الجمهورية العربية السورية
وزارة التعليم العالي والبحث العلمي
المعهد العالي لإدارة الأعمال HIBA
الماجستير في إدارة الأعمال

دور نظم إدارة أمن المعلومات في تحسين الثقة والمصداقية في المنظمات الدولية

دراسة حالة منظمة المجلس النرويجي للاجئين

رسالة أعدت لاستكمال متطلبات الحصول على درجة الماجستير في إدارة الأعمال

MBA

(اختصاص إدارة العمليات)

إعداد الطالب:

المهندس محمد رياض شربجي

إشراف:

الأستاذ الدكتور طلال عبود

العام الدراسي: 2025

©2025

ALL RIGHTS RESERVED

الإهداء

إلى روح والدي الطاهرة،

الحاضر الغائب، الذي ما زلتُ أراه في كل خطوة أخطوها، وفي كل سؤال يوقظ فضولي، وفي كل تحدٍّ يذكّرني بصوته وهو يدفعني لأفكّر، أحلّل، وأؤمن بأنني قادرٌ على تخطي أي صعوبة. كان يؤمن بي بطريقة لم يدركها أحد، وما زال أثر تلك الثقة يرافقني في دراسة وفي حياتي كلها.

وإلى أمي، القلب الذي لا يلين،

التي غمرتني بحنانها، ودعت لي في السّر والعلن، واحتضنت أخطائي قبل نجاحاتي، وظلّت تؤمن بأنني سأصل مهما طال الطريق. لها كل الامتنان والمحبة التي تعجز الكلمات عن وصفها.

وإلى زوجتي العزيزة، رفيقة الدرب،

التي تحملت صمتي حين أغرق في التفكير، ووفرت لي المساحة عندما رأت تركيزي، وأجّلت أحاديثها رغبةً في ألا تقطعَ سلسلة أفكاري. دعمتني بصبر، وتحملت مزاجي حين أعجز عن حل مسألة، ووقفت بجانبي دون تردد، وسهرت لتُبقيني مُطعَمًا ومَرتويًا، ولم تُطلب مني شيء طوال ساعات دراستي.
لها منّي كل الامتنان، فهي أكثر مما تمنيت.

وإلى زملائي في المجلس النرويجي للاجئين (NRC) وزملائي في أوكسفام،

الذين شاركوني خبراتهم، ولم يبخلوا عليّ بمشورة أو معلومة. كانوا جزءًا من تطوري المهني، وساندوني بودّ وتعاون، فكان لهم دورٌ مباشر فيما وصلت إليه في هذا العمل.
ولمديري المباشر سرجان، الذي كان أكثر من مجرد مدير؛ كان صديقًا وداعمًا، وتحمّل تغيبي المتكرر من أجل الامتحانات والدراسة، ولم يتردد في تقديم أي تسهيل يساعدني على الاستمرار.

وإلى رفاق رحلتي في هذا الماجستير (إشراق، رغيد، رغد، نغم، أسامة، لبنى، شروق، مازن، أمجد، اليسا، كفاح، ماهر، متري، محمد، ماسة، والقائمة تطول وتطول)

الأصدقاء الذين تحولت المعرفة بهم إلى صداقة، والصداقة إلى جزء مهم من حياتي. شاركوني الواجبات والوجبات، المشاريع والمشاوير، والنقاشات والضحكات، الأفكار والذكريات، وتبادلنا الخبرات لنرفع من مستوى بعضنا البعض. فكانوا عائلةً علمية وروحية في آنٍ معًا، ووجودهم جعل الطريق أكثر جمالًا وإنسانية.
لهم أهدي هذا العمل، فهم شركاء الإنجاز، وروح هذه الرحلة.

ولأصدقائي المقرّبين (دريد، أنس، ميشيل)،

الذين كانوا دائمًا إلى جانبي، ويضيفون لرحلتي ما لا تضيفه الكتب ولا القاعات الدراسية. شاركوني المواقف والضحكات، وفتحوا لي أبوابًا من الطيبة والروح الجميلة، فكانوا السند في لحظات الإرهاق، والونس في أوقات الضغط، وعونًا صادقًا في كل خطوة من هذا الطريق. وجودهم بجانبي كان نعمة لا تُقدَّر.

الشكر والتقدير

أتقدم بخالص الشكر والامتنان لكل من أسهم في إنجاز هذا البحث ووقف إلى جانبي خلال رحلتي الأكاديمية، فقد كان لكل دعمٍ، نصيحة، أو كلمة تشجيع أثر بالغ في إخراج هذا العمل بالشكل الذي أراه اليوم.

أخص بالشكر وامتنان قلبي **الأستاذ الدكتور طلال عبود**، على صبره اللامحدود، وتوجيهاته السديدة، ووقته الثمين الذي منحني إياه في كل مرحلة من مراحل إعداد هذه الدراسة. لقد كان دعمه المستمر، وإيمانه بقدرتي على الاستمرار، وملاحظاته الدقيقة، حجر الأساس في تطور هذا العمل وتوجيهه نحو الصواب.

كما أتقدم بالشكر العميق لكل **الكادر التعليمي في المعهد العالي لإدارة الأعمال**، على ما قدموه من علم ومعرفة، وإتاحة الموارد الأكاديمية، وخلق بيئة تعليمية محفزة ساعدتني على صقل مهاراتي البحثية والنظرية. وأود أن أعبّر عن امتناني العميق **لأساتذتي في الجامعة**، الذين كان لهم الفضل الأكبر في إثراء فهمي وفتح آفاق واسعة أمامي في كافة المجالات.

ولا يفوتني أن أعبر عن تقديري لمجلس المجلس النرويجي للاجئين - سوريا على دعمه العملي وتعاون كادره، والسماح بجمع البيانات والمعلومات اللازمة لإتمام البحث من الموظفين، ولزملائي على مشاركتهم لخبراتهم العملية، مما أغنى جانب الدراسة الميدانية وجعل النتائج أكثر موثوقية وواقعية.

وأخيرًا، أقدم شكري لكل من وقف معي، من أصدقاء وزملاء ورفاق درب، الذين شاركوني أفكارهم وتجاربهم، ورفعوا من سقف طموحي، وأضفوا على رحلتي روح التعاون والإلهام.

لكم جميعًا أبعث بأسمى كلمات الشكر والامتنان، وأسأل الله أن يكون هذا البحث ثمرة طيبة لجهودكم جميعًا.

ملخص البحث

تعتبر نظم إدارة أمن المعلومات (ISMS) من الأدوات الحيوية التي تسهم في تعزيز الثقة والمصداقية داخل المنظمات الدولية، خاصة في ظل التحديات المتزايدة المتعلقة بحماية البيانات الحساسة وضمان استمرارية الأعمال. تهدف هذه الدراسة إلى استكشاف دور نظم إدارة أمن المعلومات في المجلس النرويجي للاجئين، حيث تسلط الضوء على كيفية تأثير هذه النظم على حماية المعلومات الحساسة، وزيادة الدعم المالي من المانحين، وضمان استجابة فعالة للأزمات الدولية.

تم اعتماد منهج وصفي تحليلي لجمع البيانات من خلال استبانة تم توزيعه على 32 موظفًا من مختلف الأقسام داخل المنظمة. تم تصميم الاستبانة لقياس مدى فعالية نظم إدارة أمن المعلومات في معالجة القضايا المتعلقة بأمن المعلومات، بالإضافة إلى تقييم تأثير هذه النظم على العمليات الداخلية والتواصل مع المانحين. وُجد أن استخدام نظم إدارة أمن المعلومات يؤدي إلى تحسين مستويات الأمان، مما يعكس الثقة لدى المانحين ويحفزهم على تقديم المزيد من الدعم المالي.

علاوة على ذلك، أظهرت النتائج أن نظم إدارة أمن المعلومات تسهم في تعزيز القدرات التنظيمية في مواجهة الأزمات، حيث يمكن للمنظمة ضمان استمرارية العمل واستعادة الأنشطة بشكل أسرع عند حدوث أي طارئ. هذه العوامل تؤكد أهمية إنشاء بيئة عمل آمنة وموثوقة، مما يعزز السمعة المؤسسية للمجلس النرويجي للاجئين.

بالإضافة إلى ذلك، أكدت الدراسة على ضرورة توفير التدريب المستمر للموظفين في مجال أمن المعلومات، وتوسيع نطاق تطبيق نظم إدارة أمن المعلومات ليشمل جميع جوانب العمليات، من التواصل الداخلي إلى التعامل مع البيانات الحساسة. وأوصت بضرورة الاستثمار في التقنيات الأمنية المتقدمة لتعزيز فعالية نظم إدارة أمن المعلومات، مع التركيز على تعزيز الوعي الأمني بين جميع الموظفين.

تسهم هذه الدراسة في إثراء الفهم العام حول دور نظم إدارة أمن المعلومات في المنظمات الدولية، وتقديم توصيات عملية تستهدف تحسين الثقة والمصداقية. كما تسلط الضوء على أهمية هذه النظم كأداة استراتيجية لتأمين المعلومات الحساسة وضمان استمرارية العمليات، مما يؤكد على ضرورة إدراجها ضمن الخطط الاستراتيجية للمنظمات غير الحكومية.

الكلمات المفتاحية: نظم إدارة أمن المعلومات، ISMS، حماية البيانات الحساسة، الثقة بالمنظمات الدولية، المجلس النرويجي للاجئين، استمرارية الأعمال، المنظمات غير الحكومية.

ABSTRACT

Information Security Management Systems (ISMS) are considered vital tools that contribute to strengthening trust and credibility within international organizations, especially amid increasing challenges related to protecting sensitive data and ensuring business continuity. This study aims to explore the role of ISMS within the Norwegian Refugee Council, highlighting how these systems influence the protection of sensitive information, increase financial support from donors, and ensure effective responses to international crises.

A descriptive analytical method was adopted to collect data through a questionnaire distributed to 32 employees across various departments within the organization. The questionnaire was designed to measure the effectiveness of ISMS in addressing issues related to information security, as well as to assess the impact of these systems on internal operations and communication with donors. The findings indicated that the use of ISMS leads to improved security levels, which in turn enhances donor trust and motivates them to provide additional financial support.

Furthermore, the results showed that ISMS contribute to strengthening organizational capacity in crisis situations, enabling the organization to ensure business continuity and resume activities more rapidly in the event of an emergency. These factors underscore the importance of establishing a secure and reliable work environment, thereby reinforcing the institutional reputation of the Norwegian Refugee Council.

Additionally, the study emphasized the need for continuous training for staff in the field of information security and expanding the scope of ISMS implementation to include all aspects of operations, from internal communication to managing sensitive data. It recommended investing in advanced security technologies to enhance the effectiveness of information security systems, while focusing on strengthening security awareness among all employees.

This study contributes to enriching general understanding of the role of ISMS in international organizations and offers practical recommendations aimed at improving trust and credibility. It also highlights the importance of these systems as a strategic tool for securing sensitive information and ensuring operational continuity, emphasizing the need to incorporate them into the strategic plans of non-governmental organizations.

Keywords: Information Security Management Systems, ISMS, sensitive data protection, trust in international organizations, Norwegian Refugee Council, business continuity, non-governmental organizations.

الفهرس

الإهداء: III

الشكر والتقدير: IV

ملخص البحث:..... V

Abstract VI

الفهرس:..... VII

قائمة الجداول: X

قائمة الأشكال: XI

الفصل الأول: الإطار العام للبحث..... 1

1.1 مقدمة عامة 1

1.2 مشكلة البحث..... 2

1.3 أهمية البحث..... 2

1.4 أهداف البحث 3

1.5 منهج البحث 3

1.6 نموذج البحث..... 3

1.7 فرضيات البحث 4

1.8 حدود ومحددات البحث..... 4

الفصل الثاني: الإطار النّظري 7

2.1 الدراسات السابقة 7

2.1.1 ملاحظات مستخلصة من الدراسات السابقة والتمهيد للدراسة الحالية: 10

2.1.2 ما يميز البحث الحالي عن الدراسات السابقة: 11

2.2 تعريف المنظمات الدولية:..... 12

2.3 تعريف المستفيدون:..... 13

2.4 نظم إدارة أمن المعلومات(ISMS) 13
2.4.1 تعريف نظم إدارة أمن المعلومات..... 13
2.4.2 مكونات نظم إدارة أمن المعلومات 14
2.4.3 أهداف نظم إدارة أمن المعلومات..... 15
2.4.4 أهمية نظم إدارة أمن المعلومات في المنظمات الدولية 15
2.5 حماية البيانات الحساسة 16
2.5.1 تعريف البيانات الحساسة..... 16
2.5.2 تعريف حماية البيانات..... 16
2.5.3 مكوّنات حماية البيانات 16
2.5.4 أهمية حماية البيانات في المنظمات الإنسانية 17
2.6 المانحين..... 17
2.6.1 تعريف المانحين 17
2.6.2 مفهوم الثقة والمصداقية المؤسسية لدى المانحين 17
2.6.3 عوامل بناء ثقة المانحين 18
2.6.4 العلاقة بين نظم إدارة أمن المعلومات وثقة المانحين 18
2.7 استمرارية الأعمال والقدرة على الاستجابة للأزمات في المنظمات الدوليةINGOs 18
2.7.1 تعريف مفهوم استمرارية الأعمال والقدرة على الاستجابة للأزمات 18
2.7.2 مكوّنات استمرارية الأعمال في المنظمات الإنسانية..... 19
2.7.3 أهمية استمرارية الأعمال في عملINGOS 20
2.7.4 العلاقة بين نظم إدارة أمن المعلومات واستمرارية الأعمال 21
2.7.5 دور التمويل في استمرارية الأعمال والاستجابة الإنسانية..... 22
2.8 الإطار المفاهيمي للدراسة..... 23
2.8.1 مراجعة نظرية موجزة لكل متغير (ما يدعم قياسه في الدراسة)..... 24
2.8.2 التعريفات التشغيلية للمتغيرات..... 25

الفصل الثالث: الإطار العملي.....26
3.1 لمحة عن منظمة المجلس النرويجي للاجئين 26
3.1.1 الرؤية والرسالة: 27
3.1.2 القيم الأساسية: 28
3.1.3 مجالات العمل الأساسية: 28
3.1.4 انتشار العمليات: 29
3.1.5 دور نظم إدارة أمن المعلومات في المجلس النرويجي: 29
3.2 مصادر جمع البيانات 29
3.3 مجتمع وعينة الدراسة 29
3.4 أداة الدراسة.....30
3.5 أدوات التحليل الإحصائي: 32
3.6 ثبات وصدق أداة الدراسة حساب معامل الثبات الداخلي (ألفا كرو نباخ):.....32
3.7 عرض وتحليل بيانات البحث:.....33
3.7.1 خصائص العينة: 33
3.8 التحليل الوصفي لمتغيرات الدراسة: 37
3.8.1 تفسير النتائج: 38
3.9 اختبار فرضيات البحث:.....39
3.10 نتائج البحث.....47
3.11 التوصيات 50
المراجع:.....52
الاستبانة: 54

قائمة الجداول

الجدول رقم 1: نموذج البحث 3

الجدول رقم 2: مقياس ليكرت الخماسي 31

الجدول رقم 3: أطوال الفئات 31

الجدول رقم 4: اختبار الثبات لمحاور الاستبانة 32

الجدول رقم 5: الإحصاءات الوصفية لمتغيرات الدراسة 38

الجدول رقم 6: معاملي الارتباط والتحديد لمتغيرات الفرضية الفرعية الأولى 40

الجدول رقم 7: نتائج تحليل الانحدار لمتغيرات الفرضية الفرعية الأولث 40

الجدول رقم 8: معاملات نموذج الانحدار لمتغيرات الفرضية الفرعية الأولى 41

الجدول رقم 9: معاملي الارتباط والتحديد لمتغيرات الفرضية الفرعية الثانية 42

الجدول رقم 10: نتائج تحليل الانحدار لمتغيرات الفرضية الفرعية الثانية 42

الجدول رقم 11: معاملات نموذج الانحدار لمتغيرات الفرضية الفرعية الثانية 43

الجدول رقم 12: معاملي الارتباط والتحديد لمتغيرات الفرضية الفرعية الثالثة 44

الجدول رقم 13: نتائج تحليل الانحدار لمتغيرات الفرضية الفرعية الثالثة 45

الجدول رقم 14: معاملات نموذج الانحدار لمتغيرات الفرضية الفرعية الثالثة 45

الجدول رقم 15: محور الاستبانة الأول 55

الجدول رقم 16: محور الاستبانة الثاني 56

الجدول رقم 17: محور الاستبانة الثالث 56

الجدول رقم 18: محور الاستبانة الرابع 57

قائمة الأشكال

الشكل رقم 1: الإطار المفاهيمي للدراسة.....23

الشكل رقم 2: التوزع النسبي بحسب الوظيفة 33

الشكل رقم 3 التوزع النسبي بحسب مدة العمل 34

الشكل رقم 4: التوزع النسبي بحسب التعامل السابق مع ISMS.....36

الشكل رقم 5: رمز الاستجابة السريعة (QR Code) للاستبانة 54

الفصل الأول: الإطار العام للبحث

يستعرض هذا الفصل، الخطوط العريضة لتنفيذ هذا البحث، وتعريف مشكلة البحث، أهمية البحث وأهدافه، ومحددات إنجاز البحث المكانية والزمانية وغيرها

1.1 مقدمة عامة

في ظل التطور التكنولوجي السريع وتزايد الاعتماد على الأنظمة الرقمية، أصبحت حماية المعلومات الحساسة وإدارة أمن البيانات من القضايا المحورية التي تواجه المنظمات الدولية على مستوى العالم. تعاني المنظمات الدولية من تحديات فريدة نظرًا لعملياتها المعقدة التي تمتد عبر الحدود، مما يجعلها عرضة لمخاطر سيبرانية متزايدة تهدد سمعتها واستمرارية أعمالها. بالنسبة للمنظمات الدولية التي تعمل في مجالات إنسانية مثل المجلس النرويجي للاجئين، تكون المعلومات الحساسة ذات طبيعة خاصة، فهي تشمل بيانات عن الفئات الأكثر ضعفًا كالأطفال واللاجئين، وتتعلق بإدارة الموارد والمساعدات التي تمثل شريان الحياة للكثيرين. في هذا السياق، يُعد تأمين هذه البيانات أمرًا حيويًا لضمان الثقة بين المنظمة والمستفيدين من خدماتها، بالإضافة إلى تعزيز المصداقية مع الشركاء والمانحين الدوليين.

