابقة عالية بلغت 83.83%، مما يعكس منهجية تخطيط ناضجة لنظام أمن المعلومات في الشركة.

2- وتميز الأداء بوجود آلية منظمة لتحديد المخاطر وتقييمها ومعالجتها، مع تحديد أهداف أمنية قابلة للقياس والمراقبة. كما لوحظ التزام واضح بمراعاة متطلبات الأطراف المعنية والقضايا الداخلية والخارجية في عملية التخطيط.

كشف التقييم عن ضعف في التوثيق الرسمي لعمليات التكامل الاستراتيجي بين التوجه العام للشركة ونظام أمن المعلومات.

3- كما أظهر قصوراً في توثيق معايير تقييم المخاطر ومواءمة ضوابط المعالجة مع متطلبات المواصفة. ولوحفت هشاشة في آلية متابعة ومراجعة أهداف أمن المعلومات بشكل دوري.

4- رغم فاعلية النظام الحالية، تشير الفجوة البالغة 16.17% إلى حاجة ماسة لتعزيز التوثيق الشامل وتحسين التكامل الداخلي بين عمليات إدارة المخاطر والأهداف والخطط التشغيلية.

5- يُوصى بالتركيز على ربط مخرجات التخطيط بشكل منهجي لضمان استدامة الأداء والامتثال الكامل للمواصفة الدولية.

4.5 البند السابع (الدعم)

الجدول (5) الدعم على وفق متطلبات ISO/IEC 27001:2022

متطلبات المواصفة	مطبق كليا موثق كليا	مطبق كليا موثق جزئيا	مطبق كليا غير موثق	مطبق جزئيا موثق كليا	مطبق جزئيا موثق جزئيا	مطبق جزئيا غير موثق	غير مطبق غير موثق
7.الدعم	6	5	4	3	2	1	0
1.7 الموارد							
1- تحدد ادارة الشركة وتوافر الموارد اللازمة لإنشاء وتطبيق وصيانة وتحسين نظام ادارة امن المعلومات	□						
2.7الكفاءة							
2- تقوم أدارة الشركة بتحديد وتوفير الكفاءات المطلوبة لعمل نظام إدارة امن المعلومات من اجل :							
أ- تحديد الأفراد الذين يقومون بعمل يؤثر في أداء نظام ادارة أمن المعلومات.	□						
ب- ضمان امتلاك الافراد للكفاءة المطلوبة على اساس التعليم او التدريب اوالخبرة المناسبة.	□						
ج- اتخاذ الإجراءات المناسبة عند الحاجة لاكتساب الكفاءة اللازمة وتقييم فاعلية هذه الاجراءات.	□						
د- الاحتفاظ بوثائق التعليم والتدريب والمهارات والخبرات الخاصة بالافراد كمعلومة موثقة للإستدلال بها على الكفاءة.	□						
3.7 الوعي							
3- تلتزم ادارة الشركة بان الافراد الذين يعملون فيها يكونون على علم بما يأتي :							
أ- على اطلاع ودراية بسياسة امن المعلومات.		□					
ب- بتأثير مساهمتهم في فاعلية النظام وفوائده على تحسين نظام ادارة أمن المعلومات.		□					
ج- عواقب عدم الامتثال لمتطلبات نظام ادارة امن المعلومات.		□					
4.7التواصل							
4- تحدد ادارة الشركة الحاجة للاتصالات الداخلية والخارجية المرتبطة بنظام ادارة امن المعلومات ويشمل ذلك :							
أ- تحديد الامور والموضوعات المتعلقة بأمن المعلومات التي يجب التواصل بشأنها	□						

.							
ب- تعيين وقت الاتصال.							
ج- تحديد الجهات التي يتم التواصل معها							
د- تحديد كيفية وآلية التواصل .							
7.5المعلومات الموثقة							
7.5.1عام:							
5- التأكد من تضمين المعلومات الموثقة المطلوبة بالمواصفة والمعلومات الأخرى التي تراها ادارة الشركة ضرورية.							
2.5.7الإنشاء والتحديث							
6- تتأكد ادارة الشركة عند انشاء وتحديث المعلومة مما يأتي :							
أ- وجود تعريف مناسب (عنوان، مؤلف، تاريخ، مرجع).							
ب- الشكل مثل (اللغة واصدار البرامج والرسومات) والوسائط الورقية والالكترونية.							
ج- التأكد من المراجعة والموافقة من حيث الملاءمة والكفاية.							
3.5.7 ضبط المعلومات الموثقة							
7- تقوم ادارة الشركة بضبط المعلومة الموثقة التي يحتاجها نظام ادارة امن المعلومات بحيث تكون :							
أ- متاحة وصالحة للاستخدام عند الحاجة.							
ب- مؤمن عليها من الفقدان/التلف/الاستخدام غير السليم/الوصول غير المصرح به.							
8- تقوم ادارة الشركة بالسيطرة على المعلومات الموثقة من خلال الانشطة الآتية :							
أ ضبط عمليات التوزيع والوصول والقراءة والتخزين والحفظ.							
بالتحكم في التغييرات (الإصدارات، التعديلات).							
تالتخلص أو الإبقاء على الوثائق على وفق الضوابط.							
ثتحديد الوثائق ذات المصدر الخارجي الضرورية لتشغيل نظام ادارة امن المعلومات والتحكم فيها.							
التكرارات	17	5	0	0	0	0	0
النتيجة	102	25	0	0	0	0	0
الوسط الحسابي المرجح	5.77						
النسبة المئوية للمطابقة	%96.16						
حجم الفجوة %	%3.84						

المصدر: من اعداد الباحث استناداً الى بنود المواصفة القياسية الدولية (ISO/IEC 27001:2022).

1- أظهر تقييم البند السابع "الدعم" مستوى امتثال مرتفعاً جداً بلغ 96.16%، مما يعكس التطبيق الفعلي والفاعل لمتطلبات المواصفة.

