Information Security (GRC) simplified Concept

الدليل المبسط لمفهوم
الحوكمة وإدارة المخاطر والالتزام
في مجال أمن المعلومات

v.1-2022

المحتويات

المقدمة

Wanis M. Alkhamali

Senior CyberSecurity Risk Specialist|GRC-P/A | ISO27005LRM|ISO27001LI |PRINCE2|COBIT20...

دليل شامل و مبسط لشرح مفهوم الـ (GRC) من منظور أمن المعلومات والتي تعني حوكمة تكنولوجيا المعلومات وإدارة المخاطر السيبرانية والالتزام والامتثال للتشريعات الوطنية وهو موجه للمهتمين بهذا المجال من الفرق المختصه والاطراف المعنيه بالتطبيق لفتح أفق اوسع ورفع الثقافه والادراك لتحقيق أفضل النتائج المرجوة من تطبيق حوكمة تكنولوجيا المعلومات وإدارة وتقييم المخاطر المعلوماتية وتحقيق الالتزام بالتشريعات والتنظيمات الوطنية . .

م / ونيس محمد الخمعلي

شهادة الماجستير في أمن المعلومات

أخصائي أول مخاطر الأمن السيبراني

مفهوم GRC من منظور الأمن المعلوماتي

GRC حسب تعريف منظمة ISACA الامريكية

GOVERNANCE, RISK AND COMPLIANCE

GRC is an integrated assurance process

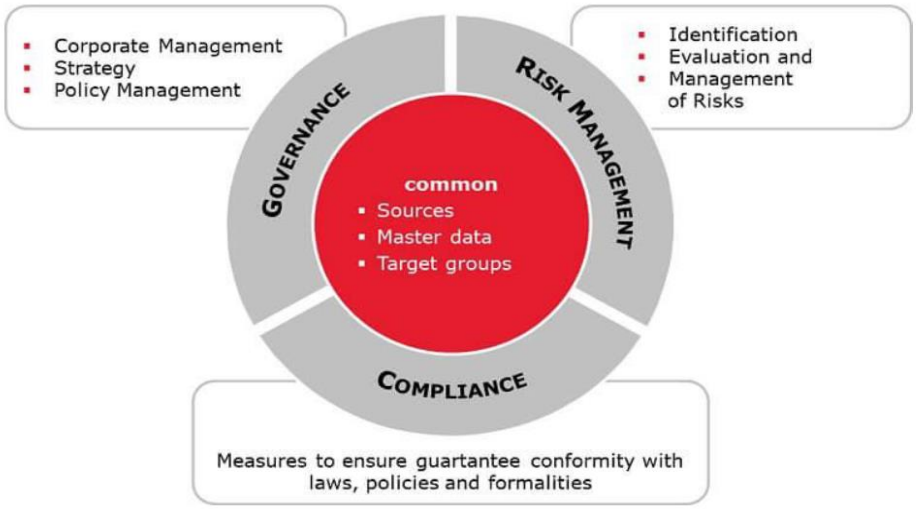
Convergence can exist independently across different business functions

Information security is often a part of GRC

ISACA

تعريف الحوكمة والمخاطر والالتزام GRC

GRC - DEFINITION



GRC هو اختصار مكون من ثلاثة أحرف، يرمز إلى "الحوكمة" و"المخاطر" و"الامتثال". فهي مجموعة متكاملة من الممكنات التي تجعل المنظمة قادرة على تحقيق الأهداف بشكل موثوق ومعالجة عدم اليقين والعمل بنزاهة. هذا العلم جديد على ساحة الأمن السيبراني حيث كان يستخدم بداية في الاعمال المالية والقانونية تم ابتكاره من قبل مجموعة تسمى OPEN COMPLIANCE AND ETHICS GROUP في عام 2007.وقد تزايد الاهتمام بهذا المدخل، الذي يضم بين جنباته ثلاثة مفاهيم معا، بعد الأحداث التي عصفت بالعالم إبان الأزمة المالية العالمية، ثم تصاعد أكثر مع أزمة انتشار فيروس كوفيد - 19، وتصاعد الهجمات الإلكترونية، ما عزز مشكلة عدم القين وأصبحت ظاهرة عالمية عامة. لذا، يطالب أصحاب المصلحة بمستويات عالية من الشفافية وآليات لمعالجة المخاطر والسيطرة على الظروف. ورغم أن مفاهيم الحوكمة تغطي مسائل مثل الشفافية، وإدارة المخاطر تغطي التهديدات والفرص، لكن بقيت هذه القضايا تعمل بشكل غير متزامن، ولهذا فإن مفهوم "الحوكمة" و"المخاطر" و"الامتثال"، يعني التناغم والتزامن بين حوكمة الشركات، وبرامج إدارة الأداء، وإدارة المخاطر، وأدوات مراقبة الامتثال، ونشاط المراجعة الداخلية، وأمن المعلومات، وقضايا المسؤولية الاجتماعية للشركات.