تتزايد التهديدات السيبرانية على الصعيد العالمي، وتصبح أكثر تعقيدًا وتستهدف بشكل متزايد المنظمات الإنسانية التي تعمل في بيئات عالية المخاطر. ومن هنا تأتي أهمية نظم إدارة أمن المعلومات(ISMS) ، التي تتيح للمنظمات وضع سياسات وإجراءات لحماية معلوماتها وضمان سلامتها وسريتها. من خلال اعتماد هذه النظم، يمكن للمنظمات تحسين قدرتها على حماية البيانات، وبالتالي تعزيز الثقة لدى أصحاب المصلحة والمستفيدين من خدماتها، فضلاً عن تحسين سمعتها ومصداقيتها في المجال الإنساني.

يهدف هذا البحث إلى تحليل دور نظم إدارة أمن المعلومات (ISMS) في تحسين الثقة والمصداقية داخل المنظمات الدولية، مع التركيز على دراسة حالة المجلس النرويجي للاجئين. سيتم استكشاف كيف ساهمت هذه النظم في تعزيز أمن البيانات وحماية المعلومات الحساسة، إضافة إلى توحيد السياسات الأمنية والامتثال للمعايير الدولية. من خلال هذه الدراسة، نسعى إلى تقديم فهم أعمق لأهمية نظم إدارة أمن المعلومات في خلق بيئة موثوقة ومأمونة داخل المؤسسات الإنسانية، وكيف يمكن لهذه النظم أن تعزز مصداقية المنظمات الدولية في مواجهة التحديات الأمنية المتزايدة.

1.2 مشكلة البحث

تسعى العديد من المنظمات الدولية الي تحسين الثقة مع المستفيدين من خدماتها ومصداقيتها امام الشركاء والمانحين الدوليين لمواجهة التحديات المستمرة التي تؤثر على قدرة هذه المنظمات في الاستجابة للأزمات الدولية في أكثر البيئات تعقيدًا من خلال تطبيقها لنظم إدارة امن المعلومات، وفي ضوء ذلك تتلخص مشكلة البحث بالسؤال التالي: ما هو دور نظم إدارة أمن المعلومات (ISMS) في تحسين الثقة والمصداقية المجلس النرويجي للاجئين؟ ويتفرع عن هذا السؤال الأسئلة التالية:

1. هل يؤثر تطبيق نظم إدارة أمن المعلومات (ISMS) في حماية البيانات الحساسة داخل المجلس النرويجي للاجئين؟
2. هل يؤثر تطبيق نظم إدارة أمن المعلومات على حجم المساعدات المقدمة من المانحين للمجلس النرويجي للاجئين لتنفيذ برامجه؟
3. هل يؤثر تطبيق نظم إدارة أمن المعلومات على استمرارية العمل والقدرة على الاستجابة للأزمات الدولية عند المجلس النرويجي للاجئين؟

1.3 أهمية البحث

يأتي هذا البحث في وقت يتزايد فيه الاعتماد على الأنظمة الرقمية وتتصاعد فيه التهديدات السيبرانية، خاصة بالنسبة للمنظمات الدولية التي تعمل في بيئات معقدة مثل المجلس النرويجي للاجئين. هذه المنظمات تتعامل مع كميات هائلة من البيانات الحساسة المتعلقة بالمستفيدين من خدماتها، وتعمل على تأمين الموارد والتمويل من الشركاء والمانحين الدوليين. لذلك، فإن تأمين هذه البيانات وحماية نظم المعلومات أصبح أمرًا جوهريًا لضمان استمرارية العمل الإنساني وتعزيز الثقة والمصداقية على جميع المستويات. ومن هنا يعد هذا البحث ذا أهمية كبرى ليس فقط للمنظمات الإنسانية مثل المجلس النرويجي للاجئين، بل أيضًا لأي منظمة دولية تسعى إلى تحسين الثقة والمصداقية مع أصحاب المصلحة الرئيسيين من خلال تبني أفضل الممارسات في مجال أمن المعلومات. كما يسهم في تعزيز قدرة هذه المنظمات على مواجهة التحديات المتزايدة في بيئات العمل المعقدة، مما ينعكس إيجابًا على عملياتها وعلى المجتمعات التي تخدمها. ويأمل الباحث ان تضيف هذه الدراسة التراكم المعرفي في مجال استخدام نظم إدارة امن المعلومات في المنظمات الدولية، كما يأمل ان تكون لنتائج هذه الدراسة أهمية عملية لأصحاب القرار في المجلس النرويجي للاجئين من اجل تطوير استخدام هذه النظم.

1.4 أهداف البحث

يسعى البحث لتحقيق الأهداف التالية:

1. التعرف على نظم إدارة امن المعلومات في المجلس النرويجي للاجئين.
2. دراسة دور نظم إدارة أمن المعلومات في تحسين الثقة والمصداقية لمنظمة المجلس النرويجي للاجئين، ويتفرع عن هذا الهدف:
   a. دارسة دور نظم إدارة أمن المعلومات (ISMS) في حماية البيانات الحساسة داخل منظمة المجلس النرويجي للاجئين.
   b. دارسة دور نظم إدارة أمن المعلومات على حجم المساعدات المقدمة من المانحين للمجلس النرويجي للاجئين لتنفيذ برامجه.
   c. دارسة دور نظم إدارة أمن المعلومات على استمرارية العمل والقدرة على الاستجابة للأزمات الدولية عند المجلس النرويجي للاجئين

1.5 منهج البحث

تم استخدام المنهج الوصفي التحليلي المتضمن جمع البيانات والمعلومات المتعلقة بمتغيرات الدراسة وتحليلها باستخدام أدوات التحليل الإحصائي الملائمة (نظم إدارة امن المعلومات والثقة والمصداقية في المجلس النرويجي للاجئين)

1.6 نموذج البحث

المتغير المستقل	المتغير التابع (تحسين الثقة والمصداقية)
نظم إدارة امن المعلومات	حماية البيانات الحساسة
	حجم المساعدات المقدمة من المانحين
	استمرارية العمل والقدرة على الاستجابة للأزمات الدولية

الجدول رقم 1: نموذج البحث
المصدر: من إعداد الباحث

1.7 فرضيات البحث

استنادًا إلى مشكلة البحث وأهدافه الرئيسة ومحاوره التطبيقية، تم صياغة مجموعة من الفرضيات التي تعكس طبيعة العلاقة بين المتغير المستقل (نظم إدارة أمن المعلومات ISMS) والمتغيرات التابعة المرتبطة بعمل المجلس النرويجي للاجئين التي يمكن اختبارها بالاعتماد على البيانات التي ستوفرها أداة الدراسة (الاستبانة). وتتمثل الفرضيات فيما يلي:

الفرضية الرئيسية: يوجد دور ذو دلالة إحصائية لتطبيق نظم إدارة أمن المعلومات (ISMS) في تعزيز مستوى الثقة والمصداقية في المجلس النرويجي للاجئين.

ويندرج تحت هذه الفرضية مجموعة من الفرضيات الفرعية كما يلي:

1. الفرضية الفرعية الأولى: يوجد دور ذو دلالة إحصائية لتطبيق نظم إدارة أمن المعلومات (ISMS) في المساهمة الفعالة في حماية البيانات الحساسة داخل المجلس النرويجي للاجئين.
2. الفرضية الفرعية الثانية: يوجد دور ذو دلالة إحصائية لتطبيق نظم إدارة أمن المعلومات (ISMS) في زيادة حجم المساعدات المقدمة من المانحين للمجلس النرويجي للاجئين.
3. الفرضية الفرعية الثالثة: يوجد دور ذو دلالة إحصائية لتطبيق نظم إدارة أمن المعلومات (ISMS) في تعزيز استمرارية العمل والقدرة على الاستجابة للأزمات في المجلس النرويجي للاجئين.

1.8 حدود ومحددات البحث

تتأثر نتائج هذه الدراسة بمجموعة من الحدود والمحددات التي ارتبطت بطبيعة الموضوع وبيئة البحث ووسائل جمع البيانات، الأمر الذي يجب مراعاته عند تفسير النتائج وتعميمها. ويمكن تلخيص أبرز هذه المحددات على النحو الآتي:

أولًا: الحدود الموضوعية:

تتناول هذه الدراسة دور نظم إدارة أمن المعلومات (ISMS) في تحسين الثقة والمصداقية داخل المنظمات الدولية واقتصرت على المجلس النرويجي للاجئين فقط، مع التركيز على ثلاث متغيرات فرعية، جرى ذكرها في اهداف البحث، وبذلك تقتصر الدراسة على هذه المتغيرات الثلاثة دون التوسع في عناصر أخرى مرتبطة بأمن المعلومات. وذلك نظراً لعدم توفر البيانات وندرة المراجع المرتبطة مباشرة بهذا البحث. كما انه تم تحديد هذا النطاق الموضوعي لضمان عمق أكبر في تحليل هذه الجوانب المرتبطة مباشرة بالثقة والمصداقية، ولأن التوسع

ليشمل عناصر أخرى مثل الامتثال القانوني أو الكفاءة التشغيلية كان سيتطلب جهودًا إضافية ووقتًا أطول لا يتناسب مع الغرض الرئيسي من هذا البحث وحجم العمل المطلوب لإنجاز الرسالة او الإطار الزمني المتاح.

ثانيًا: الحدود المكانية:

اقتصرت الدراسة على المجلس النرويجي للاجئين – سوريا، حيث تم جمع البيانات من موظفين يعملون في المكاتب المحلية للمنظمة. وبالرغم من أن المجلس النرويجي يطبّق إطارًا موحّدًا لنظم إدارة أمن المعلومات وسياسات الحماية على مستوى جميع برامجه عالميًا، فإن نتائج هذه الدراسة تعكس آراء وتجارب العاملين في السياق السوري تحديدًا. وهو ما يجعلها تعبّر عن واقع التطبيق المحلي ضمن الإطار العالمي الموحد دون أن تمتد بالضرورة لقياس تجارب أو تحديات موظفي البلدان الأخرى.

ثالثًا: الحدود الزمانية:

جرى تنفيذ الدراسة في أواخر عام 2025، وتم جمع بيانات الاستبانة من العينة خلال المدة الممتدة من اول كانون الأول الى 4 كانون الأول 2025. وبذلك تعبّر النتائج عن واقع تطبيق ISMS خلال الفترة الزمنية المذكورة دون أن تمتد لتقييم مراحل تطبيق النظام في السنوات السابقة أو التغيرات المستقبلية التي قد تطرأ على سياسات أمن المعلومات أو متطلبات المانحين.

رابعًا: محددات البحث:

تتأثر نتائج هذه الدراسة بعدد من المحددات التي كانت خارج نطاق الباحث أو ارتبطت بسياق العمل الإنساني والبيئة القانونية للمجلس النرويجي للاجئين، وأهمها:

1. **محددات الخصوصية وحماية البيانات(GDPR) :**

باعتباره منظمة أوروبية، يخضع المجلس النرويجي للاجئين للائحة حماية البيانات العامة (GDPR)، التي تفرض إطارًا صارمًا لمعالجة البيانات يقوم على الشفافية، وتحديد الغرض، وتقليل البيانات، وضمان حقوق الأفراد مثل الوصول، التصحيح، المحو، والاعتراض، إضافة إلى آليات الشكاوى عبر هيئة حماية البيانات النرويجية(Datatilsynet) . ونتيجة لهذه البيئة القانونية الصارمة لم يكن من الممكن إجراء مقابلات مع المستفيدين أو الوصول إلى بيانات حساسة، لأن ذلك يتطلب موافقات رسمية معقدة تمتد عادة لأسابيع أو أشهر، وإجراءات مطوّلة تتجاوز نطاق هذه الدراسة ووقتها. لذلك اقتصرت أدوات جمع البيانات على استبانة العاملين داخل المنظمة ولم تُجرَ مقابلات مباشرة مع المستفيدين.

2. **محدودية الوصول إلى بيانات داخلية**

اقتصر جمع البيانات على الاستبانة فقط، دون القدرة على الوصول إلى وثائق تطبيق ISMS الداخلية، سجلات الحوادث الأمنية، نتيجة لسياسات حماية البيانات الخاصة بالمنظمة.

3. **محدودية الوصول إلى الشركاء والمانحين**

لم يتم جمع بيانات مباشرة من الشركاء أو المانحين نظرًا لصعوبة الوصول إلى الجهات الدولية التي تتعامل مع المجلس النرويجي للاجئين، وتعقيدات الإجراءات المطلوبة للتواصل معهم. وبذلك اقتصر تقييم "ثقة المانحين" على المؤشر المتاح، وهو حجم التمويل السنوي الممنوح للمنظمة من مختلف المانحين، دون إجراء استبيانات أو مقابلات مباشرة معهم.

4. **انتقال الباحث إلى منظمة أخرى خلال فترة البحث**

انتقالي إلى منظمة دولية أخرى خلال مرحلة إعداد الرسالة جعل الحصول على موافقات إضافية أو بيانات تفصيلية من NRC أمرًا غير ممكن. كما أن تغيير جهة الدراسة لم يكن عمليًا بسبب الوقت المتاح ولأن معظم البحث كان قد أُنجز بالفعل ضمن سياق NRC.

5. **منهج جمع البيانات**

اعتمد البحث على الاستبانة دون مقابلات نوعية أو مجموعات تركيز، مما قد يحد من عمق التحليل النوعي لتطبيقISMS .

6. **حجم العينة**

بلغ حجم العينة 32 موظفًا، وهو مناسب للسياق المحلي، ولكنه يحدّ من إمكانية التعميم على مستوى المنظمة عالميًا.

7. **محددات مرتبطة بالاختبارات الإحصائية**

استخدمت الدراسة الإحصاءات الوصفية، معامل الثبات، والمتوسطات والانحراف المعياري والانحدار الخطي البسيط، ولم تشمل اختبارات أكثر تقدمًا مثل الانحدار المتعدد او تحليل العوامل بسبب طبيعة العينة وأداة البحث.

الفصل الثاني: الإطار النّظري

يتناول هذا الفصل الأسس النظرية والمفاهيم العلمية التي يستند إليها هذا البحث ويعرض اهم الدراسات المتعلقة بموضوع البحث، ويعمل هذا الفصل على وضع الأسس العلمية التي اعتمد عليها الباحث في بناء الإشكالية وصياغة الفرضيات، وذلك من خلال تحليل المفاهيم والنظريات والمصطلحات المرتبطة بموضوع الدراسة. حيث يتناول جملة من المفاهيم والمصطلحات والنظريات المتعلقة بمتغيرات الدراسة، وهي: نظم إدارة أمن المعلومات (ISMS)، حماية البيانات الحساسة، ثقة المانحين والمصداقية المؤسسية، واستمرارية الأعمال والقدرة على الاستجابة للأزمات. كما يتم عرض العلاقات النظرية التي تربط هذه المتغيرات ببعضها وفقًا لما ورد في الأدبيات العلمية الحديثة. مع توضيح طبيعتها، مكوناتها، وأهميتها في البيئة الإنسانية والدولية، وذلك في سياق دراسة حالة المجلس النرويجي للاجئين. ويأتي هذا الفصل ليضع القارئ ضمن السياق العلمي للموضوع ويؤسس لفهم وتوجيه تحليل النتائج في الفصول اللاحقة.

2.1 الدراسات السابقة

مع ازدياد اعتماد المنظمات غير الحكومية على البيانات الرقمية والأنظمة التقنية في تنفيذ برامجها والاستجابة للأزمات، برزت أهمية تحليل التجارب والأبحاث التي تناولت حماية البيانات، وإدارة المخاطر، وبناء الثقة بين المنظمات والجهات المانحة. حيث أُنجزت العديد من الدراسات التي تناولت دور نظم إدارة أمن المعلومات داخل المنظمات الإنسانية والدولية، وحماية البيانات، وإدارة المخاطر، وبناء الثقة بين المنظمات والجهات المانحة. وفيما يلي عرض لأبرز هذه الدراسات:

1. **Humanitarian Information Management and Systems — Van de Walle, Van Den Eede & Muhren (2009)**

يعد هذا الكتاب من أوائل الأعمال الأكاديمية التي حللت إدارة المعلومات في السياقات الإنسانية، وركّز على التحديات التقنية والتنظيمية التي تواجه المنظمات عند جمع البيانات وتبادلها أثناء الأزمات.

هدف المؤلفون إلى تقديم إطار شامل لإدارة المعلومات الإنسانية، بما في ذلك الأمن، الاتساق، الحوكمة، والشفافية. كما درسوا كيفية تأثير جودة المعلومات على فعالية التنسيق بين الفاعلين الإنسانيين وعلى مستوى الثقة بين الشركاء.

استُخدم منهج تحليلي يعتمد على دراسات حالة لأزمات إنسانية سابقة، إضافة إلى مراجعة واسعة للأدبيات.

أظهرت النتائج أن المنظمات التي تمتلك بنى معلوماتية قوية وسياسات أمن معلومات واضحة تساهم في تحسين الثقة بين الشركاء والجهات الداعمة، وأن ضعف حماية البيانات يخلق نقاط فشل تؤثر على السمعة والعمليات.

2. **The Information Management Challenge: A briefing on information security for humanitarian NGOs in the field — EISF / Ed Ayre (2010)**

تُعد هذه الورقة من أوائل الإصدارات التي تناولت أهمية أمن المعلومات في المنظمات الإنسانية، حيث ركّزت على المخاطر المرتبطة بتخزين ونقل البيانات في الميدان، خصوصًا في مناطق النزاع. تهدف الورقة إلى توعية المنظمات الإنسانية بالتحديات المرتبطة بحماية البيانات والاتصال، وتقديم إرشادات عملية لتقليل المخاطر.

اتبعت الدراسة منهجًا توصيفيًا يعتمد على تحليل الخبرات الميدانية لمنظمات إنسانية متعددة. خلصت النتائج إلى أن ضعف إدارة المعلومات قد يؤدي إلى تهديد سلامة المستفيدين والموظفين، وإلى فقدان ثقة المانحين في إسناد التمويل. كما أكدت أهمية وجود سياسات واضحة لتخزين البيانات وتشفيرها ووضع ضوابط مشاركة المعلومات.

3. **Digital Risk: How New Technologies Impact Acceptance and Raise New Challenges for NGOs — Ziad Al Achkar (2021)**

تتناول هذه الدراسة المخاطر الرقمية التي تواجه المنظمات غير الحكومية نتيجة الاعتماد المتزايد على التكنولوجيا، مثل الهجمات السيبرانية، انتهاكات الخصوصية، وتضخّم حجم البيانات. تهدف الدراسة إلى فهم تأثير هذه المخاطر على قبول المنظمات داخل المجتمعات التي تعمل فيها، وكذلك على ثقة المانحين بالمنظمة وبقدرتها على حماية البيانات والالتزام بالمعايير الدولية. استخدم الباحث منهجًا وصفياً–تحليليًا مدعومًا بمقابلات مع موظفي عدد من المنظمات غير الحكومية.