2- تميز الأداء بتوفير الموارد البشرية والتقنية اللازمة وإنشاء منظومة متكاملة لإدارة الكفاءات. كما أولت الشركة أهمية لنشر الوعي الأمني ووضع أنظمة واضحة للتواصل الداخلي والخارجي.

3- يبرز النظام كفاءة عالية في إدارة المعلومات الموثقة وضبط عمليات توزيع الوثائق وتحكمها. مع ذلك، تم رصد بعض الثغرات البسيطة التي تحتاج إلى معالجة.

4- تتعلق هذه الثغرات أساساً بضعف توثيق برامج التوعية الأمنية وقياس فاعليتها.

5- كما لوحظ قصور في آليات حماية الوثائق السرية والتحكم الدقيق في إصداراتها.

6- يوجد أيضاً نقص في توثيق إجراءات تقييم أثر التدريب والتأهيل على أداء النظام. يشكل تحسين هذه الجوانب التوثيقية مجالاً رئيسياً للارتقاء بمستوى الامتثال.

7- بشكل عام يعد تطبيق البند ناضجاً ويعكس التزاماً إدارياً قوياً وبنية تحتية مستقرة. تمثل الجهود المستقبلية في تعزيز التوثيق والقياس المستمر للكفاءات البشرية عامل استدامة أساسي للنظام

5.5 البند الثامن: التشغيل

الجدول (6) التشغيل

متطلبات المواصفة	مطبق كليا موثق كليا	مطبق كليا موثق جزئيا	مطبق جزئيا موثق كليا	مطبق جزئيا غير موثق	مطبق جزئيا موثق جزئيا	مطبق جزئيا غير موثق	غير مطبق غير موثق
8.التشغيل	6	5	3	4	2	1	0
1.8التخطيط والتحكم التشغيلي							
1- تخطيط وتنفيذ العمليات اللازمة لتلبية المتطلبات وتنفيذ الإجراءات المحددة من خلال :							
أ وضع المعايير للعمليات .							
ب تنفيذ التحكم بها على وفق المعايير.							
ت توافر المعلومات الموثقة لإثبات تنفيذ العمليات كما هو مخطط.							
ث التحكم في التغييرات المخططة ومراجعة عواقب التغييرات غير المقصودة (الحد من الآثار السلبية).							
ج التأكد من السيطرة على العمليات المتعاقد عليها خارجيًا والمرتبطة بنظام ادارة امن المعلومات.							
2.8 تقييم مخاطر أمن المعلومات							
2- اجراء تقييم للمخاطر بشكل دوري او عند حدوث تغيير هام مع مراعاة معايير تقييم المخاطر.							
3- توثيق نتائج تقييمات امن المعلومات والاحتفاظ بها في ضمن وثائق النظام.							
3.8 معالجة مخاطر أمن المعلومات							

4- تنفذ ادارة الشركة خطة لمعالجة مخاطر امن المعلومات	☐						
5- الاحتفاظ بمعلومات موثقة حول نتائج معالجة المخاطر كدليل على ان نتائج معالجة مخاطر امن المعلومات نفذت على وفق المخطط .	☐						
التكرارات	3	5	1	0	0	0	0
النتيجة	18	25	4	0	0	0	0
الوسط الحسابي المرجح	5.22						
النسبة المئوية للمطابقة	%87						
حجم الفجوة %	%13						

المصدر: من اعداد الباحث استناداً الى بنود المواصفة القياسية الدولية (ISO/IEC 27001:2022).

1- أظهر تقييم البند الثامن "التشغيل" نسبة امتثال عالية بلغت 87%، مما يعكس نضجاً تشغيلياً في إدارة نظام أمن المعلومات.

2- تميز التطبيق بفعالية إجراءات التشغيل والتحكم، ووجود خطة منهجية لمعالجة المخاطر وتوثيق نتائجها، بالإضافة إلى إجراء تقييمات دورية للمخاطر.

3- كما أظهر التقييم التزاماً قوياً بالتحكم في العمليات المتعاقد عليها خارجياً.

4- كشف التحليل عن ضعف في التوثيق الكامل لبعض العمليات التشغيلية، والحاجة إلى تحسين آلية إدارة التغييرات المخططة.

5- كما لوحظ قصور في توثيق إجراءات تقييم المخاطر والاحتفاظ بنتائجها.

6- تمثل السيطرة المعززة على العقود والعمليات الخارجية مجالاً رئيسياً للتحسين.

7- بشكل عام، يعد النظام التشغيلي فاعلاً ومستقراً، مع ضرورة التركيز على تعزيز التوثيق الشامل وضوابط العمليات الخارجية لضمان استمرارية الامتثال والفعالية على المدى الطويل.

6.5 البند التاسع [تقييم الاداء]