نظرة حول مهام الحوكمة والمخاطر والالتزام

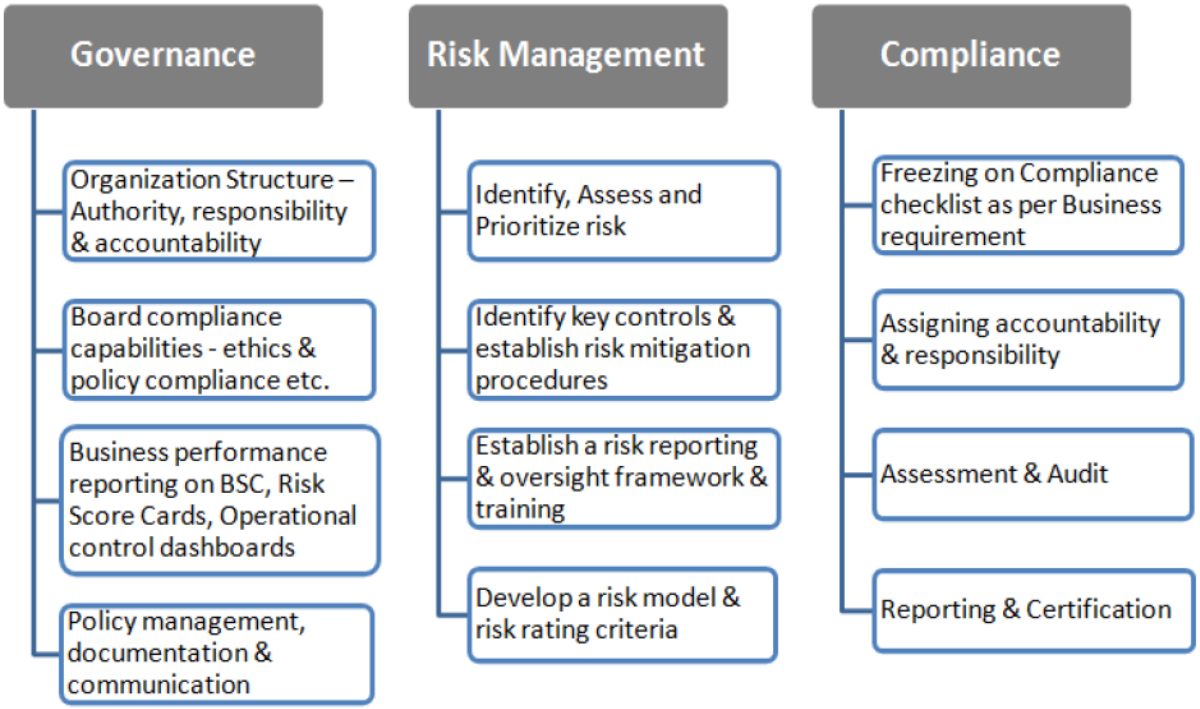
حوكمة جميع المهام والعلمليات لتتوافق مع الاهداف بشكل متوائم واطلاع الادارات العلياء على المخاطر الرئيسية واتخاذ ما يلزم لمعالجتها .

تحديد وتحليل وقياس المخاطر من خلال منهجية مخاطر معتمدة في المنظمة .

فهم الموارد وتخصيصها بكفاءة لتلبية المتطلبات التنظيمية والتأكد بالدليل من التزام الجهة لجميع التشريعات المعتمدة