توصلت الدراسة إلى أن المخاطر الرقمية أصبحت أحد العوامل المؤثرة على استدامة التمويل وعلى تقييم الجهات المانحة. كما أكدت أن غياب سياسات أمن معلومات واضحة يزيد من احتمال فقدان الثقة، بينما تطبيق إجراءات حماية قوية يعزز سمعة المنظمة ويقلل من المخاطر التشغيلية.

4. Cybersecurity Experiences and Practices in Charities — Christoffer Lindström (2022)

تركز رسالة الماجستير هذه على مستوى الوعي والممارسات الأمنية في الجمعيات الخيرية، وخاصة فيما يتعلق بحماية البيانات وتطبيق ضوابط الأمن السيبراني. وهدفت الدراسة إلى تقييم مدى استعداد الجمعيات لمواجهة التهديدات الرقمية، وقياس تأثير محدودية الموارد على فعالية أمن المعلومات.

اعتمد الباحث على منهج مختلط يجمع بين استبيانات ومقابلات مع إدارات تقنية ومجموعات عمل تطوعية في عدة منظمات خيرية أوروبية.

أظهرت النتائج أن معظم الجمعيات الخيرية تعاني من نقص في الموارد البشرية والخبرات التقنية اللازمة لحماية البيانات، وأن التهديدات السيبرانية تُعدّ عاملًا مؤثرًا في ثقة المتبرعين. كما أوصت الدراسة بضرورة تطبيق سياسات مبسّطة لأمن المعلومات وتدريب الموظفين بشكل مستمر.

5. Data Sharing Between Humanitarian Organisations and Donors — Larissa Fast (2022)

تناقش هذه الدراسة التحديات الأخلاقية والتنظيمية المتعلقة بمشاركة البيانات بين المنظمات الإنسانية والمانحين، مع التركيز على مبدأ المسؤولية والحماية.

تهدف الدراسة إلى فهم كيفية موازنة المنظمات بين ضرورة مشاركة البيانات لتعزيز الشفافية وبين الحاجة لحماية خصوصية المستفيدين.

استخدمت Fast منهجًا تحليليًا يعتمد على دراسات حالة ومراجعة سياسات للمنظمات الإنسانية الدولية.

تشير النتائج إلى أن مشاركة البيانات ترتبط بشكل وثيق بثقة المانحين، وأن المنظمات التي توضح سياساتها بخصوص أمن البيانات تحصل على مستويات أعلى من الدعم. كما تؤكد الدراسة أن المانحين باتوا يضعون معايير صارمة لحماية المعلومات كشرط أساسي للتمويل.

6. Humanitarian Technologies of Trust — J. Billaud (2023)

تبحث هذه الدراسة في كيفية تشكّل «الثقة» داخل المنظمات الإنسانية عبر استخدام التقنيات الرقمية، وخاصة تلك التي تُستخدم في إدارة المعلومات والبيانات الحساسة. تركّز الدراسة على تحليل العلاقة بين التكنولوجيا والممارسات الإنسانية اليومية، وكيف تغيّر التقنيات الحديثة من آليات التحقق، الرقابة، والشفافية داخل العمل الإنساني.

اعتمدت الباحثة على منهج كيفي قائم على الملاحظة الميدانية والمقابلات مع موظفين في منظمات دولية. وتهدف الدراسة إلى توضيح كيف تُستخدم التكنولوجيا ليس فقط لتحسين الكفاءة، بل أيضًا لتعزيز مصداقية المنظمات أمام المانحين والمجتمعات المستفيدة.

كشفت النتائج أن أدوات جمع البيانات، أنظمة الحماية، والبرمجيات التحليلية أصبحت جزءًا من «بناء الثقة» في العمل الإنساني، وأن درجة التزام المنظمة بأمن المعلومات باتت مرتبطة مباشرة بتقييم المانحين لمصداقيتها وقدرتها على إدارة التمويل بشفافية.

7. **Cybersecurity and Social Media Networks for Donations: An empirical investigation of triad of trust, commitment and loyalty — Lawson-Body et al. (2023)**

تبحث هذه الدراسة في العلاقة بين الأمن السيبراني وثقة المتبرعين عبر المنصات الرقمية، وخاصة وسائل التواصل الاجتماعي التي أصبحت قناة رئيسية لجمع التبرعات.

تهدف الدراسة إلى تحليل العوامل المؤثرة في ثقة المتبرعين، مثل الأمان، الالتزام، الشفافية، والولاء.

استخدم الباحثون منهجًا كميًا يعتمد على نماذج رياضية واستبيانات تحليلية لجمع البيانات من متبرعين عبر الإنترنت.

أظهرت النتائج أن مستوى الأمان الرقمي له تأثير مباشر على قرار التبرع وعلى ولاء المتبرعين للمنظمة.

كما بينت الدراسة أن ضعف حماية حسابات المنظمة أو تعرضها لهجمات سيبرانية يؤدي إلى تراجع سريع في الثقة وتردد الجهات المانحة في تقديم الدعم.

2.1.1 ملاحظات مستخلصة من الدراسات السابقة والتمهيد للدراسة الحالية:

أظهرت الدراسات السابقة أنّ أمن المعلومات وإدارة البيانات في المنظمات الإنسانية تعدّان عنصرين أساسيين في تعزيز موثوقية العمل الميداني وفي دعم اتخاذ القرار داخل المؤسسات الدولية. فقد ركزت معظم الدراسات على إبراز أهمية حماية البيانات الحساسة، وتأثير المخاطر الرقمية على قبول المنظمات في البيئات الإنسانية، ودور الممارسات السيبرانية السليمة في تحسين ثقة الأطراف المعنية. كما بينت الأبحاث التي تناولت التجارب التشغيلية للمنظمات الإنسانية والجمعيات الخيرية أنّ ضعف البنية الأمنية أو غياب سياسات واضحة لإدارة المعلومات يؤديان إلى تراجع الكفاءة التشغيلية وزيادة احتمالات الفجوات الأمنية، بينما ترتبط الممارسات الجيدة في الأمن السيبراني بمستوى أعلى من الثقة العامة. بالإضافة إلى ذلك، أشارت بعض الدراسات الحديثة إلى العلاقة بين الأمان الرقمي وثقة المانحين، وإن كان ذلك بصورة غير مباشرة أو من خلال تحليل سلوك المانحين عبر المنصات الرقمية.

وتتقاطع هذه النتائج مع موضوع البحث الحالي في عدة جوانب، أبرزها التأكيد على دور أمن المعلومات في بناء الثقة وتحسين الأداء المؤسسي في المنظمات الإنسانية. كما تتشابه الدراسات السابقة مع البحث الحالي في تناولها لقضايا حماية البيانات، وإدارة المخاطر الرقمية، وتأثير البيئة التقنية على سمعة المؤسسات العاملة في المجال الإنساني. ومع ذلك، فإنها غالبًا ما تطرقت لتلك الموضوعات بشكل عام أو ضمن إطار تحليلي واسع، دون الربط الصريح بين تطبيق نظم إدارة أمن المعلومات وبين مستوى ثقة المانحين وحجم التمويل، وهو ما يتناوله البحث الحالي بصورة أكثر تحديدًا وعمقًا.

واتفقت معظم هذه الدراسات على أن الامتثال للمعايير والممارسات الأمنية المعترف بها دولياً يُعد عاملاً محورياً في زيادة مصداقية المنظمة أمام شركائها وداعميها. كما اعتمدت غالبية هذه الأبحاث على أدوات منهجية مثل الاستبانة أو المقابلات لقياس أثر تطبيق هذه النظم، الأمر الذي يُتيح الاستفادة منها في صياغة أسئلة الاستبانة للبحث الحالي وتوجيه بنائه بالشكل الأمثل. ومن هذا المنطلق، تأتي الدراسة الحالية لتسهم في تعميق الفهم المتعلق بدور نظم إدارة أمن المعلومات في تعزيز الثقة والموثوقية في منظمة دولية كالمجلس النرويجي، بما يقدّم إضافة نوعية إلى الأدبيات المتوفرة.

2.1.2 ما يميز البحث الحالي عن الدراسات السابقة:

تتميز هذه الدراسة بتركيزها المباشر على المجلس النرويجي للاجئين بوصفه نموذجًا تطبيقيًا لتحليل دور نظم إدارة أمن المعلومات في السياق الإنساني، بخلاف معظم الأدبيات السابقة التي تناولت الموضوع بصورة عامة أو نظرية. وتنفرد الدراسة بربطها بين تطبيق ISMS وبين مستوى ثقة المانحين وحجم التمويل المقدم للمنظمة، وهي علاقة لم تحظَ بتناول واضح في الدراسات السابقة. كما تسلط الضوء على تأثير أمن المعلومات في تعزيز استمرارية العمل والقدرة على الاستجابة للأزمات داخل منظمة إنسانية فاعلة، مستندة إلى منهج وصفي تحليلي يعتمد على بيانات ميدانية مباشرة من داخل المنظمة. وتقدم الدراسة كذلك توصيات عملية مبنية على نتائج واقعية، مما يجعلها إضافة نوعية تسد فجوة معرفية في الأدبيات المتعلقة بأمن المعلومات في المنظمات الإنسانية.

2.2 تعريف المنظمات الدولية:

تُعرَّف المنظمات الدولية (International Organizations) بأنها كيانات مؤسسية تنشأ بموجب اتفاق دولي بين دولتين أو أكثر، وتمتلك شخصية قانونية مستقلة تخوّلها تنفيذ أنشطة متعددة على المستوى الدولي، سواء في المجالات السياسية، أو التنموية، أو الاقتصادية، أو الإنسانية. وتتميز المنظمات الدولية بهياكل تنظيمية وإدارية واضحة ومستقلة، وتمويل خارجي، ومعايير دولية تُنظّم عملها. وتشمل هذه المنظمات كل من الهيئات الحكومية الدولية (IGOs) والمنظمات الدولية غير الحكومية.(INGOs)

أما المنظمات الدولية غير الحكومية (International Non-Governmental Organizations – INGOs) فهي منظمات مستقلة لا تنشأ بموجب اتفاقيات حكومية، وإنما تؤسَّس من قبل جهات غير حكومية بهدف تنفيذ برامج إنسانية أو تنموية أو حقوقية عبر عدة دول. وتمتاز INGOs بانتشارها الواسع، واعتمادها الكبير على التمويل الدولي، وتعامُلها المكثف مع البيانات الحساسة، مما يجعل أمن المعلومات وحماية البيانات عنصرين أساسيين في عملها وشرطًا لثقة المانحين والمستفيدين على حدٍ سواء. (Van de Walle, Van Den Eede, & Muhren, 2009; NRC, 2020; Billaud, 2023) ، وتتميز INGOs بأنها:

- تتمتع باستقلال إداري ومالي عن الحكومات.
- تعتمد في تمويلها على المانحين الدوليين، الحكومات المانحة، والمؤسسات الدولية.
- تعمل في عدة بلدان، وفق سياسات، وإجراءات موحدة، ومركزية.
- تلتزم بمعايير دولية لحماية البيانات، أمن المعلومات، المساءلة والشفافية.
- تُعد الجهات الأكثر تعاملًا مع البيانات الحساسة للفئات المتضررة في سياقات الأزمات.

ومن أبرز الأمثلة على المنظمات الدولية غير الحكومية: NRC, IRC, Oxfam, Save the Children, Mercy Corps وغيرها من المنظمات العاملة في البيئات الإنسانية المعقدة.

وتُعد INGOs محورًا بالغ الأهمية في دراسات أمن المعلومات نظرًا لاعتمادها المكثف على البيانات الحساسة للمستفيدين، وارتباط مستوى امتثالها الأمني مباشرة بثقة المانحين والشركاء.

وفي سياق هذا البحث، فإن المقصود بمصطلح "المنظمات الدولية" هو تحديدًا المنظمات الدولية غير الحكومية(INGOs) ، كون المجلس النرويجي للاجئين (NRC) يمثل نموذجًا لهذه الفئة، ولأن طبيعة الدراسة ومشكلتها وأهدافها تتمحور حول دور نظم إدارة أمن المعلومات في المنظمات الإنسانية العاملة خارج الأطر الحكومية.

2.3 تعريف المستفيدون:

هم الأفراد أو الجماعات أو المجتمعات التي تتلقّى خدمات أو مساعدات أو تدخّلات مباشرة من منظّمات الإغاثة والتنمية (INGOs) ضمن برامجها الإنسانية أو التنموية. وتتضمن فئة المستفيدين اللاجئين والنازحين والناجين من الكوارث، والأسر الضعيفة، والمجتمعات المحلية المتضررة، وغيرهم ممن تُقدَّم لهم خدمات مثل الغذاء، المأوى، الحماية، الصحة، التعليم، والمساعدات النقدية. وتُعد بيانات هؤلاء الأفراد غالبًا حساسة بطبيعتها، لأن كشفها قد يؤدي إلى أذى شخصي أو اجتماعي أو أمني لهم.

(NRC, 2020; Ayre, 2010; Fast, 2022; Billaud, 2023)

في ضوء ذلك، تُعد حماية بيانات المستفيدين أحد المبررات المركزية لتبني نظم إدارة أمن المعلومات (ISMS) في المنظمات الدولية غير الحكومية.

في هذه الدراسة يُقصد بالمستفيدين :الأشخاص أو الأسر الذين تقع عليهم تأثير برامج المجلس النرويجي للاجئين في مواقع العمليات المعنية (أي المستفيدون المباشرون من خدمات NRC داخل نطاق الدراسة)، وتشمل الفئات المستهدفة بالبرامج الميدانية المسجلة لدى قواعد بيانات NRC.

2.4 نظم إدارة أمن المعلومات(ISMS)

2.4.1 تعريف نظم إدارة أمن المعلومات

تُعرّف نظم إدارة أمن المعلومات بأنها إطار متكامل من السياسات والإجراءات الهادفة إلى حماية المعلومات وضمان سريتها وسلامتها وتوافرها .(ISO, 2013) كما يرى (Whitman & Mattord, 2017) أن هذه النظم تمثل حجر الأساس في إدارة المخاطر المعلوماتية، بينما يؤكد (Dhillon, 2007) دورها في تحقيق التوازن بين الأمان والكفاءة التشغيلية.

وبناء عليه يُعرَّف الباحث نظام إدارة أمن المعلومات (Information Security Management System – ISMS) بأنه إطار عمل شامل ومتكامل يتكون من سياسات وإجراءات ومعايير وضوابط تقنية وتنظيمية، يهدف إلى حماية أصول المعلومات داخل المنظمة وضمان سريتها، وسلامتها، وتوافرها. ويُعد ISMS نظامًا إداريًا استراتيجيًا يعتمد على منهجية إدارة المخاطر كأساس في تحديد التهديدات المحتملة للمعلومات، وتحليل تأثيرها، ووضع الضوابط المناسبة لمعالجتها، بما يضمن استمرارية الأعمال والحد من الخسائر المحتملة.

ولا يقتصر دور ISMS على الجوانب التقنية فقط، بل يشمل أيضًا البعد البشري والتنظيمي للمنظمة؛ فهو يوفّر إطارًا شاملًا يساعد المؤسسات على بناء ثقافة أمن معلومات بين الموظفين، من خلال برامج التدريب، الوعي

الأمني، تحديد الصلاحيات، وتطبيق ممارسات ضوابط الوصول وإدارة الهويات، إضافة إلى تطوير خطط الاستجابة للحوادث الأمنية وخطط التعافي من الكوارث.

كما يُعد ISMS عنصرًا جوهريًا في الحوكمة المؤسسية، إذ يمكّن المنظمات من الالتزام بالمعايير والسياسات الدولية، ويُعزّز ثقة الجهات المانحة والشركاء من خلال إثبات قدرة المنظمة على إدارة بياناتها بشكل مسؤول.

وبسبب الطبيعة الحساسة للبيانات التي تتعامل معها المنظمات الإنسانية—مثل بيانات المستفيدين والمانحين وبيانات العمليات—أصبح ISMS ضرورة تشغيلية وقانونية وأخلاقية لا يمكن الاستغناء عنها. وتؤكد الأدبيات الحديثة أنّ تطبيق ISMS يُسهم في الحد من المخاطر الرقمية، وتحسين جودة الخدمات، وتعزيز القدرة على الاستجابة للأزمات، وتوفير بيئة حماية قوية للمعلومات عبر دورة حياتها كاملة، بدءًا من جمعها وتخزينها ومعالجتها وصولًا إلى أرشفتها أو إتلافها.

2.4.2 مكونات نظم إدارة أمن المعلومات

تتفق الأدبيات الحديثة في الحقل العلمي لأمن المعلومات على أن نظم إدارة أمن المعلومات يتكون عادة من العناصر التالية:

1. السياسات الأمنية:

وهي الوثائق التي تحدد توجه المنظمة العام تجاه أمن المعلومات، وتشكل المرجع الرئيسي لسلوك الموظفين في التعامل مع البيانات.

2. إدارة المخاطر:

وتشمل تحديد المخاطر المحتملة، تحليل احتمالية وقوعها وتأثيرها، ومن ثم وضع ضوابط لمعالجتها أو الحد منها.

3. الضوابط التقنية والأمنية:

مثل إدارة صلاحيات الوصول، التشفير، أنظمة كشف التهديدات، النسخ الاحتياطية، والجدران النارية.

4. الوعي والتدريب الأمني:

أحد أهم عناصرISMS ، ويهدف إلى تعزيز ثقافة أمن المعلومات بين الموظفين لضمان الالتزام بالسياسات على أرض الواقع.

5. الاستجابة للحوادث والتعافي:

أطر وإجراءات للتعامل مع أي خرق أو حادث أمني، بهدف الحد من أثره واستعادة الأنظمة بسرعة.

(ISO, 2013; Humphreys, 2008)

2.4.3 أهداف نظم إدارة أمن المعلومات

ترتكز الأهداف الرئيسة لنظم إدارة أمن المعلومات على ما يلي:

1. حماية المعلومات من الوصول غير المصرح به.
2. ضمان صحة وسلامة البيانات من التعديل أو الفقدان.
3. تعزيز موثوقية الأنظمة والخدمات.
4. دعم الامتثال للقوانين الدولية مثل GDPR - General Data Protection Regulation
5. تمكين المنظمات من مواجهة الحوادث الأمنية والاستمرار في تقديم الخدمات.