الجدول (7) تقييم الأداء

متطلبات المواصفة	مطبق كليا موثق كليا	مطبق كليا موثق جزئيا	مطبق كليا غير موثق	مطبق جزئيا موثق كليا	مطبق جزئيا موثق جزئيا	مطبق جزئيا غير موثق	غير مطبق غير موثق
9.تقييم الأداء	6	5	4	3	2	1	0
1.9 المراقبة والقياس والتحليل والتقييم							
1- تعمل ادارة الشركة على مراقبة وقياس وتحليل وتقييم نظام ادارة امن المعلومات من خلال :							
أ- تحديد ما يجب مراقبته وقياسه (بما في ذلك الضوابط والعمليات).		☐					
ب- تحديد طرائق القياس والمراقبة والتحليل والتقييم لضمان نتائج صحيحة وقابلة للمقارنة.		☐					
ج- تحديد توقيتات إجراء المراقبة والقياس وتحديد من يقوم باجرائها.	☐						
د- تحديد توقيتات واليات مراجعة وتحليل وتقييم النتائج ومن سيقوم بها.	☐						
ه- الاحتفاظ بمعلومات موثقة كدليل على النتائج.	☐						
و- استخدام النتائج وتوثيقها لتقييم فاعلية وأداء نظام ادارة أمن المعلومات.	☐						
2.9 التدقيق الداخلي							
1.2.9 عام							
2- تجري ادارة الشركة التدقيق الداخلي على فترات مخطط لها لمعرفة ما اذا كان نظام ادارة امن المعلومات :							
أ- يتوافق مع متطلبات الشركة الخاصة بنظام ادارة امن المعلومات .		☐					
ب- يتوافق مع متطلبات المواصفة ISO 27001/2022.	☐						
ج- يتم التأكد والتحقق من صيانة وتطبيق النظام بشكل فاعل.		☐					
2.2.9 برنامج التدقيق الداخلي							
3- تقوم ادارة الشركة بانشاء وتنفيذ والمحافظة على برنامج التدقيق الداخلي والذي يتضمن الطرائق المستخدمة والمسؤوليات ومتطلبات التخطيط واعداد التقارير .	☐						
4- تراعي ادارة الشركة اهمية العمليات المعنية ونتائج التدقيقات السابقة عند انشاء برنامج التدقيق.	☐						
5- تقوم ادارة الشركة عند انشاء برنامج التدقيق الداخلي بتحديد مايأتي :							
أ- معايير التدقيق ونطاق العمليات.	☐						
ب- اختيار المدققين .		☐					
ج- ضمان ابلاغ الادارة المعنية بنتائج عمليات التدقيق.	☐						
د- الاحتفاظ بمعلومات موثقة كدليل على تنفيذ برنامج التدقيق.	☐						
3.9 مراجعة الادارة							
1.3.9 عام							
6- تراجع الادارة العليا للشركة نظام ادارة امن المعلومات الخاص بالشركة على مدد زمنية مخطط لها بما يضمن استمرار النظام وملائمته وكفائته وفاعليته.	☐						
2.3.9 مدخلات مراجعة الادارة							
7- تشمل مراجعة الادارة :							
أ- حالة الاجراءات المتخذة من الادارات السابقة.	☐						
ب- التغييرات في القضايا الداخلية والخارجية المرتبطة بنظام ادارة امن المعلومات.	☐						

ج- التغييرات في توقعات واحتياجات الاطراف المهتمة والمعنية بنظام ادارة امن المعلومات.	□						
د- التغذية الراجعة والملاحظات على النظام التي تشمل (حالات عدم المطابقة ، والاجراءات التصحيحية ،ونتائج التدقيق والمراقبة والقياس وتحقيق اهداف امن المعلومات).	□						
ه- التغذية الراجعة والملاحظات الواردة من الاطراف المهتمة.	□						
و- نتائج تقييم المخاطر.	□						
ز- فرص التحسين المستمر.	□						
3.3.9 نتائج مراجعة الادارة							
8- تتضمن نتائج المراجعة القرارات المتعلقة بالتحسين المستمر والقرارات المتعلقة بالحاجة إلى موارد إضافية و التعديلات على النظام والاجراءات التصحيحية وان تكون المعلومات متاحة كدليل على نتائج مراجعة الادارة .		□					
التكرارات	18	6	0	0	0	0	0
النتيجة	108	30	0	0	0	0	0
الوسط الحسابي المرجح	5.75						
النسبة المئوية للمطابقة	%95.80						
حجم الفجوة %	%4.20						

المصدر: من اعداد الباحث استناداً الى بنود المواصفة القياسية الدولية (ISO/IEC 27001:2022).

1- أظهر تقييم البند التاسع "تقييم الأداء" نسبة امتثال مرتفعة جداً بلغت 95.8%، مما يعكس نظاماً متقدماً للمراقبة والقياس والتقييم.

2- تميز التطبيق بوجود آليات دقيقة لرصد الأداء، وتنفيذ فاعل للتدقيق الداخلي الدوري، ومراجعة إدارية منتظمة تركز على التحسين المستمر.

3- كما أظهر توثيقاً شاملاً لنتائج القياس والتحليل.

4- كشف التقييم عن فجوة طفيفة تتعلق بعدم التوثيق الكامل لمنهجيات الرقابة والقياس، مما قد يؤثر على اتساق المؤشرات عبر الزمن.

5- كما لوحظ قصور في توثيق معايير اختيار وتأهيل المدققين الداخليين، ومحدودية في توثيق مخرجات المراجعات الإدارية وقراراتها.

6- بشكل عام، يُعد نظام تقييم الأداء ناضجاً وفاعلاً، مع حاجة إلى تعزيز دقة مؤشرات القياس وتحسين توثيق عمليات الاختيار والمراجعة لضمان استدامة التحسين.