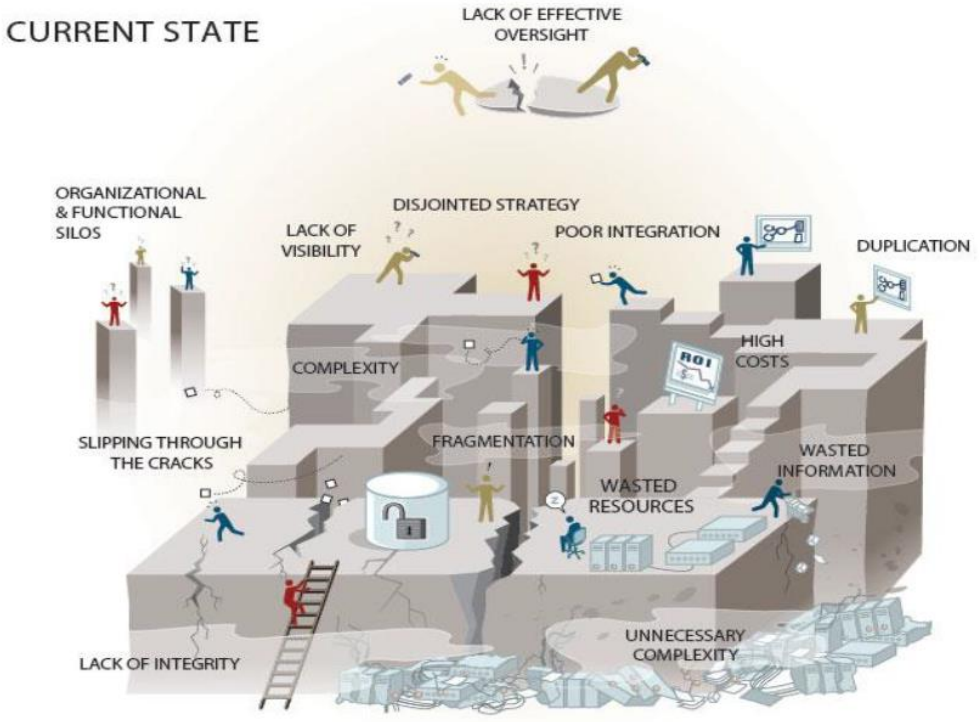
الأهداف الرئيسية للحوكمة – إدارة المخاطر – الالتزام

GRC - OBJECTIVES



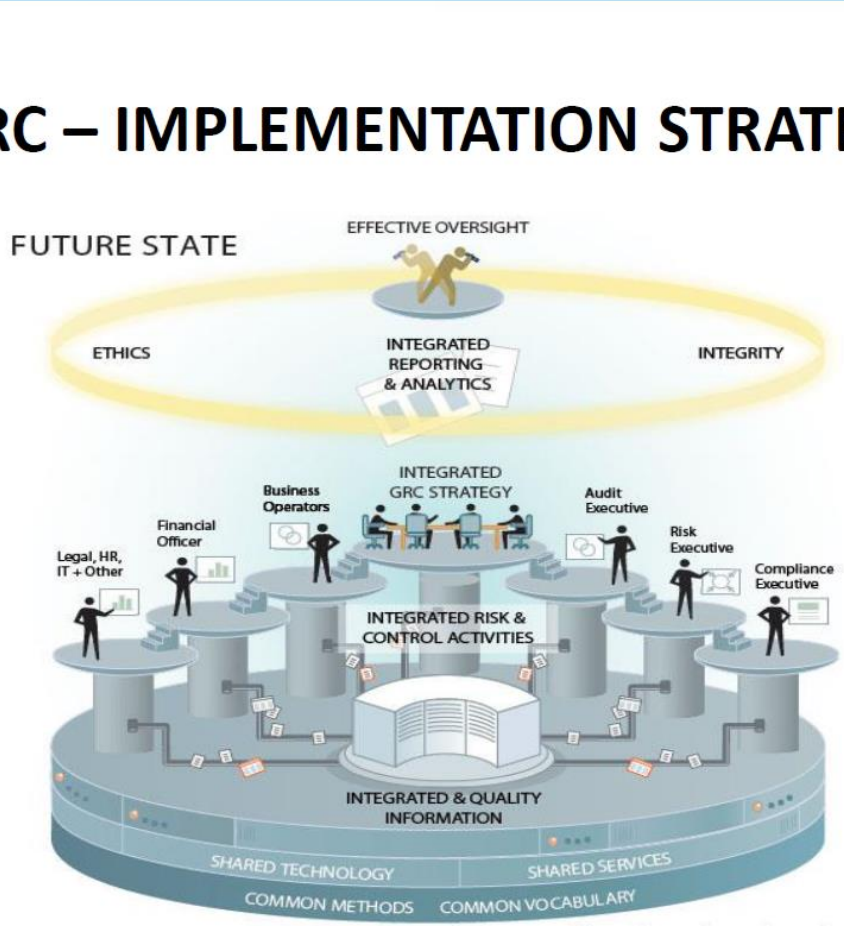
حالة المنظمات بدون تطبيق ال GRC

GRC – IMPLEMENTATION RISKS



- ضعف في فاعلية المراقبة والمتابعة
- ضبابية في الاستراتيجية
- ضعف في الرؤية
- عدم وجود تكامل بين الأنظمة والعمليات
- ضياع للمعلومات والجهد والموارد
- تكرار لنفس العلمليات

أهمية تطبيق GRC بشكل سليم في المنظمات



- رؤية واضحة لمهام واهداف المنظمة
- ممارسات وأخلاقيات عمل سليمة وصحية
- تكامل وفاعلية بين فرق العمل المختلفة
- استراتيجية واضحة ومتكاملة
- جودة في أداء الاعمال وانجاز وتنفيذ حسب الخطط
- مشاركة للمعلومات وتطور سريع في المهارات
- استغلال امثل للموارد البشرية والتقنية