(ISO, 2013; Dhillon, 2007; Gerber & Von Solms, 2005)

2.4.4 أهمية نظم إدارة أمن المعلومات في المنظمات الدولية

تكتسب نظم إدارة أمن المعلومات أهمية متزايدة في المنظمات الدولية، ولا سيما تلك العاملة في القطاعات الإنسانية والتنموية، نظرًا لتعاملها مع كمٍّ هائل من البيانات الحساسة المتعلقة بالمستفيدين والموظفين والبرامج التشغيلية وسلاسل التوريد والجهات المانحة (Ayre, 2010). وتواجه هذه المنظمات اليوم بيئة رقمية معقدة تتسم بتزايد التهديدات السيبرانية، وتنوع الجهات الفاعلة، واستخدام التقنيات المتقدمة في الهجمات (Al Achkar, 2021) ، إضافة إلى طبيعة العمل متعدد البلدان الذي يفرض تفاوتًا في البنى التحتية والأنظمة القانونية (Lindström, 2022). لذلك أصبح وجود ISMS ضرورة استراتيجية وليست خيارًا تقنيًا فقط. وتشير الدراسات إلى أن ISMS يرتبط مباشرة بسمعة المنظمة وبثقة الجهات الممولة (Billaud, 2023)، إضافة إلى دوره المحوري في ضمان استمرارية الخدمات الإنسانية خلال الأزمات.

كما تشير الدراسات السابقة إلى أن المنظمات التي تعتمد ISMS فعال ترى:

- انخفاضًا في الحوادث الأمنية.
- زيادة في ثقة المانحين.
- تحسنًا في استمرارية الأعمال والجاهزية التشغيلية.

2.5 حماية البيانات الحساسة

2.5.1 تعريف البيانات الحساسة

البيانات الحساسة هي أي معلومات يمكن أن يتسبب كشفها أو إساءة استخدامها في إلحاق ضرر بالأفراد أو الجماعات، وتشمل البيانات الشخصية، معلومات الهوية، البيانات البيو مترية، بيانات الحماية، بيانات الحالات الإنسانية، معلومات المواقع، والسجلات التشغيلية. وفي السياق الإنساني، غالبًا ما تكون هذه البيانات ذات طبيعة حساسة للغاية نظرًا لأنها تخص أشخاصًا متضررين من النزاعات أو الأزمات، ما يجعل مسؤولية حمايتها ذات أهمية قانونية وأخلاقية مضاعفة. (Ayre, 2010; Fast, 2022; Billaud, 2023)

2.5.2 تعريف حماية البيانات

تشير حماية البيانات (Data Protection) إلى مجموعة التدابير الفنية والتنظيمية التي تهدف إلى منع الوصول غير المصرح به إلى المعلومات الحساسة، أو استخدامها، أو تعديلها، أو الإفصاح عنها بطريقة غير قانونية أو غير آمنة (Pfleeger& Pfleeger, 2012). وتشمل هذه التدابير سياسات الخصوصية، ضوابط الوصول، التشفير، إدارة دورة حياة البيانات، وضمان أمن الأنظمة والبنية التحتية التي تُحفظ فيها هذه البيانات (ISO, 2013).

وتُعد البيانات الحساسة من أكثر أنواع البيانات عرضة للمخاطر، خاصةً في المنظمات الإنسانية التي تتعامل مع فئات ضعيفة، مثل النازحين واللاجئين والمجتمعات المتضررة من النزاعات. حيث يشير (Whitman & Mattord, 2017) إلى أن حماية البيانات تمثل عنصرًا حاسمًا في استمرارية الأعمال. ولذلك فإن حماية البيانات لا تُعد مجرد ضرورة تقنية، بل هي التزام قانوني وأخلاقي وإنساني.

2.5.3 مكوّنات حماية البيانات

تعمل المنظمات عادةً على حماية بياناتها عبر مجموعة من العناصر الأساسية (Al Achkar, 2021)، من أبرزها:

1. سياسات حماية الخصوصية: وتحدد كيفية جمع البيانات ومعالجتها وتخزينها ومشاركتها ومسؤوليات القائمين عليها.
2. التحكم في الوصول: ويضمن أن البيانات لا يمكن الوصول إليها إلا من قبل الأشخاص المخوّلين.
3. التشفير: سواء في أثناء النقل أو التخزين، لضمان عدم القدرة على قراءة البيانات حتى في حال حصول خرق.
4. إدارة الموافقات والحقوق: كحق الوصول، التصحيح، الحذف، والاعتراض على المعالجة.
5. خطط الاستجابة للحوادث المتعلقة بالبيانات: والتي تشمل الإبلاغ، التحقيق، وتقليل الضرر.

2.5.4 أهمية حماية البيانات في المنظمات الإنسانية

تعد حماية البيانات عاملًا أساسيًا لبناء الثقة مع المستفيدين والمانحين على حد سواء. فالمعلومات التي تمتلكها المنظمات الإنسانية غالبًا ما تكون شديدة الحساسية، وقد يتسبب تسريبها في أذى مباشر للأفراد أو المجتمعات، إضافة إلى الأثر السلبي على سمعة المنظمة ومصداقيتها.

وتشير الدراسات السابقة إلى أن المنظمات التي تطبق سياسات قوية لحماية البيانات تتمتع بمستويات أعلى من ثقة المانحين، وتحظى بتمويل أكبر، وتتمكن من المحافظة على استمرارية أعمالها خلال الأزمات.
(Ayre, 2010; Billaud, 2023; Lindström, 2022; Fast, 2022)

2.6 المانحين

2.6.1 تعريف المانحين

المانحون هم الجهات التي تقدم التمويل، أو الدعم المادي، أو اللوجستي، أو التقني للمنظمات الدولية بهدف تمكينها من تنفيذ برامجها الإنسانية والتنموية. وقد يكون المانحون دولًا، مؤسسات حكومية، اتحادات دولية، منظمات تمويل، أو جهات خاصة مثل المؤسسات غير الربحية. وتستند العلاقة بين المانحين والمنظمة إلى مستوى الثقة والمصداقية، ويُعد الامتثال لأمن المعلومات وحماية البيانات أحد أهم عوامل تعزيز هذه الثقة في الوقت الحالي. (Fast, 2022; Lawson-Body et al., 2023; Billaud, 2023)

2.6.2 مفهوم الثقة والمصداقية المؤسسية لدى المانحين

تعتمد العلاقة بين المنظمات الإنسانية والمانحين على مستوى عالٍ من الثقة والشفافية .(Fast, 2022) كما توصلت دراسة (Lawson-Body et al., 2023) إلى أن الثقة الرقمية تلعب دورًا محوريًا في قرارات التمويل، في حين يرى (Billaud, 2023) أن أمن المعلومات أصبح أحد المحددات الأساسية لهذه الثقة.

و عليه يعرف الباحث ثقة المانحين بأنها مستوى يقين الجهات المانحة تجاه قدرة المنظمة على إدارة موارده بشكل مسؤول وشفاف، وقدرتها على حماية البيانات والمعلومات التي تقدم اليها أو تتفاعل معها من خلال العمليات. وتمثل الثقة أحد المعايير الأساسية التي يُبنى عليها قرار تقديم التمويل أو زيادته.

اما المصداقية المؤسسية فهي قدرة المنظمة على إظهار المهنية والشفافية والالتزام بالمعايير الدولية في عملها، مما يعزز ثقة الأطراف الخارجية بها. وتشمل المصداقية جودة التقارير، سلامة الإجراءات، كفاءة الإدارة، والاستقرار التشغيلي. وتُعتبر حماية البيانات وأمن المعلومات من العناصر الأساسية التي تسهم في بناء المصداقية لدى المانحين.

2.6.3 عوامل بناء ثقة المانحين

تشير الدراسات السابقة (Fast, 2022; Lawson-Body et al., 2023; Al Achkar, 2021; Billaud, 2023) إلى أن ثقة المانحين تتأثر بشكل مباشر في:

- الشفافية المالية: مدى قدرة المنظمة على تقديم تقارير مالية وتشغيلية واضحة وقابلة للتتبع.
- الامتثال للمعايير الدولية: مثل سياسات حماية البيانات، مدونات السلوك، والحوكمة المؤسسية.
- أمن المعلومات وحماية البيانات: إذ يعتبر المانحون أي خلل في الأمن السيبراني مؤشرًا على ضعف القدرات.
- جودة إدارة المخاطر: وقدرة المنظمة على التعامل مع الأزمات والتهديدات.
- النتائج والأثر الميداني: مدى نجاح البرامج في تحقيق أهدافها وتأثيرها على المستفيدين.

2.6.4 العلاقة بين نظم إدارة أمن المعلومات وثقة المانحين

أظهرت الدراسات السابقة (Fast, 2022; Lawson-Body et al., 2023; Billaud, 2023; Al Achkar, 2021) أن المانحين ينظرون إلى أمن المعلومات كمؤشر على نضج المنظمة وقدرتها على حماية المستفيدين والتمويلات. كما دلت على وجود علاقة طردية قوية بين نظام إدارة أمن المعلومات وثقة المانحين، إذ يعكس ISMSقدرة المنظمة على حماية البيانات وحسن إدارتها للموارد، مما يزيد من مصداقيتها ويعزز صورتها المهنية. وتشير العديد من الدراسات إلى أن المانحين يطلبون اليوم مستويات أعلى من الامتثال الأمني، ويعتبرون أمن المعلومات شرطًا أساسيًا للتمويل.

2.7 استمرارية الأعمال والقدرة على الاستجابة للأزمات في المنظمات الدولية INGOs

2.7.1 تعريف مفهوم استمرارية الأعمال والقدرة على الاستجابة للأزمات

تُعرَّف استمرارية الأعمال في المنظمات الدولية غير الحكومية (INGOs) بأنها قدرة المنظمة على ضمان استدامة عملياتها وبرامجها الإنسانية دون انقطاع، من خلال المحافظة على تدفق الموارد المالية وتوافر البنية التشغيلية اللازمة لتقديم الخدمات للمستفيدين، حتى في ظلّ الأزمات (Gerber & Von Solms, 2005). ويشمل ذلك قدرة المنظمة على الحصول على التمويل الكافي وفي الوقت المناسب لضمان عدم توقف برامجها الأساسية، وتحقيق استجابة فعّالة لحاجات الفئات المتضررة.

أما القدرة على الاستجابة للأزمات فتشير إلى مدى استعداد المنظمة للتحرك السريع عند وقوع كوارث طبيعية، نزاعات، أزمات إنسانية مفاجئة أو أزمات لوجستية وتشغيلية، وذلك عبر تفعيل آليات داخلية وخطط طوارئ وبرامج جاهزة تُمكّنها من تعبئة التمويل بسرعة، نشر فرق ميدانية، وإطلاق تدخلات إنسانية ضمن أطر زمنية حرجة (Humphreys, 2008).

وتتجلى أهمية هذا المفهوم لدى ال INGOs في:

- قدرتها على الوصول السريع للتمويل الإنساني من خلال الثقة التي يمنحها المانحون، وهو عنصر محوري في عمل المنظمات الإنسانية.
- استمرار خدماتها الأساسية (مثل التعليم، الحماية، المساعدات النقدية، المياه والإصحاح، المأوى...) دون انقطاع رغم التحديات.
- التكيف مع الأزمات العالمية كالنزاعات واسعة النطاق أو الكوارث الطبيعية، مع المحافظة على الحد الأدنى من الكفاءة التشغيلية.
- تعزيز جاهزيتها التشغيلية عبر خطط واضحة لإدارة المخاطر والحوادث وضمان استمرار البرامج. (Van de Walle et al., 2009)

وفي سياق الدراسة الحالية، يرتبط مفهوم استمرارية الأعمال والقدرة على الاستجابة للأزمات بشكل مباشر بـ نظم إدارة أمن المعلومات(ISMS) ، حيث تؤثر قوة النظام الأمني على قدرة المنظمة في حماية البيانات، الامتثال لمتطلبات المانحين، والحصول السريع على التمويل اللازم لاستمرار عملياتها واستجابتها الفعّالة للأزمات.

2.7.2 مكوّنات استمرارية الأعمال في المنظمات الإنسانية

تعتمد INGOs في الحفاظ على استمراريتها على مجموعة من العناصر الجوهرية، أبرزها:

1. توفر التمويل واستدامته:

يشكّل التمويل المستمر والسريع أساسًا لاستمرارية برامج المنظمات، وخاصة في حالات الطوارئ. وتعتمد سرعة الاستجابة على قدرة المنظمة على ضمان تدفق التمويل المخصص للبرامج ولتغطية الاحتياجات التشغيلية.

2. خطط الطوارئ التشغيلية:

وتشمل سيناريوهات واضحة للتعامل مع الأزمات، تحديد فرق التدخل السريع، وتفعيل إجراءات ميدانية عاجلة.

3. إدارة المخاطر المؤسسية:

تحديد المخاطر المحتملة—سواء كانت أمنية أو تشغيلية أو مالية—ووضع إجراءات للتعامل معها.

4. الموارد البشرية المؤهلة:

فرق مدرّبة على العمل في الطوارئ وعلى إدارة الأزمات.

(Gerber & Von Solms, 2005; Humphreys, 2008; ISO, 2013; Whitman & Mattord, 2017)

2.7.3 أهمية استمرارية الأعمال في عمل INGOs

تحظى استمرارية الأعمال بأهمية خاصة في بيئة العمل الإنساني للأسباب التالية:

1. ضمان استمرار الخدمات الأساسية:

مثل الغذاء، المأوى، التعليم، المياه والإصحاح، والمساعدات النقدية، والتي يعتمد عليها المتضررون في تلبية احتياجاتهم الحيوية.

2. تعزيز ثقة المانحين واستمرار التمويل:

المنظمات التي تظهر قدرة على مواصلة عملها بفعالية تحظى بتجديد التمويل وزيادته، إذ يُنظر إليها كجهات موثوقة وقادرة على إدارة الموارد بكفاءة.

3. تقليل الفجوات التشغيلية والخسائر الإنسانية:

أي توقف في البرامج قد يؤدي إلى فجوات حرجة في الاستجابة، ما قد ينعكس سلبًا على حياة المستفيدين.

4. تعزيز الجاهزية المؤسسية:

الاستمرارية ليست مجرد خطة طوارئ بل ثقافة مؤسسية تتعلق بالتخطيط، التنبؤ بالمخاطر، وتوزيع المسؤوليات.

5. مواءمة عمل المنظمة مع متطلبات المانحين:

تفرض كثير من الجهات المانحة سياسات صارمة لضمان استمرارية الخدمات، وربط التمويل بقدرة المنظمة على الاستجابة الفعّالة.

(Ayre, 2010; NRC, 2020; Billaud, 2023; World Economic Forum, 2021)

2.7.4 العلاقة بين نظم إدارة أمن المعلومات واستمرارية الأعمال

تسهم نظم إدارة أمن المعلومات بشكل مباشر في تعزيز استمرارية الأعمال من خلال تقليل المخاطر وتحسين الاستجابة للحوادث .(ISO, 2013) كما يرى (Gerber & Von Solms, 2005) أن الإدارة الفعالة للمخاطر المعلوماتية تدعم استقرار العمليات، وهو ما يتقاطع مع ما أشار إليه(Humphreys, 2008) . لذلك يرى الباحث ان نظم إدارة أمن المعلومات (ISMS) تلعب دورًا محوريًا في تعزيز استمرارية الأعمال والقدرة على الاستجابة للأزمات، وذلك من خلال:

1. ضمان توافر البيانات وعدم انقطاع الخدمات الرقمية:

وجود بنية أمنية قوية يقلل من احتمالية توقف الأنظمة نتيجة هجمات سيبرانية أو تسريب بيانات.

2. تعزيز ثقة المانحين وبالتالي ضمان استمرار التمويل:

المنظمات التي تُظهر التزامًا قويًا بأمن المعلومات غالبًا ما تحصل على تسهيلات مالية واستجابة أسرع من المانحين.

3. دعم استجابة المنظمة للأزمات:

إذ يضمن ISMS حماية الأنظمة الأساسية التي تعتمد عليها التدخلات الإنسانية، مثل قواعد بيانات المستفيدين وأنظمة التوزيع.

4. تحسين قدرة المنظمة على التعافي بعد الحوادث:

من خلال وجود إجراءات واضحة للنسخ الاحتياطي، استعادة البيانات، وإدارة الحوادث الأمنية.

وتشير الدراسات السابقة إلى أن المنظمات التي تطبق ISMS بشكل فعّال تكون أكثر قدرة على الاستجابة للأزمات، وتحافظ على خدماتها دون انقطاع، خصوصًا في البيئات الإنسانية المعقدة.

2.7.5 دور التمويل في استمرارية الأعمال والاستجابة الإنسانية

يتسم التمويل في INGOs بأنه العامل الأبرز في استمرار عملياتها، ويؤثر بشكل مباشر في:

- سرعة إطلاق برامج الطوارئ.
- حجم التدخلات وقدرة المنظمة على التوسع.
- الاحتفاظ بالكادر المؤهل.
- القدرة على الاستجابة المستدامة طويلة الأمد.

وترتبط سرعة التمويل وثباته بمستوى امتثال المنظمة لمعايير أمن المعلومات، إذ بحسب الدراسات السابقة تقيّم الجهات المانحة التزام المنظمات بحماية البيانات قبل ضخ التمويل.

(Fast, 2022; Lawson-Body et al., 2023; NRC, 2020; Billaud, 2023)

2.8 الإطار المفاهيمي للدراسة

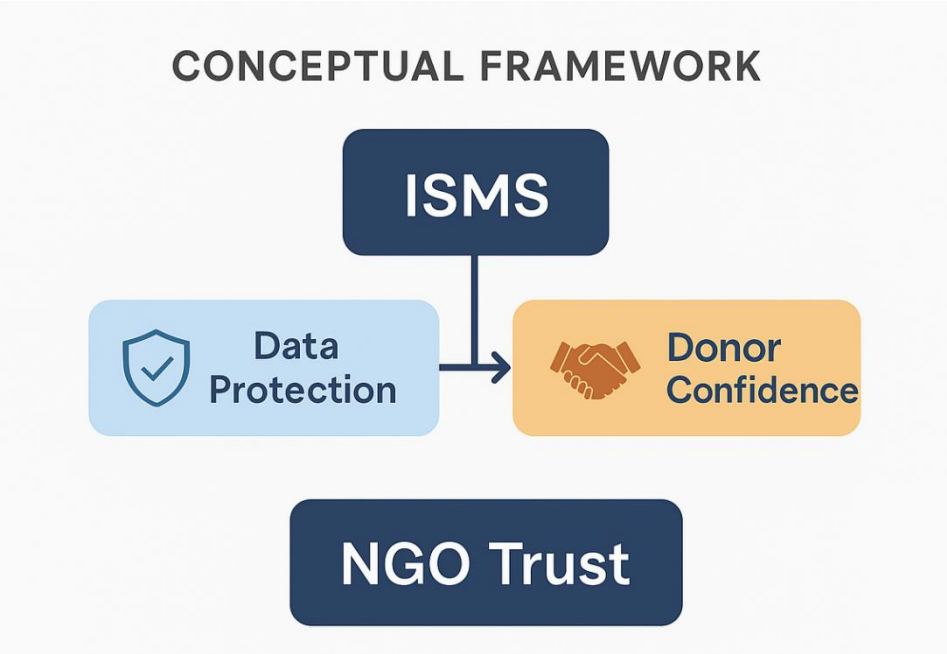
يعتمد الإطار المفاهيمي لهذه الدراسة على نموذج سببي بسيط يوضّح دور المتغير المستقل (واقع تطبيق نظم إدارة أمن المعلومات ISMS) في التأثير على ثلاث متغيرات تابعة:

1. حماية البيانات الحساسة
2. ثقة المانحين / حجم المساعدات
3. استمرارية العمل والقدرة على الاستجابة للأزمات.