7.5 البند العاشر التحسين

الجدول (8) التحسين

متطلبات المواصفة 10.التحسين	مطبق كليا موثق كليا	مطبق كليا موثق جزئيا	مطبق كليا غير موثق	مطبق جزئيا موثق كليا	مطبق جزئيا موثق جزئيا	مطبق جزئيا غير موثق	غير مطبق غير موثق
	6	5	4	3	2	1	0
1.10التحسين المستمر							
1- التأكد من ان ادارة الشركة تعمل بشكل مستمر على تحسين ملاءمة وكفاية وفاعلية نظام إدارة أمن المعلومات لديها .	✓	✓					
2.10 عدم المطابقة والاجراء التصحيحي							
2- تقوم ادارة الشركة في حالة عدم المطابقة بالآتي:							
أ- اتخاذ الاجراءات المطلوبة وتصحيح حالة التعامل مع العواقب.		✓	✓				
ب- تقييم الحاجة الى اتخاذ اجراءات للقضاء على عدم المطابقة وضمان عدم تكرارها او حدوثها في مكان اخر من خلال مراجعة عدم المطابقة وتحديد عدم اسبابها وتحديد الحالات المماثلة والمحتملة.		✓	✓				
ج-تنفيذ الاجراءات المطلوبة.		✓	✓				
د- مراجعة فاعلية الاجراءات التصحيحية المتخذة.		✓	✓				
ه- اجراء التغييرات المطلوبة على النظام اذا لزم الامر.		✓	✓				
و- ضمان ان تناسب الاجراءات التصحيحية حالات عدم المطابقة التي تم تشخيصها.		✓	✓				
3- توثيق المعلومات واتاحتها كدليل على :							
أ-طبيعة حالات عدم المطابقة والاجراءات التي يتم اتخاذها لاحقا .		✓	✓				
ب-نتائج الاجراءات التصحيحية.		✓	✓				
التكرارات	1	8	0	0	0	0	0
النتيجة	6	40	0	0	0	0	0
الوسط الحسابي المرجح	5.11						
النسبة المئوية للمطابقة	85.16%						
حجم الفجوة %	14.84%						

المصدر: من اعداد الباحث استناداً الى بنود المواصفة القياسية الدولية (ISO/IEC 27001:2022).

1- أظهر تقييم البند العاشر "التحسين" نسبة امتثال بلغت 85.16%، مما يعكس التزاماً بمبدأ التحسين المستمر لنظام أمن المعلومات.
2- تميز الأداء بمعالجة منهجية لحالات عدم المطابقة وتطبيق إجراءات تصحيحية فاعلة، مع تحليل للأسباب الجذرية ومراجعة دورية لفعالية الإجراءات المتخذة.
3- كشف التقييم عن ضعف كبير في التوثيق الرسمي لآليات التحسين المستمر ومنهجياته. كما لوحظ قصور في التوثيق الشامل للإجراءات التصحيحية ونتائجها، مما يحد من إثبات فعاليتها أثناء عمليات التدقيق.
4- يؤثر هذا الضعف في ربط الإجراءات التصحيحية بالأهداف الأمنية المحددة وقياس أثرها الحقيقي.
5- يؤدي غياب التوثيق الكامل إلى انفصال الممارسات الفعلية عن دورة التحسين المغلقة (PDCA)، مما يعيق استخلاص الدروس المستفادة ويعرض النظام لتكرار الأخطاء.
6- يُوصى ببناء إطار توثيقي معياري لعمليات التحسين، وربطها بشكل منهجي بالأهداف الأمنية، لضمان استدامة التحسين وقابلية القياس.
ومن خلال ما ورد في اعلاه يمكن تلخيص نتائج قائمة الفحص (نسبة المطابقة , حجم الفجوة) لنظام ادارة امن المعلومات على وفق المواصفة ISO/IEC27001:2022 على مستوى الشركة المبحوثة وكما مبين في الجدول في أدناه :

جدول(9) ملخص لتقييم متطلبات لنظام ادارة امن المعلومات على وفق المواصفة ISO/IEC27001:2022

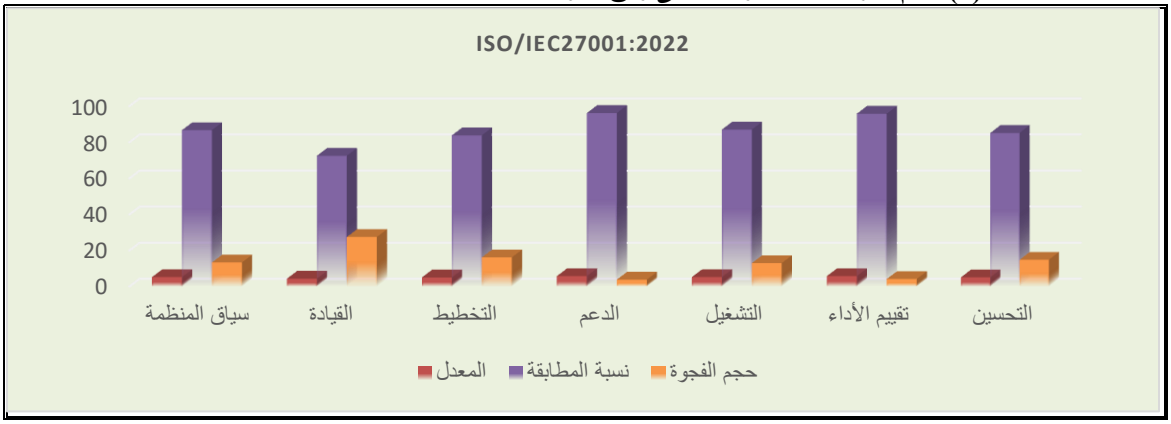
ت	تسلسل البند	بنود المواصفة	الوسط الحسابي المرجح	النسبة المئوية للمطابقة (%)	حجم الفجوة(%)
1	4	سياق المنظمة	5.2	86.66	13.34
2	5	القيادة	4.35	72.5	27.5
3	6	التخطيط	5.03	83.83	16.17
4	7	الدعم	5.77	96.16	3.84
5	8	التشغيل	5.22	87	13
6	9	تقييم الأداء	5.75	95.8	4.2
7	10	التحسين	5.11	85.16	14.84
المجموع			36.43	607.11	92.89
المعدل			5.20	86.73	13.27

المصدر: من اعداد الباحث استناداً الى بنود المواصفة القياسية الدولية (ISO/IEC 27001:2022).