أهمية التكامل والفوائد من تطبيقها على استراتيجية المنظمات

GRC – IMPLEMETATION STRATEGY

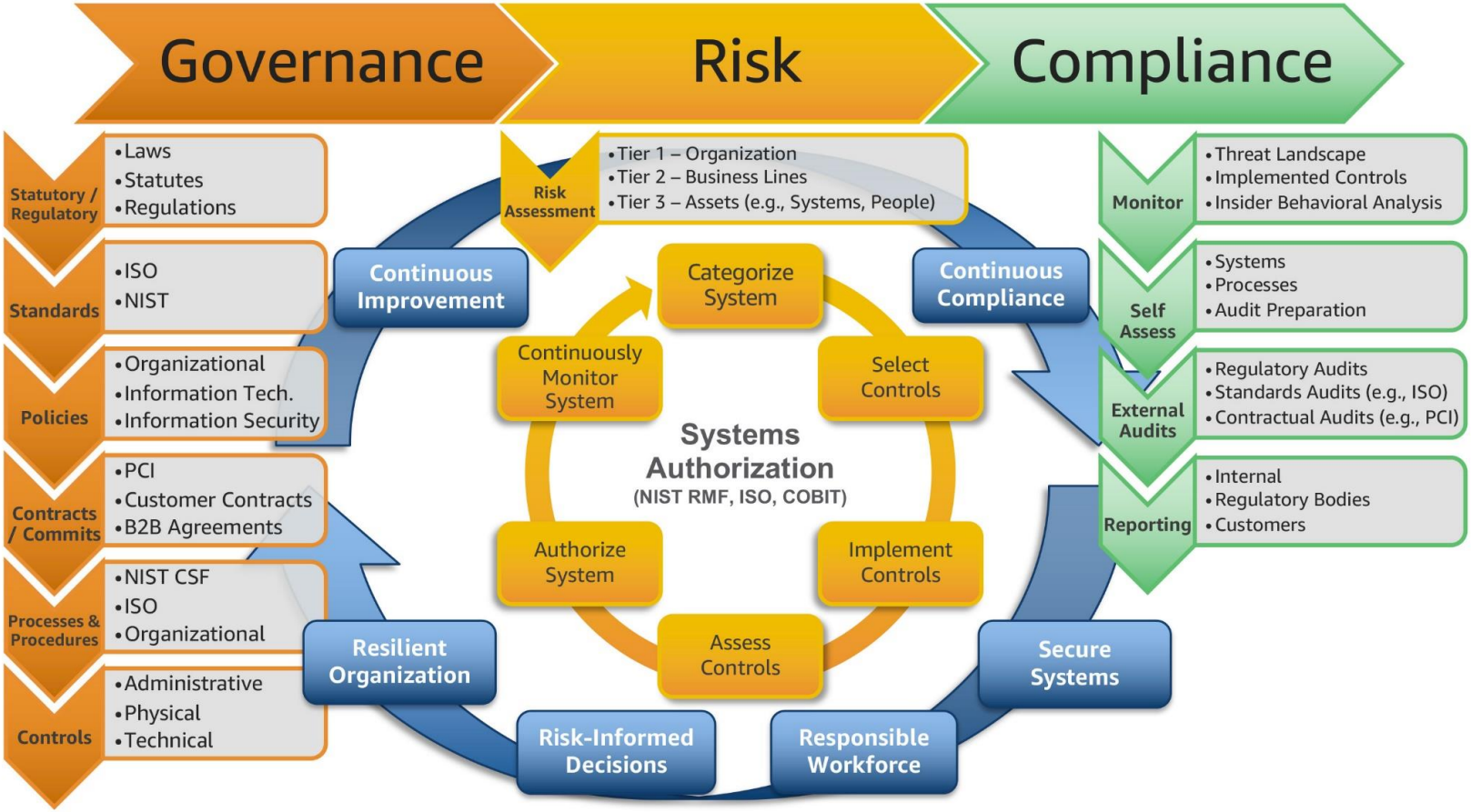
- Integrating GRC capabilities does not mean creating a mega-department of GRC and doing away with decentralised management.

- Establishing an approach that ensures:
  - the right people get the right information at the right times;
  - the right objectives are established;
  - the right actions and controls are put in place to address uncertainty and act with integrity.