هذا الإطار مستمدّ من الجمع بين نتائج الدراسات السابقة ونطاق البحث العملي. حيث سيتم اختبار هذه العلاقات في الفصل العملي

نظم إدارة أمن المعلومات ← (حماية البيانات، ثقة المانحين، استمرارية الأعمال)

وكل من هذه المتغيرات قد يكون له دور متبادل على مستوى الأداء المؤسسي والتمويل، لكن هذه الدراسة اختُبرت الدور المباشر لـ ISMS على كل متغير تابع على حدة.



الشكل رقم 1: الإطار المفاهيمي للدراسة
المصدر: من إعداد الباحث لغرض التوضيح

2.8.1 مراجعة نظرية موجزة لكل متغير (ما يدعم قياسه في الدراسة)

1. ما يدعم قياس واقع تطبيق ISMS

تُركّز الدراسات السابقة على عناصر يمكن قياسها لقياس واقع ISMS، مثل: وجود سياسة أمنية رسمية، تخصيص الموارد، وجود دور مسؤول عن أمن المعلومات، برامج تدريب، وتوافر ضوابط تقنية مثل إدارة الوصول والتشفير وأنظمة المراقبة. اعتمدت أداة الدراسة (الاستبانة) على قياسات مماثلة استنادًا إلى الممارسات الموصى بها في الدراسات السابقة.

2. ما يدعم قياس حماية البيانات الحساسة

تشير الدراسات السابقة إلى مجموعة من السلوكيات والنتائج التي تدل على فاعلية الحماية: التزام الموظفين بتعليمات حماية البيانات، قلة الحوادث/التسريبات، وجود ضوابط للوصول للبيانات، وجود إجراءات للتعامل مع الحوادث. هذه المؤشرات شُكّلت على هيئة عبارات ليكرت في الاستبانة.

3. ما يدعم قياس ثقة المانحين / حجم المساعدات

استخدم في الدراسات السابقة مؤشرات متنوعة لقياس الثقة: مؤشرات تصادفية (تحليل سلوك المانحين عبر المنصات الرقمية مثل زيادة التمويل)، مؤشرات إدراكية (مستوى الثقة المبلغ عنه)، ومؤشرات التزاميه (طلب أدلة امتثال أو متطلبات أمنية من المانحين). في هذه الدراسة اقتصر التقييم العملي على مقياسٍ مبني على تصور الموظفين لتأثير ISMS على ثقة المانحين وتأكيده عبر ملاحظة اتجاهات حجم التمويل المتاح.

4. ما يدعم قياس استمرارية الأعمال والقدرة على الاستجابة للأزمات

المنهجيات في الدراسات السابقة تربط وجود عناصر التخطيط لاستمرارية الأعمال واستعداد فرق التكنولوجيا والعمليات بتقليل زمن الاسترجاع بعد حادث. لذلك تم تضمين عبارات قياس حول وجود خطط استمرارية، واختباراتها، والاستجابة للحوادث ضمن الاستبانة.

2.8.2 التعريفات التشغيلية للمتغيرات

فيما يلي التعريفات التي اعتمدت عليها الدراسة عند تصميم أداة القياس وتفسير النتائج:

- واقع تطبيق ISMS (المتغير المستقل) :مجموع متوسطات الإجابة على عبارات تقيس وجود سياسات ISMS، تخصيص الموارد، البرامج التدريبية، الضوابط التقنية، والإجراءات الإدارية (مقياس ليكرت 1–5).
- حماية البيانات الحساسة (متغير تابع) :متوسط استجابات العبارات المتعلقة بالالتزام بتعليمات حماية البيانات، وجود ضوابط وصول، وتسجيل الحوادث أو غيابها.
- ثقة المانحين / حجم المساعدات (متغير تابع) :تقدير العاملين لتأثير ISMS على مستوى ثقة المانحين مع اعتبار المؤشرات الكمية المتاحة (مثل اتجاهات التمويل) كمؤشر داعم.
- استمرارية الأعمال والقدرة على الاستجابة للأزمات (متغير تابع): متوسط استجابات عبارات حول وجود خطط استمرارية، تجارب الاستجابة للحوادث، ووقت الاسترداد المتوقع أو المحقق.

الفصل الثالث: الإطار العملي

يحتوي هذا الفصل على دراسة ميدانية حول دور نظم إدارة أمن المعلومات في تحسين الثقة والمصداقية في منظمة المجلس النرويجي للاجئين من خلال استبانة تم توزيعها على موظفين في المجلس النرويجي للاجئين في سوريا كمحاولة لإسقاط المعلومات النظرية على واقع هذه المنظمة ومن ثم استخلاص بعض النتائج والتوصيات.

3.1 لمحة عن منظمة المجلس النرويجي للاجئين

يُعد المجلس النرويجي للاجئين (Norwegian Refugee Council - NRC) من بين أبرز المنظمات الإنسانية الدولية المستقلة التي تركز على تقديم الدعم والحماية للأشخاص المتضررين من النزاعات المسلحة والتهجير القسري. تتمثل مهمتها الرئيسية في دعم اللاجئين والنازحين داخليًا والمجتمعات المضيفة من خلال توفير المساعدة الطارئة والمستدامة التي تمكنهم من استعادة حياتهم بكرامة. تأسست المنظمة في عام 1946 في أعقاب الحرب العالمية الثانية، كرد فعل مباشر للتحديات الهائلة التي واجهت اللاجئين والنازحين في أوروبا. في تلك الفترة، كانت أوروبا تعاني من أزمة لجوء واسعة النطاق، حيث اضطر ملايين الأشخاص إلى النزوح بسبب الدمار الكبير الذي خلفته الحرب. جاء المجلس النرويجي للاجئين ليكون أحد الحلول التي تقدم المساعدات الطارئة والسريعة لهؤلاء الأفراد من خلال توفير المأوى والطعام والملابس والاحتياجات الأساسية.

- **النشأة والتأسيس:** تأسس المجلس على يد مجموعة من النرويجيين المتحمسين للعمل الإنساني والذين شعروا بمسؤولية كبيرة تجاه مساعدة ضحايا الحرب. بدأ عمله كمنظمة وطنية تهدف إلى تقديم المساعدة للاجئين في أوروبا، حيث كانت القارة الأوروبية مركزًا رئيسيًا للنزوح في تلك الفترة. وركز المجلس في البداية على دعم اللاجئين الأوروبيين، خاصة في المناطق الأكثر تضررًا من الحرب، مثل ألمانيا والنرويج نفسها.
- **التحول والتوسع:** مع تغير الظروف الدولية وظهور نزاعات جديدة خارج أوروبا، بدأ المجلس النرويجي للاجئين في التوسع جغرافيًا لتلبية الاحتياجات الإنسانية في أماكن أخرى. بحلول السبعينيات والثمانينيات، كانت المنظمة قد بدأت في تقديم المساعدات في مناطق جديدة تعاني من أزمات مثل أفريقيا وأمريكا اللاتينية وآسيا. ومع توسع نطاق الأزمات الإنسانية عالميًا، كان على المجلس أن يكيف استراتيجياته ليشمل المزيد من الخدمات والبرامج التي تستجيب لتحديات متنوعة مثل النزاعات المسلحة، الكوارث الطبيعية، والأزمات الاقتصادية.

- **التوسع الدولي:** اليوم، يعمل المجلس في أكثر من 30 دولة حول العالم، ويقدم خدماته للأشخاص المتضررين في مناطق تشهد نزاعات مستمرة أو أزمات إنسانية كبيرة. تشمل هذه الدول بعضًا من أكثر البيئات تعقيدًا وخطورة، مثل سوريا، اليمن، العراق، جنوب السودان، الكونغو الديمقراطية، وغيرها. يعمل المجلس على تلبية الاحتياجات الأساسية للأشخاص المتضررين من خلال مجموعة من البرامج التي تشمل الإيواء، التعليم، الأمن الغذائي، الحماية القانونية، والمياه والصرف الصحي.
- **تطوير نموذج العمليات:** على مر السنين، طوّر المجلس نموذج عملياته ليشمل الاستجابة الطارئة وكذلك برامج التنمية المستدامة. لا يقتصر دور المجلس على تقديم المساعدات الطارئة فحسب، بل يعمل أيضًا على دعم المجتمعات المتضررة في إعادة بناء حياتهم وتأمين استقرارهم على المدى الطويل. هذا يشمل تمكينهم من الوصول إلى حقوقهم القانونية وتوفير التعليم لأطفالهم وبناء القدرات المحلية لتحسين سبل العيش.
- **السمعة الدولية:** اكتسب المجلس النرويجي للاجئين سمعة عالمية باعتباره منظمة رائدة في مجال حقوق اللاجئين والنازحين، واعتُبر مرجعًا رئيسيًا في هذا المجال. وهو عضو نشط في العديد من التحالفات الدولية الإنسانية مثل مجلس اللاجئين النرويجي في الاتحاد الأوروبي، ويعمل بشكل وثيق مع المنظمات الأممية مثل مفوضية الأمم المتحدة لشؤون اللاجئين (UNHCR)، وبرنامج الأغذية العالمي (WFP)، واليونيسف (UNICEF).

3.1.1 الرؤية والرسالة:

تتمثل رؤية المجلس النرويجي للاجئين في عالمٍ يتمتع فيه جميع الأشخاص المتضررين من النزاعات والتهجير بفرص لحياة كريمة وآمنة، حيث يتمتعون بالحماية، والحق في التعليم، والمأوى، والأمن الغذائي، والخدمات الأساسية الأخرى. أما رسالته فهي تقديم المساعدة الفورية والعملية للاجئين والنازحين والمجتمعات المتأثرة من خلال برامج إنسانية مدروسة ومتكاملة تُلبي الاحتياجات الملحة، وتدعم عمليات التعافي على المدى الطويل.

3.1.2 القيم الأساسية:

يرتكز عمل المجلس النرويجي للاجئين على خمسة قيم أساسية، وهي:

1. التفاني(Dedicated) : يلتزم المجلس بتقديم المساعدة للأشخاص المتضررين من النزاعات والتهجير القسري، ويعمل بلا كلل لضمان تلبية احتياجاتهم الأساسية وضمان حقوقهم.
2. الاحترام(Respectful) : يتعامل المجلس مع جميع الأفراد والمجتمعات التي يخدمها باحترام وكرامة، بغض النظر عن جنسهم، أو دينهم، أو خلفيتهم العرقية، أو السياسية.
3. الاستقلالية(Independent) : يعمل المجلس كمنظمة مستقلة وغير منحازة، حيث يضمن عدم تأثر عملياته الإنسانية بأي ضغوط سياسية أو اقتصادية.
4. الشمولية(Inclusive) : يؤمن المجلس بأهمية الشمولية، ويضمن أن كل من يحتاج إلى المساعدة يمكنه الوصول إليها، مع التركيز على تلبية احتياجات الفئات الأكثر تهميشًا وضعفًا.
5. المساءلة(Accountable) : يتحمل المجلس مسؤولية عالية تجاه المستفيدين، المانحين، والشركاء لضمان أن المساعدات تُستخدم بطريقة شفافة وفعالة، وأن يتم الالتزام بأفضل الممارسات والمعايير الإنسانية.

3.1.3 مجالات العمل الأساسية:

يغطي المجلس النرويجي للاجئين مجموعة واسعة من الأنشطة الإنسانية التي تهدف إلى دعم اللاجئين، النازحين داخليًا، والمجتمعات المضيفة في البيئات الأكثر تضررًا في العالم. وتتمثل مجالات العمل الأساسية للمجلس فيما يلي:

1. الإيواء(Shelter) : يقدّم المجلس حلولًا سكنية ملائمة للنازحين واللاجئين الذين فقدوا منازلهم بسبب النزاعات والكوارث. سواء كان ذلك من خلال بناء ملاجئ مؤقتة أو إعادة تأهيل المنازل المتضررة، يلعب المجلس دورًا حيويًا في توفير بيئة آمنة للمتضررين.
2. التعليم(Education) : يدير المجلس برامج تعليمية للأطفال والشباب المتضررين من النزاعات، خاصة أولئك الذين لا تتوفر لهم فرص التعليم الرسمي. يسعى المجلس من خلال هذه البرامج إلى إعادة الأطفال إلى المدارس، وضمان حصولهم على تعليم نوعي حتى في ظروف الطوارئ.
3. المساعدات القانونية(ICLA) : يقدم المجلس استشارات قانونية ومساعدات لدعم النازحين واللاجئين في الدفاع عن حقوقهم القانونية. يشمل ذلك مسائل تتعلق بتوثيق الهوية، والممتلكات والأراضي، وحقوق العمل والإقامة.

4. الأمن الغذائي وسبل العيش(Food Security & Livelihoods) : يساعد المجلس النرويجي للاجئين في تحسين الظروف المعيشية للمجتمعات المتضررة من خلال توزيع المواد الغذائية أو تقديم الدعم المالي والمساعدات التي تضمن تحسين فرص سبل العيش وتعزيز الاستقلال المالي.
5. المياه والصرف الصحي(WASH) : يدير المجلس مشاريع لتحسين الوصول إلى مياه الشرب النظيفة وتوفير مرافق الصرف الصحي الضرورية في المجتمعات التي تعاني من أوضاع إنسانية حرجة، مع ضمان مراعاة معايير النظافة والسلامة العامة.

3.1.4 انتشار العمليات:

يعمل المجلس النرويجي للاجئين في بعض من أصعب البيئات في العالم، حيث يدير برامج إنسانية في دول تعاني من نزاعات مسلحة أو أزمات إنسانية كبرى مثل سوريا، اليمن، جنوب السودان، العراق، أفغانستان، الصومال، جمهورية الكونغو الديمقراطية وغيرها. بفضل وجوده الواسع في هذه المناطق، يتمتع المجلس بقدرة كبيرة على الوصول إلى الفئات الأكثر ضعفًا واحتياجًا، ويعتبر مصدرًا موثوقًا للمساعدة الإنسانية.

3.1.5 دور نظم إدارة أمن المعلومات في المجلس النرويجي:

في ضوء الاعتماد المتزايد على التكنولوجيا الحديثة لحفظ وإدارة البيانات، يلعب نظام إدارة أمن المعلومات (ISMS) دورًا حيويًا في حماية البيانات الحساسة التي يتعامل معها المجلس النرويجي للاجئين، بما في ذلك معلومات اللاجئين والنازحين. يساهم ISMS في تأمين هذه البيانات ومنع التهديدات السيبرانية، كما ان استخدام المجلس لمثل هذا الأنظمة بحد ذاته يعزز الثقة بين المجلس والمستفيدين من خدماته، بالإضافة إلى تحسين المصداقية مع المانحين الدوليين والشركاء.

3.2 مصادر جمع البيانات

تم جمع البيانات الأولية بواسطة استبانة وزع على عدد من العاملين في المجلس النرويجي للاجئين. أما البيانات الثانوية فقد تم جمعها من خلال التقارير السنوية للمنظمة والكتب والدوريات والمواقع الإلكترونية ذات العلاقة بموضوع الدراسة حول دور نظم إدارة أمن المعلومات في تحسين الثقة والمصداقية في المجلس النرويجي للاجئين.

3.3 مجتمع وعينة الدراسة

أن مجتمع الدراسة هو العاملين في المجلس النرويجي للاجئين – سوريا.

تم تطبيق استبانة على 32 موظف (عينة عشوائية) ووزعت عليهم الاستبانة

3.4 أداة الدراسة

قام الباحث ببناء الاستبانة اللازمة لجمع البيانات المطلوبة لتحقيق أهداف الدراسة واختبار فرضياتها استنادًا إلى إطار نظري علمي ودراسات سابقة متخصصة في مجال نظم إدارة أمن المعلومات وتأثيرها على أداء المنظمات الدولية. فقد تم تطوير محاور وعبارات الاستبانة بالاعتماد على:

- ❖ الدراسات السابقة المعروضة في بداية الفصل الثاني الإطار النظري التي تناولت حماية البيانات، الثقة، واستمرارية الأعمال في المنظمات الدولية غير الحكومية.
- ❖ النماذج المستخدمة في الأدبيات العلمية لتقييم تطبيقات ISMS، وحماية البيانات، وثقة المانحين، واستمرارية الأعمال.
- ❖ دراسات أكاديمية حول نظم إدارة أمن المعلومات في القطاعات الإنسانية والقطاع غير الربحي.
- ❖ خبرة الباحث بالبيئة التشغيلية للمجلس النرويجي للاجئين وإجراءاته المؤسسية المتعلقة بأمن المعلومات والامتثال.

وانطلاقًا من هذه الأسس، صيغت عبارات كل محور بما يتوافق مع عناصر المتغيرات كما وردت في الإطار النظري، وبناءً عليه جاءت الاستبانة على الشكل الآتي:

1. البيانات الشخصية :وهو قسم اختياري يتضمن /3/ أسئلة.
2. نظم إدارة أمن المعلومات (ISMS) في المجلس النرويجي للاجئين (المتغير المستقل):
   ويتضمّن /7/ عبارات مستندة إلى الأدبيات الخاصة ببنية ISMS، مثل: السياسات الأمنية، إدارة الحوادث، ضوابط الوصول، والتوعية الأمنية.
3. دور نظم إدارة أمن المعلومات في حماية البيانات الحساسة (متغير تابع):
   ويتضمّن /4/ عبارات مستمدة من المبادئ المعتمدة في دراسات حماية البيانات الإنسانية ومرجعيات GDPR.
4. دور نظم إدارة أمن المعلومات في تعزيز المساعدات المقدمة من المانحين (متغير تابع):
   ويتضمّن /4/ عبارات صيغت بالاستناد إلى الأدبيات التي تناولت بناء الثقة والشفافية والامتثال في المنظمات الدولية غير الحكومية.
5. دور نظم إدارة أمن المعلومات في استمرارية العمل والقدرة على الاستجابة للأزمات (متغير تابع):
   ويتضمّن /4/ عبارات مبنية على مبادئ BCP/BIA ونتائج الدراسات التي تناولت جاهزية INGOs للاستجابة الإنسانية.