في ضوء النتائج الواردة في الجدول، يتّضح أن المنظمة تمتلك نظام عملٍ مستقرٍ وقادرٍ على تحقيق مستوى جيد من مطابقة المواصفة، إذ بلغ المعدل العام قرابة 86.7%، وهو مؤشر يعكس التزامًا واضحًا بالممارسات الأساسية للجودة وتشير الأرقام إلى وجود جوانب متقدمة في بيئة العمل، سيما في بنود الدعم وتقييم الأداء، حيث يظهر الجدول أن البنية التنظيمية قادرة على توفير الموارد المناسبة وضبط عمليات القياس والمتابعة بشكل فاعل، مما يعزز موثوقية النظام ويُسهِم في رفع مستوى الأداء بشكل عام. وبرغم من هذا التقدم، تُظهِر النتائج فجوة بارزة في جانب القيادة، وهي الفجوة الأكبر مقارنة ببقية البنود. هذا يشير إلى الحاجة لتعزيز الدور القيادي في التواصل الداخلي، وتوضيح التوجهات الاستراتيجية، وتفعيل المتابعة المستمرة لضمان تبنّي العاملين لسياسات النظام وأهدافه. معالجة هذا الجانب تحديدًا ستنعكس إيجابًا على بقية مكونات النظام، لأن القيادة تُعدّ العامل الأساسي في ترسيخ ثقافة الجودة. أما البنود الأخرى مثل سياق المنظمة، والتخطيط، والتشغيل، والتحسين فهي تحقق نسبًا جيّدة ، لكنها تستدعي تطويرًا تدريجيًا لضمان انسجام أكبر بين العمليات وتعزيز الارتباط بين الخطط والتطبيق الفعلي و تحسين هذه الجوانب سيساعد المنظمة على تقليص الفجوات المتبقية ودفع مستوى المطابقة إلى نطاق أكثر استدامة. وبشكل عام، تُظهر النتائج صورة إيجابية تؤكد أن المؤسسة تسير في الاتجاه الصحيح، وأن الفجوات المتبقية محدودة ويمكن التعامل معها بسهولة عبر خطوات تطويرية واضحة ومباشرة، سيما في الجوانب القيادية والتنظيمية. ويوضح

المخطط البياني في أدناه النسب الاجمالية للمطابقة وحجم الفجوات لبنود نظام ادارة امن المعلومات على وفق المواصفة القياسية ISO/IEC27001:2022 وكما مبين في الشكل (2)

الشكل (2) نظام ادارة امن المعلومات على وفق المواصفة القياسية ISO/IEC27001:2022



الاستنتاجات والتوصيات

الجدول(10) الاستنتاجات والتوصيات وآليات التنفيذ

ت	الاستنتاجات	التوصيات	الية تنفيذ
1	يبين التحليل أن الشركة العامة لتعبئة وخدمات الغازتمتلك قاعدة مؤسسية راسخة تدعم تطبيق أنظمة الإدارة الحديثة و تحسن اداءها فضلاً عمّا تقوم به الشركة من انشطة ترتبط بخدمات الغاز السائل LPG والمتمثلة (التعبئة، والنقل، والتوزيع، والخدمات الفنية، وتركيب شبكات الغاز ومنافذ تجهيز سيارات الغاز) وأسهمت هذه البيئة المؤسسية بشكل مباشر بدعم بنود متعددة من المواصفة ISO 27001:2022 مثل الدعم وتقييم الأداء وسياق المنظمة .	استثمار القاعدة المؤسسية الحالية والنظام المتكامل الناجح كأساس متين وحاضنة طبيعية لبناء نظام إدارة أمن معلومات (ISMS) قوياً ومتماسكاً، بحيث يكون متجذراً في ثقافة الشركة ومتناغماً تماماً مع أهدافها الاستراتيجية التشغيلية والتجارية، مما يضمن الاستدامة والكفاءة.	أ- تشكيل لجنة تضم من التشكيلات ذات العلاقة. ب- تقوم اللجنة بتحليل نقاط التداخل بين متطلبات ISO 27001 والأنظمة الحالية. ج-تطوير دليل إجراءات موحد للسياسات والعمليات المشتركة. د- تدريب فرق التدقيق الداخلي على معايير النظام المدمج. ه- تنفيذ دورة تدقيق تجريبية ومتابعة النتائج.
2	حققت الشركة معدل امتثال كلي مقدارهُ 86.7% و يعكس ذلك أجراءات وممارسات الشركة التي تقوم بها الشركة في مجال أمن المعلومات بشكل يومي وفعلي وضمن بيئة مستقرة ومنظمة وعلى الرغم من ذلك فهنالك تحدٍ مهمّ يتمثل في "غياب الأثر الكتابي" أي أنها تفتقر الى التوثيق بشكل كافٍ هذا الأمر يجعل النظام معتمداً بشكل مفرط على خبرات الأفراد وذاكرتهم (المعرفة الضمنية)، مما يهدد استمرارية العمل في حال مغادرة الكوادر المؤهلة.	تحويل رأس المال البشري والممارسات العملية الفردية إلى أصول مؤسسية صريحة وموثقة، يمكن الاعتماد عليها ومراجعتها وتطويرها بمعزل عن الأفراد. يهدف هذا التحول إلى ضمان استدامة النظام الأمني، وحمايته من تقلبات الموارد البشرية، وخلق أساس متين للتدريب والتفويض والمساءلة.	أ- تشكيل فريق توثيق. ب- جمع الممارسات الحالية و إعادة صياغتها في ضمن إجراءات رسمية. ج- اعتماد نماذج موحّدة. د- إجراء مراجعات دورية للتأكد من تحديث المستندات بما يتلاءم مع المتغيرات التشغيلية والتقنية.
3	تمتلك الشركة أنظمة تقنية متقدمة مثل نظم الموارد البشرية والصادر الإلكتروني، إلا إن هذه الأنظمة تعمل بشكل منفصل عن الأهداف الاستراتيجية لأمن المعلومات، ما يقلل من القيمة الأمنية للمنظومة الرقمية.	يُوصى بإعادة تعريف دور تقنية المعلومات من مزوّد خدمات داعم إلى شريك استراتيجي في تحقيق الأهداف الأمنية، من خلال دمج مبادئ الأمن منذ مراحل التصميم الأولية للمشاريع الرقمية، واعتماد إطار حوكمة يضمن اتساق القرارات التقنية مع إدارة المخاطر، مع عَد الأصول التقنية مثل أنظمة البيانات أصولًا معلوماتية استراتيجية تتطلب مستويات حماية تتناسب مع قيمتها وأثرها المؤسسي.	أ- دمج الحوكمة التقنية والأمنية لضمان مراجعة المشاريع رقميًّا من منظور أمني مبكّر. ب- تصنيف الأصول المعلوماتية حسب الحساسية والأثر لتحديد مستويات الحماية. ج-تضمين ممثل أمني في فرق تطوير المشاريع الرقمية لتطبيق "الأمن بالتصميم." د- ربط مؤشرات الأداء التقنية بفاعلية الأمن في تقييم نجاح المشاريع.
4	إن وجود تشكيلات متخصصة مثل شعبة ادارة الجودة وتقييم الاداء المؤسسي و قسم تقنية المعلومات والاتصالات المدعوم بشعب متخصصة في الشبكات وأمن	يُوصى بأن يكون أمن المعلومات من اولويات صنع القرار الاستراتيجي في الشركة ، مع تحديد واضح وموثّق للمسؤوليات	تشكيل لجنة أمن معلومات تنفيذية تمثل التشكيلات الأساسية لتقوم بما يأتي : أ- تحديد الأدوار والصلاحيات لكل وحدة