- Benefits of implementing GRC correctly:
  - Reduced costs
  - Reduced duplication of activities
  - Reduced impact on operations
  - Achieved greater information quality
  - Achieved greater ability to gather information quickly and efficiently
  - Achieved greater ability to repeat processes in a consistent manner

عمليات الحوكمة والمخاطر والالتزام GRC Process

الحوكمة والمخاطر والامتثال (GRC) هي طريقة مهيكلة الغرض منها هو توفيق تكنولوجيا المعلومات مع أهداف العمل وفي الوقت نفسه إدارة المخاطر واستيفاء متطلبات جميع اللوائح الصناعية والحكومية.



ملخص مفهوم ال GRC

GRC - SUMMARY

Information Security Governance حوكمة أمن المعلومات

مفهوم الحوكمة بشكل عام

وفقا لـ Harvard Business review فإن الحوكمة هي مجموعة القواعد والقوانين والاسس التي تضبط عمل المنظمات وتحقق الرقابة الفعالة على مجلس إدارتها ، وتنظم العلاقة بينها وبين أصحاب المصلحة ، وذلك في سبيل تحقيق الشفافية والعدالة ومكافحة الفساد .

تعرف " مؤسسة التمويل الدولية " (IFC) الحوكمة بأنها نظام يتم من خلاله إدارة الشركات والمنظمات والتحكم في أعمالها ، أما منظمة التعاون الاقتصادية والتنمية (OECD) فتعتبر بأن الحوكمة مجموعة من العلاقات التي تربط بين القائمين على إدارة المنظمة ومجلس الادارة واصحاب المصلحة .

الفرق بين الحوكمة والادارة

GOVERNANCE VS. MANAGEMENT

Governance

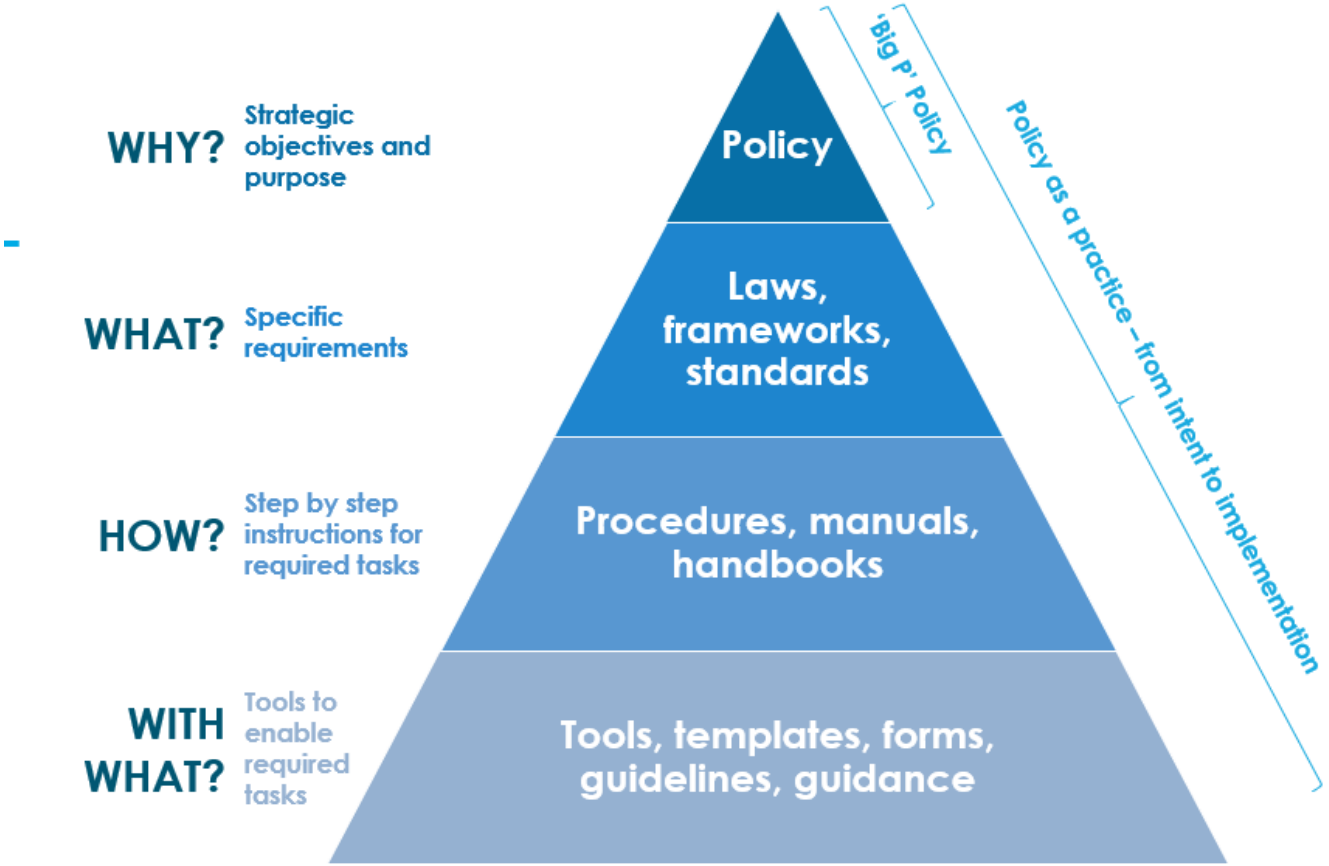
- Purpose is to set goals

“Do the right thing”