وبذلك تأتي الأداة البحثية مبنية على مرجعية أكاديمية واضحة، الأمر الذي يدعم صدقيتها ويؤكد ملاءمتها لقياس متغيرات الدراسة بصورة منهجية. وقد تم ارفاق نسخة من الاستبانة المذكورة في ملحق البحث كما تم استخدام مقياس ليكرت الخماسي بالاتجاه الإيجابي لقياس تقييم استجابات افراد العينة لفقرات الاستبانة كما في الجدول التالي:

الاستجابة	غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة
الوزن / الدرجة	1	2	3	4	5

الجدول رقم 2: مقياس ليكرت الخماسي
المصدر: من إعداد الباحث

كما تم تحديد طول الفئات في مقياس ليكرت الخماسي من خلال حساب المدى بين درجات المقياس (أكبر قيمة – اقل قيمة) في تدرج المقياس (5 – 1 = 4)، وطول الفئة = المدى ÷ عدد الفئات أي (4 / 5 = 0.80) وبعد ذلك تم إضافة هذه القيمة الى أقل قيمة في المقياس (بداية المقياس) وهي واحد صحيح وذلك لتحديد الحد الأعلى لكل فئة، وبالتالي يصبح التوزيع كما هو موضح في الجدول التالي:

طول الفئة	الوزن النسبي المقابل له	مستوى الموافقة
من 1 – 1.79	من 20% - 36 %	منخفضة جداً
أكبر من 1.80 – 2.59	أكبر من 36% – 52%	منخفضة
أكبر من 2.60 – 3.39	أكبر من 52% – 68%	متوسطة
أكبر من 3.40 – 4.19	أكبر من 68% – 84%	عالية
أكبر من 4.20 – 5	أكبر من 84% – 100%	عالية جداً

الجدول رقم 3: أطوال الفئات
المصدر: من إعداد الباحث

وفضلاً عما قدمه الإحصاء الوصفي من أوساط حسابية وانحرافات معيارية ودلالة الفروق للأوساط الحسابية لمتغيرات الدراسة، وكذلك تأثير وعلاقة المتغيرات المستقلة بالمتغير التابع من حيث طبيعة التأثيرات والعلاقات ودرجات المعنوية، فقد تم استخدام عدد من الأساليب الإحصائية التحليلية الاستدلالية لتحقيق إهداف الدراسة وتم اعتماد مستوى الدلالة الإحصائية 5% الذي يقابله مستوى ثقة 95% لتفسير نتائج الاختبارات التي أجراها الباحث.

3.5 أدوات التحليل الإحصائي:

بعد ان تم جمع البيانات المطلوبة من عينة الدراسة قام الباحث بإدخال هذه البيانات الى الحاسب ومن ثم تحليلها باستخدام برنامج Excel وبرنامج SPSS للتحليل الإحصائي وتم الاعتماد على الأساليب الإحصائية التالية لتحليل البيانات:

1. الإحصاءات الوصفية لمتغيرات البحث الممثلة بعبارات الاستبانة والتوزيعات التكرارية النسبية
2. معامل الثبات الداخلي (ألفا كرو نباخ) الذي يعكس استقرار المقياس وعدم تناقضه مع نفسه
3. المتوسط الحسابي: للحصول على متوسط إجابات أفراد عينة البحث على أسئلة الاستبانة
4. الانحراف المعياري: الذي يمكن من معرفة مدى التشتت المطلق بين الأوساط الحسابية
5. اختبار الانحدار الخطي البسيط في إيجاد العلاقة بين المتغير المستقل والتابع.

3.6 ثبات وصدق أداة الدراسة حساب معامل الثبات الداخلي (ألفا كرو نباخ):

تم استخدام طريقة ألفا كرو نباخ لقياس ثبات الاستبانة للتعبير عن متوسط الارتباط الداخلي بين العبارات التي يقيسها. تتراوح قيمة هذا المعامل بين (0 – 1) وتعتبر أقل قيمة مقبولة أكبر او تساوي 0.6 حيث انه كلما اقتربت قيمته من الواحد كلما ارتفعت درجة ثبات الأداة وصلاحيتها للاستخدام

المحور	عدد العبارات	ألفا كرو نباخ
واقع نظم إدارة أمن المعلومات (ISMS) في المجلس النرويجي للاجئين	7	0.814
دور نظم إدارة أمن المعلومات في حماية البيانات الحساسة	4	0.636
دور نظم إدارة أمن المعلومات في تعزيز المساعدات المقدمة من المانحين	4	0.862
دور نظم إدارة أمن المعلومات في استمرارية العمل والقدرة على الاستجابة للأزمات	4	0.737

الجدول رقم 4: اختبار الثبات لمحاور الاستبانة
المصدر: من إعداد الباحث

بناء على ما ورد في الجدول السباق يمكن القول بأن الاستبانة تتمتع بالثبات الداخلي والمصداقية ويمكن الاعتماد عليها في تحليل النتائج والإجابة على أسئلة البحث واختبار فرضياته.

3.7 عرض وتحليل بيانات البحث:

سيتم خلال هذه الموضوع التعرف على خصائص عينة الدراسة ومن ثم التحليل الوصفي لبيانات الدراسة من خلال تحديد استجابات أفراد العينة تجاه العبارات التي تتضمنها الاستبانة الخاصة بالدراسة.

3.7.1 خصائص العينة:

تتمثل خصائص العينة بما يلي:

3.7.1.1 التوزع النسبي بحسب الوظيفة:

الشكل رقم 2: التوزع النسبي بحسب الوظيفة
المصدر: من إعداد الباحث باستخدام برنامج مايكروسوفت فورمز

الشرح:

1. مدير إداري:
   - العدد: 6
   - النسبة: 19%

هذا يعني أن 19% من المشاركين في الدراسة أو العينة هم من المديرين الإداريين. تمثل هذه النسبة أقل الفئات من حيث العدد، مما قد يشير إلى أن عدد المديرين في المنظمة أقل مقارنة بالوظائف الأخرى.

2. موظف في قسم تكنولوجيا المعلومات:
   - العدد: 10
   - النسبة: 31%

يمثل موظفو قسم تكنولوجيا المعلومات 31% من العينة، مما يجعلهم الفئة الأكبر. هذه النسبة تشير إلى أهمية وجود عدد كبير من الموظفين في هذا القسم، ربما بسبب طبيعة العمل أو الحاجة المتزايدة لتكنولوجيا المعلومات.

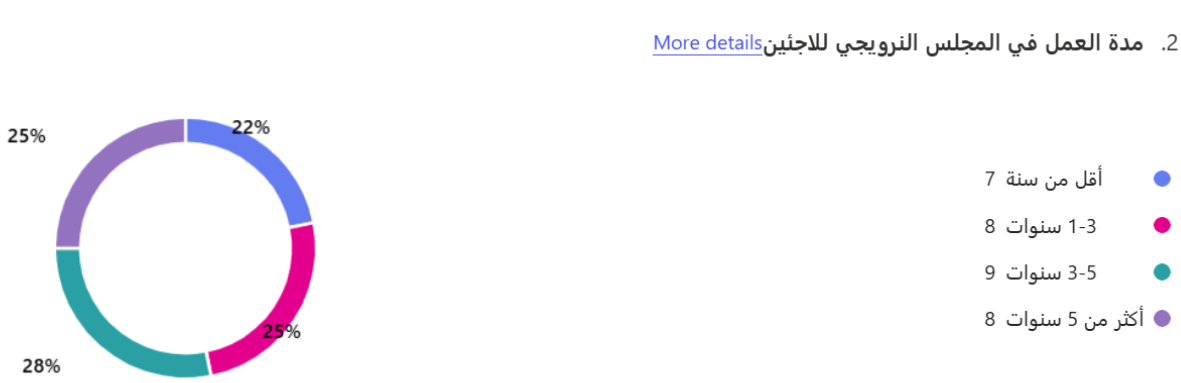
3. موظف في قسم البرامج:
   - العدد: 7
   - النسبة: 22%

   يشير إلى أن 22% من المشاركين هم من موظفي قسم البرامج. يمثل هذا العدد نسبة ملحوظة ويظهر أن هناك اهتمامًا بالبرامج في المنظمة.
4. موظف آخر:
   - العدد: 9
   - النسبة: 28%

   يشير إلى أن 28% من المشاركين هم من فئة "موظف آخر"، والتي قد تشمل موظفين من أقسام مختلفة غير محددة. تشير هذه النسبة إلى تنوع الأدوار في المنظمة.

الاستنتاج: تشير النتائج إلى توزيع متنوع للوظائف داخل المنظمة. يهيمن موظفو قسم تكنولوجيا المعلومات بنسبة 31%، مما يعكس أهمية هذا القسم. النسب الإجمالية تشير إلى وجود هيكل تنظيمي مختلط، مع وجود تمثيل جيد من جميع الفئات، مما قد يسهل التعاون بين الأقسام المختلفة.

3.7.1.2 التوزع النسبي بحسب مدة العمل في المجلس النرويجي:



الشكل رقم 3 التوزع النسبي بحسب مدة العمل
المصدر: من إعداد الباحث باستخدام برنامج مايكروسوفت فورمز

الشرح:

1. أقل من سنة:
   - العدد: 7
   - النسبة: 22%

   يشير إلى أن 22% من المشاركين لديهم خبرة أقل من سنة. هذا يعكس وجود عدد من الموظفين الجدد أو المتدربين في المنظمة.

2. 1-3 سنوات:
   - العدد: 8
   - النسبة: 25%

   تعني أن 25% من المشاركين لديهم خبرة تتراوح بين سنة وثلاث سنوات. هذه الفئة قد تمثل الموظفين الذين بدأوا في تطوير مهاراتهم ومعرفتهم في مجالاتهم.

3. 3-5 سنوات:
   - العدد: 9
   - النسبة: 28%

   تشير إلى أن 28% من المشاركين لديهم خبرة تتراوح بين ثلاث وخمس سنوات، مما يجعلها أكبر فئة من حيث العدد. يدل ذلك على وجود موظفين ذوي خبرة متوسطة ومستوى جيد من الكفاءة.

4. أكثر من 5 سنوات:
   - العدد: 8
   - النسبة: 25%

   تعني أن 25% من المشاركين لديهم أكثر من خمس سنوات من الخبرة. تمثل هذه الفئة الموظفين الأكثر خبرة، مما قد يشير إلى استقرار في القوة العاملة.

الاستنتاج: تنوع الخبرة: يشير الجدول إلى تنوع سنوات الخبرة بين المشاركين، مما يمكن أن يعزز تبادل المعرفة والتوجيه داخل المنظمة. تركيز على الكفاءة المتوسطة: تتركز النسبة الأكبر (28%) في فئة 3-5 سنوات، مما يدل على أن هناك مجموعة كبيرة من الموظفين ذوي الخبرة المتوسطة، مما قد يكون مفيدًا في بناء فرق فعالة.

وجود حديثي التخرج: وجود 22% من الموظفين ذوي الخبرة أقل من سنة يدل على استقطاب المنظمة للموظفين الجدد، مما يعكس ديناميكية في بيئة العمل.

3.7.1.3 التوزع النسبي بحسب التعامل السابق مع نظم إدارة أمن المعلومات:

الشكل رقم 4: التوزع النسبي بحسب التعامل السابق مع ISMS
المصدر: من إعداد الباحث باستخدام برنامج مايكروسوفت فورمز

الشرح:

1. نعم:
   - العدد: 27
   - النسبة: 84%

يشير هذا إلى أن 84% من المشاركين في الدراسة أو العينة أجابوا بـ "نعم". هذه النسبة العالية تعكس تأييدًا قويًا أو قبولًا لفكرة أو موضوع ما تم طرحه في السؤال.

2. لا:
   - العدد: 5
   - النسبة: 16%

تعني أن 16% فقط من المشاركين أجابوا بـ "لا". هذه النسبة تعكس وجود أقلية من الآراء المعارضة أو غير القابلة للتطبيق بالنسبة لما تم طرحه.

الاستنتاج: تأييد قوي: تعكس النتائج نسبة تأييد مرتفعة (84%)، مما يشير إلى أن الأغلبية العظمى من المشاركين تتفق مع الفكرة المطروحة. قليل من المعارضة: نسبة الـ 16% تعكس معارضة أو عدم قبول، مما يدل على وجود بعض التنوع في الآراء، لكن بشكل عام، الأغلبية تؤيد الفكرة.

3.8 التحليل الوصفي لمتغيرات الدراسة:

يهدف تحليل نتائج إجابات عينة الدراسة الأساسية لأخذ صورة أولية عن تقييمهم لمحور الدراسة، والتي يتم من خلاله الوقوف على أهمية كل من العبارات المرشة للتحليل التي وردت التي تناولها الاستبيان و مدى توافق الآراء تجاه كل من هذه المتغيرات حيث سيتم اجراء استعراض عام لنتائج التحليل الوصفي باعتماد المتوسط الحسابي و الانحراف المعياري لمعرفة درجة توافق أو تباين الآراء بين افراد عينة الدراسة تجاه كل من متغيرات الدراسة، و بالتالي الإجابة على تساؤلات الدراسة، و كانت حصيلة التحليل باستخدام برنامج SPSS على النحو الاتي:

الإحصاءات الوصفية					
	N	الحد الأدنى	الحد الأقصى	المتوسط	الانحراف المعياري
الوظيفة	32	1.00	4.00	2.5938	1.10306
مدة العمل في المجلس النرويجي للاجئين	32	1.00	4.00	2.5625	1.10534
هل سبق لك التعامل مع نظم إدارة أمن المعلومات في عملك	32	1.00	2.00	1.1563	.36890
هناك نظام لإدارة أمن المعلومات (ISMS) مطبق بشكل كامل داخل المجلس النرويجي للاجئين	32	3.00	5.00	4.3438	.60158
إدارة المنظمة تلتزم بتطبيق سياسات أمن المعلومات بشكل دائم	32	3.00	5.00	4.4375	.71561
تتوفر الموارد التقنية والمالية الكافية لدعم تطبيق نظام إدارة أمن المعلومات (ISMS) في المجلس.	32	3.00	5.00	4.3438	.70066
يتلقى موظفو المجلس تدريبًا دوريًا على أفضل الممارسات في أمن المعلومات.	32	2.00	5.00	4.2813	.77186
الموظفون يتبعون بدقة إرشادات أمن المعلومات في التعامل مع البيانات الحساسة.	32	2.00	5.00	4.3125	.73780
هناك قنوات اتصال واضحة للإبلاغ عن الحوادث الأمنية أو انتهاكات نظام إدارة أمن المعلومات.(ISMS)	32	3.00	5.00	4.2500	.80322
تطبيق نظم إدارة أمن المعلومات يساهم في الحد من التهديدات السيبرانية التي تواجه المنظمة.	32	3.00	5.00	4.3750	.60907
نظام إدارة أمن المعلومات (ISMS) يحمي البيانات الحساسة داخل المجلس النرويجي للاجئين بشكل فعال.	32	3.00	5.00	4.3750	.65991
تطبيق نظم إدارة أمن المعلومات يساهم في تقليل مخاطر تسريب أو اختراق البيانات الحساسة.	32	3.00	5.00	4.3125	.64446

الموظفون في المجلس النرويجي للاجئين مدربون بشكل كافٍ على تطبيق إجراءات أمن المعلومات لحماية البيانات الحساسة.	32	3.00	5.00	4.1875	.78030
التعامل مع التقارير أو الحوادث المتعلقة بأمن المعلومات داخل المنظمة يتم بجدية كافية.	32	3.00	5.00	4.2813	.68318
تطبيق نظم إدارة أمن المعلومات يؤثر بشكل إيجابي على ثقة المانحين في المجلس النرويجي للاجئين.	32	3.00	5.00	4.4688	.62136
المانحون يقدمون مساعدات أكبر للمجلس نتيجة تطبيق نظم إدارة أمن المعلومات.	32	3.00	5.00	4.1563	.88388
نظم إدارة أمن المعلومات تساهم في زيادة حجم المساعدات المقدمة للمجلس النرويجي للاجئين.	32	2.00	5.00	4.1563	.72332
هناك متطلبات أمنية إضافية من قبل المانحين تتأثر بشكل إيجابي بتطبيق نظم إدارة أمن المعلومات في المجلس.	32	3.00	5.00	4.3438	.70066
نظم إدارة أمن المعلومات تساهم بشكل كبير في استمرارية العمل داخل المجلس النرويجي للاجئين.	32	2.00	5.00	4.2500	.76200
تطبيق نظم إدارة أمن المعلومات يعزز قدرة المجلس النرويجي للاجئين على الاستجابة للأزمات الدولية بشكل فعال.	32	3.00	5.00	4.1563	.76662
وجود نظام نظم إدارة أمن المعلومات يقلل من التحديات اللوجستية التي تواجه المنظمة في بيئات الأزمات.	32	2.00	5.00	3.8750	.70711
تطبيق نظم إدارة أمن المعلومات يقلل من احتمالية توقف الأنظمة أو تسريب البيانات خلال الأزمات.	32	3.00	5.00	4.1563	.72332

الجدول رقم 5 : الإحصاءات الوصفية لمتغيرات الدراسة

المصدر: من إعداد الباحث باستخدام برنامج SPSS

3.8.1 تفسير النتائج:

فيما يلي شرحًا تفصيليًا لنتائج الجدول السابق:

1. N (عدد المشاركين) :جميع المتغيرات تشمل 32 مشاركًا، مما يعني أن حجم العينة متساوي عبر جميع المتغيرات.
2. الحد الأدنى والحد الأقصى :تم تحديد الحد الأدنى والحد الأقصى لكل متغير، مما يشير إلى مدى تنوع الردود.
3. المتوسط :

- يُظهر المتوسط قيمة مركزية للردود. القيم الأعلى (مثل 4.4375 لإدارة المنظمة التي تلتزم بتطبيق سياسات أمن المعلومات) تشير إلى أن الأغلبية تعتقد أن هناك التزامًا قويًا من الإدارة.
- القيم الأقل (مثل 2.5938 للوظيفة) قد تشير إلى تنوع أكبر في أنواع الوظائف أو مستويات الخبرة.

4. الانحراف المعياري: يعكس الانحراف المعياري مدى تشتت البيانات حول المتوسط. القيم الأقل تشير إلى تشتت أقل، مما يعني أن الآراء متقاربة. على سبيل المثال، الردود حول "تطبيق نظم إدارة أمن المعلومات يساهم في الحد من التهديدات السيبرانية" لديها انحراف معياري قدره 0.60907، مما يدل على أن الآراء حول هذا الموضوع متقاربة.