	المعلومات يُسهم في تحقيق نسب امتثال جيدة في بنود "الدعم" و"تقييم الأداء" وبرغم من ذلك يُلحظ ضعف توظيف هذه الإمكانيات في تعزيز الحوكمة الأمنية الشاملة.	والصلاحيات لكل وحدة تخصصية، وتعزيز التنسيق بين الإدارات لربط متطلبات الأمن سيما معايير ISO/IEC 27001:2022 بمؤشرات الأداء وضمان المساءلة الفاعلة.	عبر مصفوفة مسؤوليات واضحة. ب- دمج متطلبات ISO/IEC 27001:2022في السياسات والإجراءات التشغيلية الحالية. ج-ربط مؤشرات أمن المعلومات بمؤشرات الأداء الرسمية لكل إدارة. د- اجراء المراجعة الدورية لقياس الفاعلية واتخاذ قرارات تحسينية.
5	تقوم الشركة بممارسة اجراءات أمن المعلومات ضمن بيئة تتبنى أصلاً نظام الإدارة المتكامل IMS الذي يضم مجموعة من المواصفات وهي(9001 ،14001، 45001)مما عزز من جاهزية الشركة في مواءمة العمليات والإجراءات مع متطلبات ISO 27001:2022.مما انعكس على ارتفاع نسب الالتزام ببند "سياق المنظمة" وهو دليل على قدرة الشركة على تحليل بيئتها الداخلية والخارجية وتحديد الأطراف المعنية بوعي مؤسسي واضح.	توسيع نطاق نظام الإدارة المتكامل ليشمل ISO 27001:2022 بشكل كامل، مع الافادة من التجربة المتراكمة في تطبيق المواصفات الأخرى لتسريع عملية الامتثال.	اعداد آلية لمراجعة الإجراءات المشتركة لنظام تشمل: أ- تحديث نماذج السجلات. ب- دمج أمن المعلومات في برامج التدقيق الداخلي. ج-تحديد آليات للرصد والتحسين المستمر في ضمن الإطار المؤسسي القائم.
6	أظهر التقييم وجود قصور في مستوى توثيق ضوابط الأمنية بالرغم من التكامل التنظيمي ويظهر ذلك بوضوح في وثيقة بيان التطبيق إذ تبين عدم توفر مبررات رسمية لاختيار الضوابط أو استبعادها وهو ما يشكل فجوة جوهرية تعيق قدرة الشركة على إثبات الامتثال أمام الجهات الرقابية.	يُوصى بتوثيق رسمي وشفاف لجميع الضوابط الأمنية المطبّقة أو المستبعدة، يتضمّن تبريرات موضوعية قائمة على تقييم المخاطر، ويوضّح أسباب اعتماد كل إجراء أمني أو التخلّي عنه، وذلك لضمان انسجام الإطار الأمني مع طبيعة العمليات المؤسسية وجعله قابلاً للمراجعة والتدقيق من قبل الجهات الداخلية والخارجية.	تشكيل فريق متعدد التخصصات لمراجعة الضوابط كما الآتي: أ- مقارنة كل ضابطة بسجل المخاطر المؤسسي. ب- توثيق قرار الاعتماد أو الاستبعاد. ج-مراجعة الوثيقة من الإدارة العليا واعتمادها د- تحديثها دوريًا وربطها بدورة مراجعة نظام أمن المعلومات.
7	تفتقر أهداف أمن المعلومات في الشركة إلى أدوات قياس دقيقة أو مؤشرات أداء واضحة برغم من وجودها في ضمن النظام حيث أشارت نتائج التقييم إلى ضعف متابعة الأهداف وربطها بنتائج تقييم المخاطر مما أدى إلى فجوات في التخطيط الأمني وعدم وضوح أثر الأهداف على الأداء المؤسسي العام رغم أشتراط المواصفة بوضوح الأهداف وقابليتها للقياس.	يُوصى بتطوير منظومة متكاملة لقياس أداء أمن المعلومات تقوم على مؤشرات أداء رئيسة ، قابلة للقياس والمتابعة والتحسين المستمر، وتُرتكز على ربط الأهداف الأمنية بإطار المخاطر المؤسسية، بما يحوّل أمن المعلومات إلى وظيفة إدارية قادرة على إثبات قيمتها الملموسة وتأثيرها المباشر في استمرارية الأعمال واتخاذ القرار.	أ- تحديد الأصول والمعلومات الحرجة وربطها بمخاطر الأعمال الأساسية. ب- استخلاص أهداف أمنية ذكية من إطار تقييم المخاطر المؤسسي. ج-تصميم مؤشرات أداء رئيسة لكل هدف، مع تحديد مصادر البيانات و طريقة القياس. د-مراجعة المؤشرات وتحديثها في فترات محددة أو عند حدوث تغيير جوهري في العمليات أو المخاطر.
8	تبين نتائج التقييم ان نسبة المطابقة في بند القيادة بلغت 72.5%مع وجود فجوة مقدارها27.5% وهي أعلى فجوة مسجلة في ضمن بنود التقييم و يشير ذلك إلى ضرورة تعزيز دور القيادة في دعم النظام الأمني بخاصة في الجوانب المتعلقة بتحديد المسؤوليات والصلاحيات الأمنية وتوثيقها بشكل كامل .	يُوصى بتعزيز التزام القيادة العليا بنظام أمن المعلومات من خلال تحديد أدوارها الأمنية وتوثيق مسؤولياتها وصلاحياتها بشكل رسمي عبر مصفوفة مُعتمدة وتجسيد هذا الالتزام عبر قرارات وتوجيهات استراتيجية ملموسة، تُظهر إشرافها المباشر وتجعل دعمها للمنظومة الأمنية مرئيًا، قابلاً للقياس، ومُلزِمًا لبقية مستويات المؤسسة.	أ- تعريف الادارة العليا بأدوارها الامنية. ب- إعداد مصفوفة للأمن وتوثيق الأدوار (مسؤول، مساهِم، مُطلَع، موافِق). ت- اعتماد المصفوفة رسميًا ضمن وثائق النظام بقرار إداري. ث- ربط التزام القيادة بمؤشرات أداء قابلة للقياس. ج- اجراء المراجعة الدورية لضمان الاستمرارية والفاعلية.
9	بلغت نسبة مطابقة بند تقييم الأداء 95.8% ويبين ذلك مستوى النضج العال بينما كانت الفجوة منخفضة جداً حيث بلغت4.2% مما يدل على قدرة الشركة على تنفيذ عمليات المراقبة والقياس والتدقيق الداخلي بفاعلية كبيرة لكن رغم هذا المستوى المتقدم ظهرت مجموعة من الملاحظات المتعلقة بضعف تحديد ما يجب قياسه وطرائق القياس بدقة كافية .	يُوصى بتطوير منهجية موحدة لقياس أداء أمن المعلومات تُحدد ما يُقاس، كيف يُقاس، ومتى، عبر دليل إجرائي يشمل مصادر البيانات وأدوات التحليل، بهدف الانتقال من قياس «الوجود» إلى تقييم فعلي لـ«الفاعلية» و«الكفاءة».	أ- تحديد مؤشرات الأداء التي تعكس الفاعلية والكفاءة (وليست مجرد تطبيق شكلي). ب- تطوير دليل إجراءات قياس يُحدّد: مصادر البيانات، وأدوات الجمع، وطرائق التحليل، وتوقيتات المراجعة. ج-تدريب الفرق المعنية على تطبيق المنهجية وتوحيد أساليب القياس. د- مراجعة دورية للمنهجية وتحديثها بناءً على نتائج التقييم والتغيرات التشغيلية.