Management

- Purpose is plan, build, execute and monitor activities to achieve goals
- “Do the thing right”

Governance Hierarchy هرمية الحوكمة

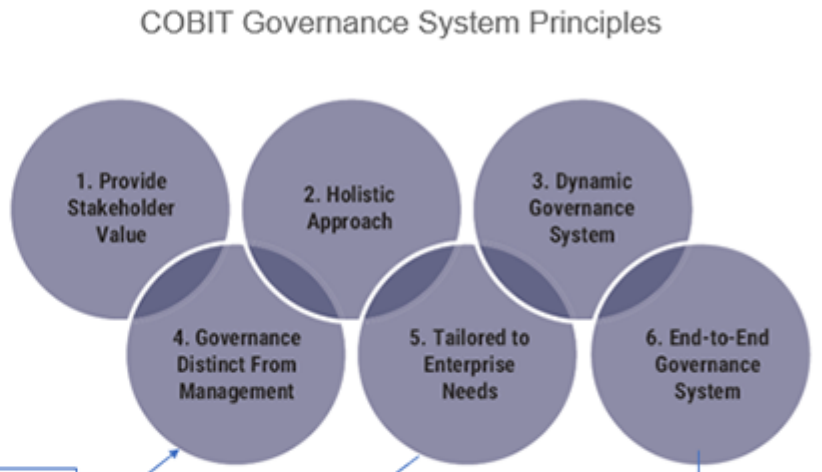


مبادئ ومفاهيم نظام الحوكمة

2 The board should ensure that key stakeholders are identified and, where appropriate, stakeholder feedback is regularly solicited to evaluate whether corporate policies meet key stakeholders' needs and expectations.

3 Board members should act in the best interest of the company and the shareholders while balancing the interests of other key external and internal stakeholders.

4 The board should ensure that the company maintains a sustainable strategy focused on long-term performance and value.

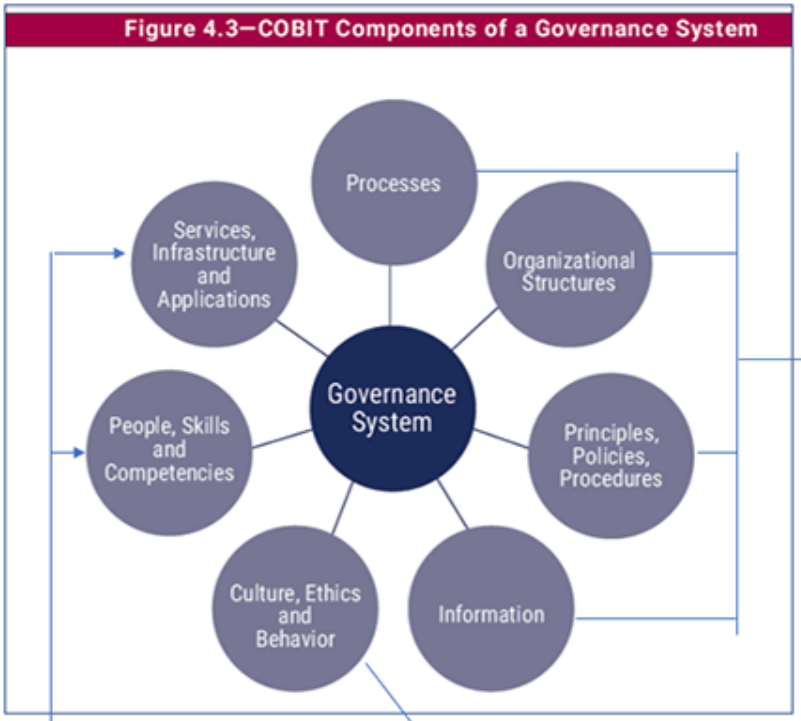


There should be a clear form of leadership for the board that is distinct from management.

Corporate governance does not allow for a one-size-fits-all approach. Organizations need to find their own best practices based on the organization's characteristics.

1 Effective corporate governance requires regular and constructive interaction among key stakeholders, the board, management, internal audit, legal counsel, and external audit and other advisors.