الاستنتاج:

- ❖ الالتزام والموارد: النتائج تشير إلى وجود التزام قوي من الإدارة تجاه تطبيق نظم إدارة أمن المعلومات، بالإضافة إلى توافر الموارد اللازمة.
- ❖ تدريب الموظفين: يظهر أن الموظفين يتلقون تدريبًا جيدًا ويظهرون اتباعًا لإرشادات أمن المعلومات، مما يعكس بيئة عمل مستندة إلى الأمان.
- ❖ تأثير نظم إدارة أمن المعلومات على الثقة: هناك شعور قوي بأن تطبيق نظم إدارة أمن المعلومات له تأثير إيجابي على الثقة لدى المانحين وزيادة المساعدات.
- ❖ التنوع في الخبرة: الاختلاف في المتوسطات والحدود يشير إلى أن هناك تنوعًا في مستويات الخبرة والمعرفة بين المشاركين.

3.9 اختبار فرضيات البحث:

يهدف هذا البحث إلى دراسة دور نظم إدارة أمن المعلومات (ISMS) في تحسين الثقة والمصداقية لدى منظمة المجلس النرويجي للاجئين. استنادًا إلى هذا الهدف الرئيسي، سيتم اختبار مجموعة من الفرضيات التي ترتبط بشكل مباشر بالأهداف الفرعية من خلال البيانات التي تم جمعها وتحليلها باستخدام أدوات التحليل الإحصائي المناسبة للتحقق من صحتها ودورها في تحقيق الأهداف المحددة للبحث.

الفرضية الرئيسية: تطبيق نظم إدارة أمن المعلومات (ISMS) يعزز الثقة والمصداقية في منظمة المجلس النرويجي للاجئين.

ويتفرع عنها ثلاث فرضيات فرعية:

1. **الفرضية الفرعية الأولى:** يوجد دور ذو دلالة إحصائية لتطبيق نظم إدارة أمن المعلومات في المساهمة الفعالة في حماية البيانات الحساسة داخل المجلس النرويجي للاجئين.

لاختبار الفرضية الأولى قام الباحث بتطبيق تحليل الانحدار الخطي لدراسة دور المتغير المستقل (نظم إدارة امن المعلومات) على التابع مستوى الثقة والمصداقية في المجلس النرويجي للاجئين من حيث (حماية البيانات الحساسة) وكانت النتائج وفق الاتي:

Model Summary									
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.696[a]	.484	.467	.35048	.484	28.116	1	30	.000

الجدول رقم 6: معاملي الارتباط والتحديد لمتغيرات الفرضية الفرعية الأولى
المصدر: من إعداد الباحث باستخدام برنامج SPSS

- **R**: 0.696، وهو معامل الارتباط بين المتغير المستقل (واقع نظم إدارة أمن المعلومات) والمتغير التابع (حماية البيانات الحساسة). يشير إلى علاقة قوية بين المتغيرين.
- **R Square**: 0.484، وهذا يعني أن حوالي 48.4% من التباين في المتغير التابع يمكن تفسيره بواسطة المتغير المستقل.
- **Adjusted R Square**: 0.467، يشير إلى القيمة المعدلة التي تأخذ في الحسبان عدد المتغيرات والمشاهدات. هذه القيمة تظل جيدة، مما يعني أن النموذج موثوق.
- **Std. Error of the Estimate**: 0.35048، وهو الخطأ المعياري للتقدير، ويقيس مدى دقة التنبؤات.

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	3.454	1	3.454	28.116	.000[b]
	Residual	3.685	30	.123		
	Total	7.139	31			
a. Dependent Variable: دور نظم إدارة أمن المعلومات في حماية البيانات الحساسة						
b. Predictors: (Constant), واقع نظم إدارة أمن المعلومات في المجلس النرويجي للاجئين						

الجدول رقم 7: نتائج تحليل الانحدار لمتغيرات الفرضية الفرعية الأولى
المصدر: من إعداد الباحث باستخدام برنامج SPSS

- **F**: 28.116، وهي قيمة كبيرة مما يشير إلى أن النموذج جيد ويمكن استخدامه لتفسير المتغير التابع.
- **Sig.**: القيمة الدالة هي .000، وهي أقل بكثير من 0.05، مما يعني أن النموذج ككل ذو دلالة إحصائية. هناك تأثير كبير للمتغير المستقل على المتغير التابع.

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.322	.563		2.348	.026
	واقع نظم إدارة أمن المعلومات (ISMS) في المجلس النرويجي للاجئين	.684	.129	.696	5.302	.000
a. Dependent Variable: دور نظم إدارة أمن المعلومات في حماية البيانات الحساسة						

الجدول رقم 8: معاملات نموذج الانحدار لمتغيرات الفرضية الفرعية الأولى
المصدر: من إعداد الباحث باستخدام برنامج SPSS

- **B (Constant)**: الثابت 1.322، وهو القيمة التقديرية لحماية البيانات الحساسة عندما تكون قيمة المتغير المستقل (واقع نظم إدارة أمن المعلومات) تساوي صفر.
- B (واقع نظم إدارة أمن المعلومات): 0.684، وهي تشير إلى أن كل زيادة بمقدار وحدة واحدة في نظم إدارة أمن المعلومات تؤدي إلى زيادة في حماية البيانات الحساسة بمقدار 0.684 وحدة.
- **t-value**: 5.302، وهي قيمة كبيرة تشير إلى أن المتغير المستقل له تأثير كبير على المتغير التابع
- **Sig.:** القيمة الدالة هي .000، مما يعني أن هذا المتغير ذو دلالة إحصائية قوية وتأثيره ليس عشوائيًا

الاستنتاج: النتائج تشير إلى أن هناك علاقة قوية ومؤثرة بين واقع نظم إدارة أمن المعلومات (ISMS) وحماية البيانات الحساسة داخل المجلس النرويجي للاجئين. النموذج التفسيري ذو دلالة إحصائية، مما يعني أن فرضيتك الفرعية الأولى مدعومة بشكل جيد بناءً على تحليل الانحدار.

2. **الفرضية الفرعية الثانية:** يوجد دور ذو دلالة إحصائية لتطبيق نظم إدارة أمن المعلومات في زيادة حجم المساعدات المقدمة من المانحين للمجلس النرويجي للاجئين..

لاختبار الفرضية الثانية قام الباحث بتطبيق تحليل الانحدار الخطي لدراسة دور المتغير المستقل (نظم إدارة امن المعلومات) على التابع مستوى الثقة والمصداقية في المجلس النرويجي للاجئين من حيث (تعزيز المساعدات المقدمة من المانحين) وكانت النتائج وفق الاتي:

Model Summary									
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.637[a]	.406	.386	.48673	.406	20.522	1	30	.000

الجدول رقم 9: معاملي الارتباط والتحديد لمتغيرات الفرضية الفرعية الثانية
المصدر: من إعداد الباحث باستخدام برنامج SPSS

- **R**: 0.637، وهو معامل الارتباط بين المتغير المستقل (واقع نظم إدارة أمن المعلومات) والمتغير التابع (تعزيز المساعدات المقدمة من المانحين). هذا يشير إلى وجود علاقة قوية نسبياً بين المتغيرين.
- **R Square**: 0.406، يعني أن 40.6% من التباين في المتغير التابع (تعزيز المساعدات المقدمة من المانحين) يمكن تفسيره بواسطة المتغير المستقل (واقع نظم إدارة أمن المعلومات).
- **Adjusted R Square**: 0.386، يأخذ في الاعتبار عدد المتغيرات وعينة البيانات، ويشير إلى أن النموذج تفسيري جيد حتى بعد التعديل.
- **Std. Error of the Estimate**: 0.48673، يشير إلى مقدار الخطأ المعياري للتقدير، ويستخدم لقياس مدى دقة التوقعات.

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	4.862	1	4.862	20.522	.000[b]
	Residual	7.107	30	.237		
	Total	11.969	31			
a. Dependent Variable: دور نظم إدارة أمن المعلومات في تعزيز المساعدات المقدمة من المانحين						
b. Predictors: (Constant), واقع نظم إدارة أمن المعلومات في المجلس النرويجي للاجئين						

الجدول رقم 10: نتائج تحليل الانحدار لمتغيرات الفرضية الفرعية الثانية
المصدر: من إعداد الباحث باستخدام برنامج SPSS

- **F:** قيمة F تساوي 20.522، وهي قيمة كبيرة تشير إلى أن النموذج قادر على تفسير التغيرات في المتغير التابع.
- **Sig.:** القيمة الدالة (p-value) هي .000، وهي أقل بكثير من 0.05، مما يعني أن النموذج ذو دلالة إحصائية عالية، وبالتالي هناك تأثير كبير لنظم إدارة أمن المعلومات (ISMS) على تعزيز المساعدات المقدمة من المانحين.

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.761	.782		.973	.338
	واقع نظم إدارة أمن المعلومات (ISMS) في المجلس النرويجي للاجئين	.812	.179	.637	4.530	.000
a. Dependent Variable: دور نظم إدارة أمن المعلومات في تعزيز المساعدات المقدمة من المانحين						

الجدول رقم 11: معاملات نموذج الانحدار لمتغيرات الفرضية الفرعية الثانية
المصدر: من إعداد الباحث باستخدام برنامج SPSS

- **B (Constant):** الثابت هو 0.761، وهو القيمة التقديرية لتعزيز المساعدات المقدمة من المانحين عندما تكون قيمة المتغير المستقل (واقع نظم إدارة أمن المعلومات) تساوي صفر.
- **B (واقع نظم إدارة أمن المعلومات):** 0.812، مما يعني أن كل زيادة بمقدار وحدة واحدة في نظم إدارة أمن المعلومات تؤدي إلى زيادة في تعزيز المساعدات المقدمة من المانحين بمقدار 0.812 وحدة.
- **t-value**: 4.530، وهي قيمة كبيرة تشير إلى أن تأثير نظم إدارة أمن المعلومات على تعزيز المساعدات المقدمة من المانحين ذو دلالة إحصائية.
- **Sig.:** القيمة الدالة هي .000، مما يعني أن التأثير ليس عشوائياً وله دلالة قوية جداً.

الاستنتاج: هذه النتائج تشير إلى أن هناك علاقة قوية بين واقع نظم إدارة أمن المعلومات في المجلس النرويجي للاجئين وتعزيز المساعدات المقدمة من المانحين. النموذج تفسيري جيد وله دلالة إحصائية كبيرة، مما يعني أن الفرضية الفرعية الثانية التي تقول بأن "تطبيق نظم إدارة أمن المعلومات يساهم بشكل فعال في تعزيز المساعدات المقدمة من المانحين" مدعومة بقوة من خلال تحليل الانحدار.

3. **الفرضية الفرعية الثالثة:** يوجد دور ذو دلالة إحصائية لتطبيق نظم إدارة أمن المعلومات في تعزيز استمرارية العمل والقدرة على الاستجابة للأزمات في المجلس النرويجي للاجئين.

لاختبار الفرضية الثالثة قام الباحث بتطبيق تحليل الانحدار الخطي لدراسة دور المتغير المستقل (نظم إدارة امن المعلومات) على التابع مستوى الثقة والمصداقية في المجلس النرويجي للاجئين من حيث (استمرارية العمل والقدرة على الاستجابة للأزمات) وكانت النتائج وفق الاتي:

Model Summary									
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.453[a]	.206	.179	.50137	.206	7.761	1	30	.009

الجدول رقم 12: معاملي الارتباط والتحديد لمتغيرات الفرضية الفرعية الثالثة
المصدر: من إعداد الباحث باستخدام برنامج SPSS

- **R**: 0.453، وهو معامل الارتباط بين المتغير المستقل (واقع نظم إدارة أمن المعلومات) والمتغير التابع (استمرارية العمل والقدرة على الاستجابة للأزمات). يشير إلى وجود علاقة متوسطة القوة بين المتغيرين.
- **R Square**: 0.206، يعني أن 20.6% من التباين في استمرارية العمل والقدرة على الاستجابة للأزمات يمكن تفسيره من خلال نظم إدارة أمن المعلومات.
- **Adjusted R Square**: 0.179، يأخذ في الاعتبار عدد المتغيرات وحجم العينة، وهو مشابه إلى حد كبير لR Square ، مما يشير إلى استقرار النموذج.
- **Std. Error of the Estimate**: 0.50137، يمثل مقدار الخطأ في التقدير.

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1.951	1	1.951	7.761	.009[b]
	Residual	7.541	30	.251		
	Total	9.492	31			
a. Dependent Variable: دور نظم إدارة أمن المعلومات في استمرارية العمل والقدرة على الاستجابة للأزمات						
b. Predictors: (Constant), واقع نظم إدارة أمن المعلومات في المجلس النرويجي للاجئين						

الجدول رقم 13: نتائج تحليل الانحدار لمتغيرات الفرضية الفرعية الثالثة
المصدر: من إعداد الباحث باستخدام برنامج SPSS

- **F:** قيمة F تساوي 7.761، وهي تشير إلى أن النموذج يفسر كمية كبيرة من التباين في المتغير التابع.
- **Sig.:** القيمة الدالة (p-value) هي .009، وهي أقل من 0.05، مما يعني أن النموذج ذو دلالة إحصائية وأن هناك علاقة بين نظم إدارة أمن المعلومات واستمرارية العمل.

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.879	.805		2.334	.027
	واقع نظم إدارة أمن المعلومات في المجلس النرويجي للاجئين (ISMS)	.514	.185	.453	2.786	.009
a. Dependent Variable: دور نظم إدارة أمن المعلومات في استمرارية العمل والقدرة على الاستجابة للأزمات						

الجدول رقم 14: معاملات نموذج الانحدار لمتغيرات الفرضية الفرعية الثالثة
المصدر: من إعداد الباحث باستخدام برنامج SPSS

- **B (Constant):** الثابت هو 1.879، وهو قيمة استمرارية العمل عندما تكون قيمة نظم إدارة أمن المعلومات صفر.
- **B (واقع نظم إدارة أمن المعلومات):** 0.514، مما يعني أن كل زيادة بوحدة واحدة في نظم إدارة أمن المعلومات تؤدي إلى زيادة في استمرارية العمل والقدرة على الاستجابة للأزمات بمقدار 0.514 وحدة.

- **t-value**: 2.786، وهي قيمة كبيرة تشير إلى أن التأثير ذو دلالة إحصائية.
- **Sig.:** القيمة الدالة هي .009، مما يعني أن التأثير ذو دلالة قوية جداً.

الاستنتاج: هذه النتائج تشير إلى أن نظم إدارة أمن المعلومات لها تأثير إيجابي ومهم على استمرارية العمل والقدرة على الاستجابة للأزمات. النموذج ذو دلالة إحصائية قوية، مما يعني أن الفرضية الفرعية الثالثة، التي تقول "تطبيق نظم إدارة أمن المعلومات يساهم بشكل فعال في استمرارية العمل والقدرة على الاستجابة للأزمات الدولية"، مدعومة بنتائج التحليل.

3.10 نتائج البحث

تهدف هذه الدراسة إلى استقصاء دور نظم إدارة أمن المعلومات في تعزيز الثقة والمصداقية داخل المنظمات الدولية غير الحكومية، من خلال فحص دورها في حماية البيانات الحساسة، وفي مستوى ثقة المانحين، وفي دعم استمرارية أعمال المجلس النرويجي للاجئين وقدرته على الاستجابة للأزمات. وبعد إجراء التحليل الإحصائي للبيانات المجمّعة من عينة الموظفين، تبيّنت مجموعة من النتائج التي تُسهم في فهم العلاقة بين هذه المتغيرات، وتوضّح انعكاس تطبيق نظم أمن المعلومات على واقع العمل الإنساني. وتعرض الفقرات التالية نتائج الدراسة بحسب أسئلتها الرئيسة، مع تفسيرها وربطها بالأدبيات السابقة وبسياق عمل المنظمات الدولية.

1. تأثير نظم إدارة أمن المعلومات على حماية البيانات الحساسة:

أظهرت النتائج وجود دور قوي وذي دلالة إحصائية بين تطبيق ISMS وحماية البيانات الحساسة؛ إذ بلغ معامل الارتباط (0.696)، وفسّر نموذج الانحدار ما نسبته (48.4%) من التغير في حماية البيانات. وتشير هذه النتيجة إلى أن ممارسات أمن المعلومات داخل المنظمة—مثل سياسات الوصول، التوعية الأمنية، وإدارة الحوادث—تسهم بشكل مباشر في تقليل احتمالات التسريب أو سوء الاستخدام.

وتتوافق هذه النتيجة مع ما ورد في الدراسات السابقة، خاصة الدراسات التي أبرزت حساسية بيانات المستفيدين ودور الالتزام الأمني في الحد من المخاطر. كما تتماشى مع ما وجدتْه دراسات مثل Lindström (2022) حول دور الإجراءات التقنية والتنظيمية في تحسين حماية البيانات في المنظمات الخيرية. ويعكس ذلك أيضًا الوعي المرتفع لدى موظفيNRC ، حيث أكد معظمهم تعاملهم المباشر مع ISMSوالتزامهم بإجراءات التعامل مع البيانات.

ومن وجهة نظر الباحث، فإن هذه النتيجة منطقية بالنظر إلى البنية المؤسسية ل NRC، الذي يعتمد على نظام حماية بيانات متوافق مع GDPR، الأمر الذي يعزز فعالية ISMS في هذا السياق.

2. تأثير نظم إدارة أمن المعلومات على ثقة المانحين وحجم المساعدات المقدمة:

نتائج البحث أوضحت بأن تطبيق ISMS يرتبط بشكل إيجابي وواضح بثقة المانحين وبحجم المساعدات المقدمة للمنظمة، حيث أشارت تحليلات الانحدار إلى علاقة قوية بين المتغيرين، وانعكس ذلك في متوسطات مرتفعة لتقييم الموظفين لدور ISMS في تعزيز ثقة الجهات الممولة. ويشير ذلك إلى أن الالتزام بأمن المعلومات يقدم لإدارة التمويل أدلة ملموسة على مصداقية المنظمة، مما يجعلها أكثر قدرة على جذب التمويل وتجديده.

تتفق هذه النتيجة مع الدراسات السابقة التي تناولت علاقة الأمن الرقمي بالثقة، ومنها دراسة Lawson-Bodyوغيره (2023) التي أظهرت أن ممارسات حماية البيانات تعزز ولاء ودعم الجهات الممولة. كما تنسجم مع ما أشار إليه Al Achkar (2021) حول أهمية الأمن السيبراني في الحد من "مخاطر الثقة" بين المانحين والمنظمات الإنسانية.