10	رغم امتلاك الشركة آلية واضحة لمعالجة الأخطاء عند حدوثها إلا أنها تفتقر إلى مرحلة "إغلاق الدورة"، و التي يتم فيها توثيق الحلول وتسجيل الدروس المستفادة والتأكد من فاعلية الحل على المدى الطويل ويؤدي غياب هذه الخطوة الى جعل الأخطاء تتكرر لأن الحلول لا تتم متابعة نتائجها بشكل كامل ولا يتم تحديث الإجراءات بناءً عليها	يُوصى بتبني دورة تصحيحية ووقائية متكاملة لإدارة الحوادث الأمنية، تتضمّن توثيق الإجراءات، التحقق من فاعليتها، واستخلاص الدروس المستفادة، لضمان إغلاق منهجي للحوادث وتحويل الخبرات السابقة إلى تحسينات استباقية ومستدامة.	أ- تفعيل نموذج موحد للإبلاغ عن الحوادث الأمنية يتضمّن حقولًا للإجراءات التصحيحية والوقائية. ب- إدراج خطوة إلزامية للتحقق من فاعلية كل إجراء بعد تنفيذه (باستخدام مؤشرات أو مراجعة ميدانية). ج- إنشاء سجل مركزي للدروس المستفادة، يُحدّث بعد كل حادث ويُرفق بإجراءات التحسين ذات الصلة. د- مراجعة دورية للإجراءات المُعتمدة لضمان استمرار فاعليتها وملاءمتها للمتغيرات.
11	لنشاط الشركة الواسع الذي يمتد ليشمل مجموعة كبيرة من معامل تعبئة الغاز الحكومية والاهلية وورش إضافة منظومات غاز السيارات ومنافذ تعبئة فضلاً عن النشاطات الاخرى يوضح ذلك أن الأطراف الخارجية تمثل عاملاً حرجاً في أمن المعلومات ويتضح ذلك فعلياً في التقييم من خلال ضعف الضوابط المتعلقة بالموردين والمتعاقدين ما يجعل هذا الجانب أحد مصادر الخطر التي تحتاج إلى معالجة استراتيجية.	يُوصى بدمج متطلبات أمن المعلومات في دورة حياة إدارة الموردين بكامل مراحلها من الاختيار إلى إنهاء العلاقة عبر إطار استباقي لإدارة مخاطر الأطراف الخارجية يتضمّن ضوابط أمنية ملزمة ومعايير تقييم واضحة قبل وأثناء وبعد التعاقد، لضمان سلامة سلسلة التوريد وحماية القيمة المؤسسية.	أ- تحديد معايير أمنية إلزامية لتقييم الموردين الجدد (مثل شهادات الامتثال، وسياسات الحماية). ب- إدراج بنود أمنية في عقود الموردين، مع تحديد مسؤولياتهم في حماية المعلومات. ج- إجراء تقييم دوري أو عند التغيير لأمن موردي الخدمات الحساسة. د- إنشاء سجل مركزي لجميع تقييمات الموردين والحوادث المرتبطة بهم. ه- مراجعة إجراءات إنهاء العلاقة مع الموردين لضمان استرداد البيانات وقطع الوصول بشكل آمن.
12	برغم من امتلاك الشركة برامج توعية أمنية عامة إلا أن التقييم أظهر ضعفاً في توثيق هذه البرامج وغياب القياس الحقيقي لمدى تأثيرها في سلوك العاملين. ونظراً لاتساع القوى العاملة وتعدد مواقع العمل، يعد هذا القصور ثغرة مهمة قد تؤدي إلى مخاطر بشرية لا يمكن تجاهلها.	يُوصى بتحويل برامج التوعية الأمنية إلى استثمار استراتيجي مستدام، عبر حملات مستهدفة تشمل التدريبات، ومحاكاة الهجمات، وأنشطة تفاعلية، مع ربطها بمؤشرات قياس تُركّز على تغيير السلوك الفعلي لا مجرد الحضور لبناء ثقافة أمنية مؤسسية فاعلة.	أ- تحليل الفجوات والمخاطر لتحديد احتياجات كل فئة وظيفية ب- تصميم حملات توعوية مخصصة (ورش و محاضرات) ج- تطبيق مؤشرات قياس للسلوك مثل نسبة الوقوع في اختبارات التصيد قبل وبعد التدريب. د- اعتماد خطة سنوية موحدة تشمل التوقيت، والمحتوى، وآليات التقييم. ه- مراجعة النتائج دوريًا وتحديث المحتوى بناءً على البيانات والتطورات الأمنية.