عناصر ومكونات نظام الحوكمة

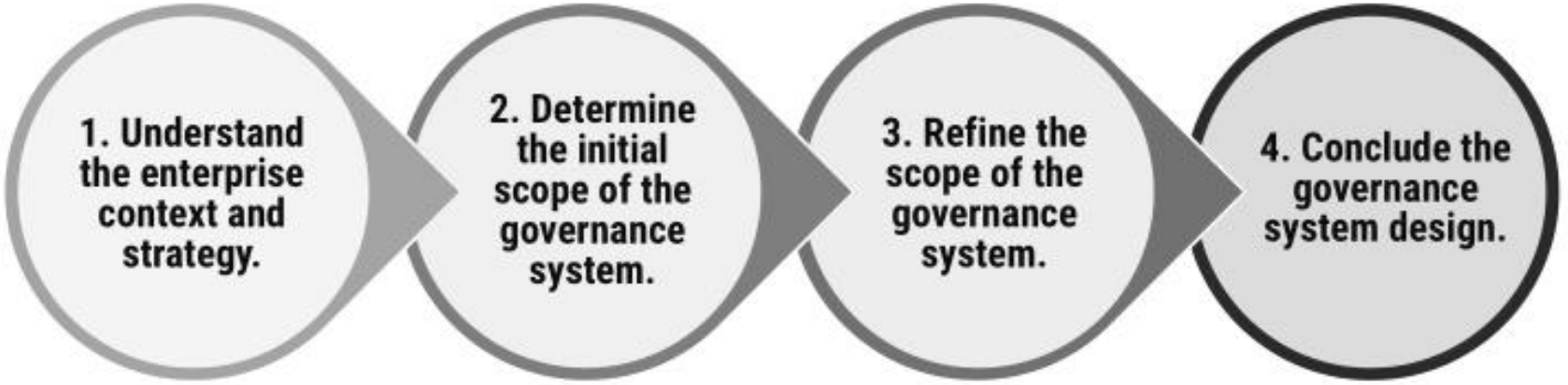


6 The board should ensure that structures and practices exist and are well-governed so that it receives timely, complete, relevant, accurate, and reliable information to perform its oversight effectively.

4 Ensuring that all employees receive adequate training.

5 The board should ensure that the culture of the organization is healthy, regularly monitor and evaluate the organization's core culture and values, assess the integrity and ethics of senior management, and, as needed, intervene to correct misaligned corporate objectives and culture.

مخطط تصميم نظام الحوكمة



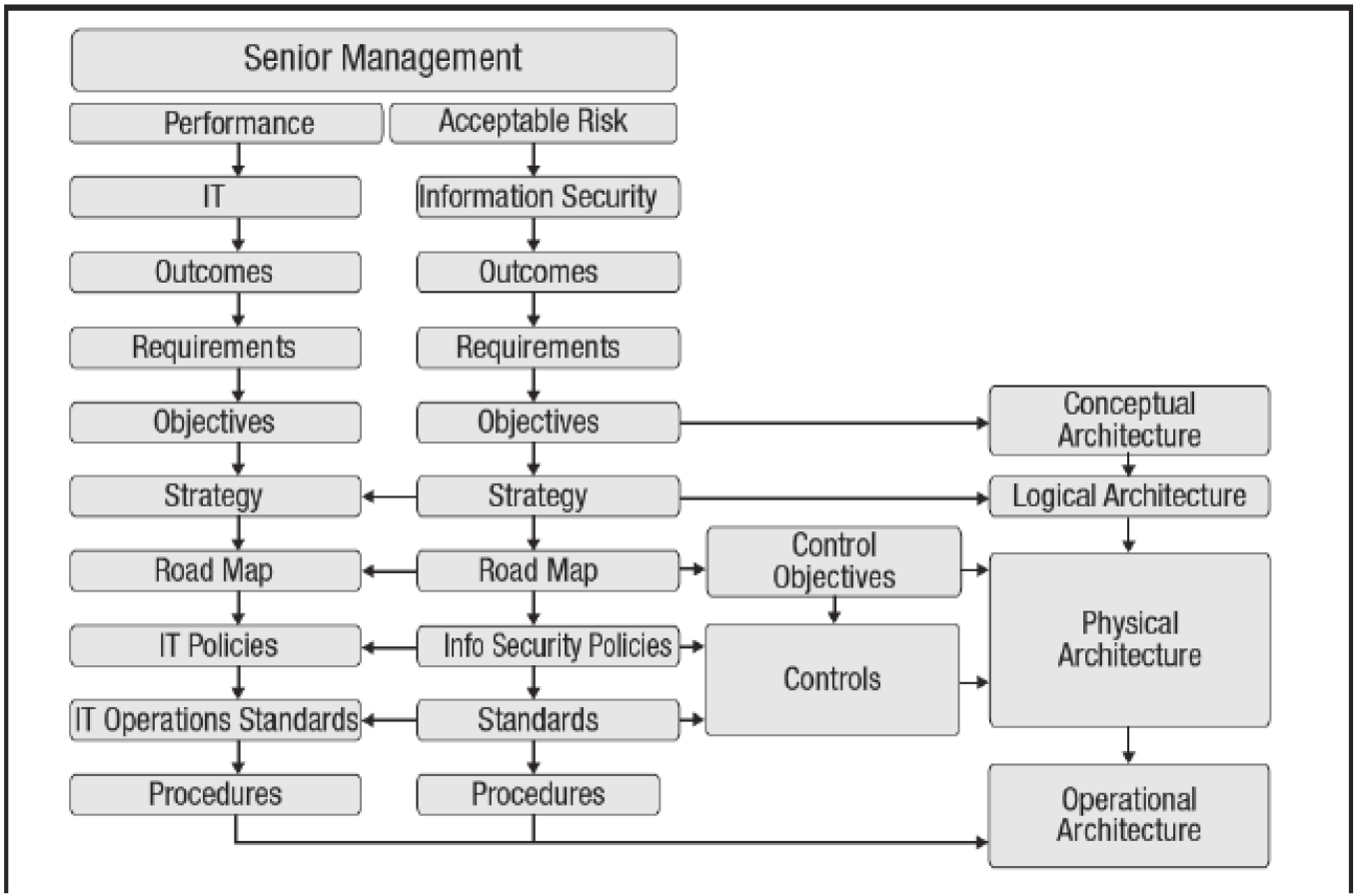
- 1.1 Understand enterprise strategy.
- 1.2 Understand enterprise goals.
- 1.3 Understand the risk profile.
- 1.4 Understand current I&T-related issues.