ويلاحظ الباحث أن ارتفاع مستوى الانسجام بين نتائج الدراسة والأدبيات يعود إلى طبيعة بيئة العمل في INGOs، حيث يُعد الامتثال الأمني مؤشرًا مهمًا على الجدارة المؤسسية، خصوصًا مع ارتفاع متطلبات المانحين المتعلقة بالحوكمة والشفافية.

3. تأثير نظم إدارة أمن المعلومات على استمرارية العمل والقدرة على الاستجابة للأزمات:

كشفت نتائج الدراسة وجود تأثير إيجابي مهم لتطبيق ISMS على استمرارية الأعمال وقدرة المنظمة على الاستجابة للأزمات، إذ ارتفعت المتوسطات المرتبطة بهذا البعد إلى مستوى جيد، مع دلالة واضحة في نموذج الانحدار. وتدل هذه النتيجة على أن وجود بنية أمنية قوية يحدّ من توقف الأنظمة، ويحسن قدرة المنظمة على الحفاظ على عملياتها الأساسية، ويعزز ثقة المانحين، مما يسهل الحصول على التمويل في الوقت المناسب عند وقوع الأزمات.

وتتوافق هذه النتيجة مع ما عرضته دراسات مثل Fast (2022) وVan de Walle (2009)، التي أكدت أن حماية المعلومات ونضج نظمها الداخلية تعزز قدرة المنظمات الإنسانية على الاستجابة والانتشار السريع في حالات الطوارئ. كما تُظهر النتائج بعض التباين في تقييم الموظفين لمسائل الاستمرارية مقارنة بالجوانب الأخرى، ما قد يعكس التحديات التشغيلية وبيئة العمل المعقدة في السياق الإنساني، وهو ما يتسق مع ملاحظات الأدبيات التي ترى أن الاستمرارية في INGOs تعتمد بدرجة كبيرة على التمويل الخارجي وعلى استقرار الأنظمة التقنية.

ويرى الباحث أن نتائج هذا المحور تُظهر تكامل العلاقة بين ISMS والجاهزية الإنسانية، وأن تحسين الضوابط الأمنية يسهم في رفع كفاءة الاستجابة، مما يعزز مكانة المنظمة لدى الممولين.

4. تحليل خصائص العينة:

يبيّن توزيع العينة المكوّنة من 32 موظفاً أن فئة تكنولوجيا المعلومات كانت الأكثر تمثيلاً، وهو ما قد يفسّر الميل الإيجابي في تقييم فعالية نظم إدارة أمن المعلومات نظراً لخبرتهم المباشرة في التعامل معه. كما يظهر توازن نسبي في سنوات الخبرة، مما يعكس تنوّعاً يمكن أن يؤثر في اختلاف طرق فهم مستوى حماية البيانات واستمرارية العمل داخل المنظمة. ويلاحظ أن 84% من أفراد العينة لديهم تعامل سابق مع ISMS، الأمر الذي يدعم موثوقية إجاباتهم حول أسئلة الدراسة، لكنه قد يحدّ من رصد بعض جوانب القصور التي قد يلاحظها مستخدمون أقل خبرة.

وتتفق هذه الملاحظات مع ما أشارت إليه الدراسات السابقة في ضرورة فهم خصائص العينة عند تفسير نتائج الأمن المعلوماتي، حيث يؤثر التمثيل الوظيفي والخبرة التقنية في اتجاهات الإجابة. وبناءً عليه، تُعد خصائص العينة عاملاً تفسيرياً مهماً للنتائج المتعلقة بحماية البيانات وثقة المانحين واستمرارية الأعمال، مع الإقرار بأن محدودية حجم العينة وتركيزها الوظيفي يحدّان من إمكانية تعميم النتائج بشكل كامل.

3.11 التوصيات

بناءً على نتائج الدراسة وتحليل البيانات المتعلقة بواقع تطبيق نظم إدارة أمن المعلومات (ISMS) في المجلس النرويجي للاجئين في سوريا، وبالنظر إلى خصائص العينة ومستوى المعرفة المسبق لدى الموظفين، يمكن تقديم التوصيات التالية لتعزيز فعالية النظام ورفع مستوى الثقة والمصداقية لدى المانحين والشركاء والمستفيدين:

1. **تعزيز التدريب المستمر للموظفين** :يظهر من تحليل العينة أن فئة التكنولوجيا تمثّل الحصة الأكبر، مما يعزز الحاجة إلى توسيع التدريب ليشمل الموظفين غير التقنيين الذين قد يفتقرون إلى المعرفة الكافية بممارسات .ISMS ويُوصى بتقديم برامج تدريبية دورية تركز على حماية البيانات، وإدارة الحوادث، والوعي الأمني، بما يسهم في الحد من الأخطاء البشرية وتحسين الالتزام العام بالسياسات.

2. **توسيع نطاق تطبيق ISMS ليشمل العمليات الإدارية وغير التقنية:** تشير النتائج إلى أن المعرفة السابقة بالنظام مرتفعة بين العاملين في المجال التقني، بينما قد تكون أقل لدى الأقسام الأخرى. لذلك يُوصى بتفعيل ISMS على مستوى جميع الإدارات، بما في ذلك المالية والبرامج والموارد البشرية، لضمان تغطية شاملة للعمليات وتعزيز الشفافية والمصداقية أمام المانحين.

3. **تحسين قنوات التواصل الداخلي والإبلاغ عن الحوادث:** توضح الدراسة وجود حاجة إلى تعزيز آليات الإبلاغ عن الثغرات والحوادث الأمنية، بما يضمن الاستجابة السريعة ويقلل احتمال تفاقم المخاطر. ويُوصى بتطوير قنوات تواصل فعّالة وسرية، وتوعية الموظفين بكيفية استخدامها دون تخوف من أية تبعات.

4. **الاستثمار في التقنيات الأمنية المتقدمة:** في ظل زيادة التحديات السيبرانية، ينبغي للمجلس الاستثمار في أنظمة الكشف المبكر وتحليل التهديدات، بما في ذلك حلول مراقبة الشبكات، وأنظمة إدارة الهويات، والتحقق متعدد العوامل، وذلك لضمان حماية البنية التحتية الرقمية بطريقة استباقية.

5. **مراقبة وتقييم فعالية نظم إدارة أمن المعلومات بشكل دوري وضمان التوافق مع المتطلبات الدولية:** تُظهر النتائج أهمية المتابعة المستمرة لمدى فعالية النظام، خصوصاً في البيئات الإنسانية التي تتغير فيها المخاطر بسرعة. ويُوصى بتنفيذ اختبارات اختراق دورية، ومراجعات امتثال، وتقييم مستويات النضج الأمني وفق المعايير الدولية مثل ISO 27001.

6. **تعزيز شفافية سياسات أمن المعلومات مع المانحين**: نظراً لدور ISMS في زيادة ثقة المانحين، يُوصى بمشاركة السياسات الرئيسية المتعلقة بالأمن السيبراني ومستوى الامتثال، بما يعكس التزام المنظمة بحماية البيانات وتأمين الأنظمة. يمكن أن تسهم هذه الشفافية في زيادة الثقة وبالتالي تعزيز حجم المساعدات المقدمة.

7. **تقوية خطط استمرارية العمل والتعافي من الكوارث:** تشير النتائج إلى أهمية دور ISMS في استمرارية الأعمال، لذلك يُوصى بتطوير خطط مرنة وواضحة للتشغيل أثناء الأزمات، وتحديثها بشكل مستمر بما يتناسب مع المخاطر المتجددة التي تواجه بيئات العمل الإنسانية.

8. **التنسيق مع المانحين لتوحيد متطلبات أمن المعلومات:** يمكن أن يسهم التناغم بين سياسات المنظمة ومتطلبات المانحين في تعزيز فرص التمويل. لذلك يُوصى بإجراء مشاورات منتظمة لضمان توافق بنية ISMS مع توقعات الجهات الداعمة.

9. **تشجيع المنظمات الشريكة على تبني نظم إدارة أمن المعلومات:** نظراً لكثرة العمل مع شركاء محليين ودوليين، يُوصى بدعم تلك المؤسسات في تبني سياسات أمن معلومات مماثلة، بما يقلل من المخاطر الناتجة عن تبادل البيانات ويعزز الثقة المتبادلة.

10. **متابعة التطورات القانونية المتعلقة بأمن المعلومات** :يوصى بمتابعة التطورات في القوانين واللوائح الدولية المتعلقة بأمن المعلومات، وذلك لضمان الامتثال التام لمتطلبات الجهات التشريعية في المناطق التي تعمل فيها المنظمة.

هذه التوصيات تستند مباشرة إلى ما أظهرته نتائج الدراسة من نقاط قوة وفرص تحسين في تطبيق نظم إدارة أمن المعلومات داخل المجلس النرويجي للاجئين، وتستهدف تعزيز مستوى النضج الأمني، ورفع ثقة المانحين، وضمان استمرارية العمليات الإنسانية في البيئات عالية المخاطر.

المراجع

فيما يلي بعض المراجع التي تم الاعتماد عليها في إطار تحضير هذا البحث المتواضع:

1. **Al Achkar, Z.** (2021). *Digital risk: How new technologies impact acceptance and raise new challenges for NGOs.* Retrieved from https://gisf.ngo/wp-content/uploads/2021/12/Digital_Risk_how_new_technologies_impact_acceptance_and_raise_new_challenges_for_NGOs.pdf
2. **Ayre, E.** (2010). *The information management challenge: A briefing on information security for humanitarian NGOs in the field.* European Interagency Security Forum (EISF). Retrieved from https://www.researchgate.net/publication/314096686_Cybersecurity_in_Non-Profit_and_Non-Governmental_Organizations
3. **Billaud, J.** (2023). *Humanitarian technologies of trust.* Retrieved from https://www.berghahnjournals.com/view/journals/cja/41/2/cja410204.pdf
4. **Brotby, K.** (2009). *Information security governance: Guidance for information security managers.* Auerbach Publications.
5. **Council of Europe.** (2001). *Convention on cybercrime (Budapest Convention).* Retrieved from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
6. **Dhillon, G.** (2007). *Principles of information systems security: Text and cases.* Wiley.
7. **Fast, L.** (2022). *Data sharing between humanitarian organizations and donors: Toward understanding and articulating responsible practice.* Norwegian Centre for Humanitarian Studies. Retrieved from https://www.humanitarianstudies.no/resource/data-sharing-between-humanitarian-organisations-and-donors/
8. **Gerber, M., & Von Solms, R.** (2005). Management of risk in the information age. *Computers & Security, 24*(1), 16–30. https://doi.org/10.1016/j.cose.2004.11.003
9. **Hancock, B., Ockenden, N., Windridge, K., & Edwards, J.** (2009). *An introduction to qualitative research.* Trent Focus.
10. **Humphreys, E.** (2008). Information security management standards: Compliance, governance and risk management. *Information Security Technical Report, 13*(4), 247–255. https://doi.org/10.1016/j.istr.2008.10.010
11. **International Organization for Standardization (ISO).** (2013). *ISO/IEC 27001:2013 – Information security management systems requirements.* ISO.

12. **Lawson-Body, A., Waung, M., Hu, M., & Lu, F.** (2023). Cybersecurity and social media networks for donations: An empirical investigation of the triad of trust, commitment, and loyalty. *Journal of Retailing and Consumer Services, 71*, Article 103201. https://doi.org/10.1016/j.jretconser.2023.103201
13. **Lindström, C.** (2022). *Cybersecurity experiences and practices in charities* (Master's thesis). Retrieved from https://www.diva-portal.org/smash/get/diva2%3A1784358/FULLTEXT01.pdf
14. **NATO Cooperative Cyber Defence Centre of Excellence.** (2012). *National cyber security framework manual.* CCDCOE Publications.
15. **Norwegian Refugee Council (NRC).** (2020). *Annual report 2020.* Retrieved from https://www.nrc.no
16. **Pfleeger, C. P., & Pfleeger, S. L.** (2012). *Analyzing computer security: A threat/vulnerability/countermeasure approach.* Prentice Hall.
17. **Rohde, R. A., & Shapiro, B. A.** (2000). Information security management in non-profit organizations: Issues and strategies. *The Nonprofit Quarterly, 7*(4), 10–17.
18. **Stahl, B. C., Doherty, N. F., & Shaw, M.** (2012). Information security policies in the UK healthcare sector: A critical evaluation. *Information Systems Journal, 22*(1), 77–94. https://doi.org/10.1111/j.1365-2575.2011.00379.x
19. **Van de Walle, B., Van Den Eede, G., & Muhren, W.** (2009). *Humanitarian information management and systems.* Springer. Retrieved from https://www.researchgate.net/publication/221536592_Humanitarian_Information_Management_and_Systems
20. **Von Solms, R., & Van Niekerk, J.** (2013). From information security to cyber security. *Computers & Security, 38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004
21. **Whitman, M. E., & Mattord, H. J.** (2017). *Principles of information security* (6th ed.). Cengage Learning.
22. **World Economic Forum.** (2021). *The global risks report 2021* (16th ed.). Retrieved from https://www.weforum.org/reports/the-global-risks-report-2021
23. محاضرات الدكتور راتب البلخي في طرائق البحث العلمي.
24. محاضرات الأستاذ الدكتور طلال عبود في التحليل الإحصائي المتقدم.

الاستبانة

عزيزي المشارك/عزيزتي المشاركة، نشكرك على تخصيص وقتك للمشاركة في هذا الاستبانة، الذي يهدف إلى دراسة دور نظم إدارة أمن المعلومات (ISMS) في تعزيز الثقة والمصداقية داخل منظمة المجلس النرويجي للاجئين. استجابتك ستسهم في تقديم رؤى مهمة حول فعالية هذه النظم وتأثيرها على العمليات المختلفة في المنظمة. يرجى العلم بأن إجاباتك ستكون سرية ولن تستخدم إلا لأغراض البحث العلمي.

رابط الاستبانة: https://forms.office.com/e/bCu4yspyxr

الشكل رقم 5: رمز الاستجابة السريعة (QR Code) للاستبانة

المصدر: من إعداد الباحث باستخدام برنامج مايكروسوفت فورمز

البيانات الشخصية (اختياري)

1. **الوظيفة:**
   - مدير إداري
   - موظف في قسم تكنولوجيا المعلومات
   - موظف في قسم البرامج
   - موظف آخر
2. **مدة العمل في المجلس النرويجي للاجئين:**
   - أقل من سنة
   - 1-3سنوات
   - 3-5سنوات
   - أكثر من 5 سنوات

3. **هل سبق لك التعامل مع نظم إدارة أمن المعلومات (ISMS) في عملك؟**
   - نعم
   - لا

المحاور الرئيسية للاستبانة

#	المحور الأول: واقع نظم إدارة أمن المعلومات (ISMS) في المجلس النرويجي للاجئين	غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة
		1	2	3	4	5
1	هناك نظام لإدارة أمن المعلومات (ISMS) مطبق بشكل كامل داخل المجلس النرويجي للاجئين.					
2	إدارة المنظمة تلتزم بتطبيق سياسات أمن المعلومات بشكل دائم.					
3	تتوفر الموارد التقنية والمالية الكافية لدعم تطبيق نظام إدارة أمن المعلومات (ISMS) في المجلس.					
4	يتلقى موظفو المجلس تدريبًا دوريًا على أفضل الممارسات في أمن المعلومات.					
5	الموظفون يتبعون بدقة إرشادات أمن المعلومات في التعامل مع البيانات الحساسة.					
6	هناك قنوات اتصال واضحة للإبلاغ عن الحوادث الأمنية أو انتهاكات نظام إدارة أمن المعلومات (ISMS).					
7	تطبيق نظم إدارة أمن المعلومات يساهم في الحد من التهديدات السيبرانية التي تواجه المنظمة.					

الجدول رقم 15: محور الاستبانة الأول
المصدر: من إعداد الباحث

#	المحور الثاني: دور نظم إدارة أمن المعلومات في حماية البيانات الحساسة	غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة
		1	2	3	4	5
1	نظام إدارة أمن المعلومات (ISMS) يحمي البيانات الحساسة داخل المجلس النرويجي للاجئين بشكل فعال.					
2	تطبيق نظم إدارة أمن المعلومات يساهم في تقليل مخاطر تسريب أو اختراق البيانات الحساسة.					
3	الموظفون في المجلس النرويجي للاجئين مدربون بشكل كافٍ على تطبيق إجراءات أمن المعلومات لحماية البيانات الحساسة.					
4	التعامل مع التقارير أو الحوادث المتعلقة بأمن المعلومات داخل المنظمة يتم بجدية كافية.					

الجدول رقم 16: محور الاستبانة الثاني

المصدر: من إعداد الباحث

#	المحور الثالث: دور نظم إدارة أمن المعلومات في تعزيز المساعدات المقدمة من المانحين	غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة
		1	2	3	4	5
1	تطبيق نظم إدارة أمن المعلومات يؤثر بشكل إيجابي على ثقة المانحين في المجلس النرويجي للاجئين.					
2	المانحون يقدمون مساعدات أكبر للمجلس نتيجة تطبيق نظم إدارة أمن المعلومات.					
3	نظم إدارة أمن المعلومات تساهم في زيادة حجم المساعدات المقدمة للمجلس النرويجي للاجئين.					
4	هناك متطلبات أمنية إضافية من قبل المانحين تتأثر بشكل إيجابي بتطبيق نظم إدارة أمن المعلومات في المجلس.					

الجدول رقم 17: محور الاستبانة الثالث

المصدر: من إعداد الباحث

#	المحور الرابع: دور نظم إدارة أمن المعلومات في استمرارية العمل والقدرة على الاستجابة للأزمات	غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة
		1	2	3	4	5
1	نظم إدارة أمن المعلومات تساهم بشكل كبير في استمرارية العمل داخل المجلس النرويجي للاجئين.					
2	تطبيق نظم إدارة أمن المعلومات يعزز قدرة المجلس النرويجي للاجئين على الاستجابة للأزمات الدولية بشكل فعال.					
3	وجود نظم إدارة أمن المعلومات يقلل من التحديات اللوجستية التي تواجه المنظمة في بيئات الأزمات.					
4	تطبيق نظم إدارة أمن المعلومات يقلل من احتمالية توقف الأنظمة أو تسريب البيانات خلال الأزمات.					

الجدول رقم 18: محور الاستبانة الرابع
المصدر: من إعداد الباحث

نشكرك على إسهامك في هذا البحث. استجاباتك ستكون ذات قيمة كبيرة في فهم دور نظم إدارة أمن المعلومات في تعزيز الثقة والمصداقية وتحسين العمل داخل المجلس النرويجي للاجئين.