المصادر References

1- International Telecommunication Union. (2020). Security in telecommunications and information technology: An overview of issues and the deployment of existing ITU-T recommendations for secure telecommunications (7th ed.). https://www.itu.int/pub/T-HDB-STR-SEC_MANUAL-2020

2- ISO, International Organization for Standardization, "ISO 31000 Risk management – Guidelines", Second edition (2018), Geneva, Switzerland.

3- ISO, International Organization for Standardization, "ISO 8000-2 Data quality – Part 2: Vocabulary", Second edition (2020), Geneva, Switzerland.

4- ISO. (2020). ISO 8000-2:2020 – Data quality — Part 2: Vocabulary. International OrganizationStandardizationhttps://cdn.standards.iteh.ai/samples/80543/52a290375802 4943b67d346ffb2a64bc/ISO-8000-2-2020.

5- ISO/IEC, International Organization for Standardization/International Electrotechnical Commission, "ISO/IEC 27000 Information technology – Security techniques – Information security management systems – Overview and vocabulary", Fifth edition (2018), Geneva, Switzerland.

6- ISO/IEC, International Organization for Standardization/International Electrotechnical Commission, "ISO/IEC 27001 Information security, cybersecurity and

privacy protection – Information security management systems – Requirements", Third edition (2022), Geneva, Switzerland.
7- ISO/IEC, International Organization for Standardization/International Electrotechnical Commission, "ISO/IEC 27002 Information security, cybersecurity and privacy protection – Information security controls", Third edition (2022), Geneva, Switzerland.
8- ISO/IEC, International Organization for Standardization/International Electrotechnical Commission, "ISO/IEC 27005 Information security, cybersecurity and privacy protection – Guidance on information security risk management", Fourth edition (2022), Geneva, Switzerland.
9- ISO/IEC, International Organization for Standardization/International Electrotechnical Commission, "ISO/IEC 27032 Cybersecurity – Guidelines for internet security", Second edition (2023), Geneva, Switzerland.
10- ISO/IEC, International Organization for Standardization/International Electrotechnical Commission, "ISO/IEC 11179-1 Information technology – Metadata registries (MDR) – Part 1: Framework", Fourth edition (2023), Geneva, Switzerland.
11- ISO/IEC. (2023). Information technology — Metadata registries (MDR) — Part 1: Framework (ISO/IEC 11179 1:2023). International Organization for Standardization. https://cdn.standards.iteh.ai/samples/78914/e8406ec4368241d6817147cb5ddb5d85/ISO-IEC-11179-1-2023.
12- Joint Task Force Transformation Initiative. (2013). Security and privacy controls for federal information systems and organizations (NIST Special Publication 800-53, Rev. 4). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r4
13- Maurer, T., & Morgus, R. (2014). Compilation of existing cybersecurity and information security related definitions. New America. https://www.newamerica.org/cybersecurity-initiative/reports/compilation-existing-cybersecurity-and-information-security-related-definitions/
14- National Institute of Standards and Technology)NIST(. (2004). Standards for Security Categorization of Federal Information and Information Systems (FIPS PUB 199). U.S. Department of Commerce. https://csrc.nist.gov/publications/detail/fips/199/final
15- National Institute of Standards and Technology. (2017). An introduction to information security (Special Publication No. 800-12 Rev. 1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-12r1
16- Voicu, Adelina-Elena. 2022. *Combined approach to perform Security Maturity Reviews based on best practice industry standards for OT*. Master's Thesis, Department of Mathematics and Computer Science, Eindhoven University of Technology.
17- Yli-Karro, Valtteri, (2025), Ensuring NIS 2 Compliance in an ISO/IEC 27001 Certified Organization Master's Thesis. Faculty of Information Technology and Communication Sciences, Tampere University.