- 2.1 Consider enterprise strategy.
- 2.2 Consider enterprise goals and apply the COBIT goals cascade.
- 2.3 Consider the risk profile of the enterprise.
- 2.4 Consider current I&T-related issues.

- 3.1 Consider the threat landscape.
- 3.2 Consider compliance requirements.
- 3.3 Consider the role of IT.
- 3.4 Consider the sourcing model.
- 3.5 Consider IT implementation methods.
- 3.6 Consider the IT adoption strategy.
- 3.7 Consider enterprise size.

- 4.1 Resolve inherent priority conflicts.
- 4.2 Conclude the governance system design.

Relationship between العلاقة بين عناصر ومكونات الحوكمة Governance elements



مخرجات حوكمة أمن المعلومات

OUTCOMES OF INFORMATION SECURITY GOVERNANCE

Six basic outcomes of a security program:

- Strategic alignment
- Risk management
- Value delivery
- Resource optimization
- Performance measurement
- Assurance process integration

اشهر شهادات الحوكمة المعلوماتية

ما هو إطار كوبت ((COBIT؟

هو إطار عمل تم إنشاؤه بواسطة منظمة التدقيق والرقابة على نظم المعلومات (ISACAالإدارة وحوكمة تقنية المعلومات داخل المؤسسات، حيث تعتبر الحوكمة الفعالة لتقنية المعلومات أمر بالغ الأهمية وأساس نجاح الأعمال.

يعرف إطار العمل كوبيت (COBIT): بأنه إطار حوكمة تقنية المعلومات المعترف به دوليا، ويسمى أيضا الإطار/ النموذج المرجعي، للأمن ولضمان استغلال تقنية المعلومات بالشكل الأمثل، يستخدم لتحسين أداء الأعمال بإطار متوازن لخلق قيمة لتقنية المعلومات وخفض المخاطر المحتملة منها.

يتكون من مجموعة من الممارسات والعمليات الراسخة والمقبولة (مع كل عملية يتم تحديد المدخلات والمخرجات للعملية، وأنشطة العملية الرئيسية، وأهداف العملية، ومقاييس الأداء، ونموذج نضج القدرة) لتضمن أن تقنية المعلومات المستخدمة داخل المنشآت تغطي أهداف العمل، وأن الموارد تستخدم بشكل جيد، وأن المخاطر يتم رصدها بشكل كافٍ.

سعر أمتحان الشهادة : 175دولار

رابط الدخول على الموقع : https://www.isaca.org/credentialing/cobit-foundation#schedule

إدارة مخاطر أمن المعلومات
Information Security Risk Management

What is Information Security Risk Concept
ماهو مفهوم المخاطر المعلوماتية

- **Information security risk is the probability of exposure or loss resulting from a cyber attack or data breach on your organization**

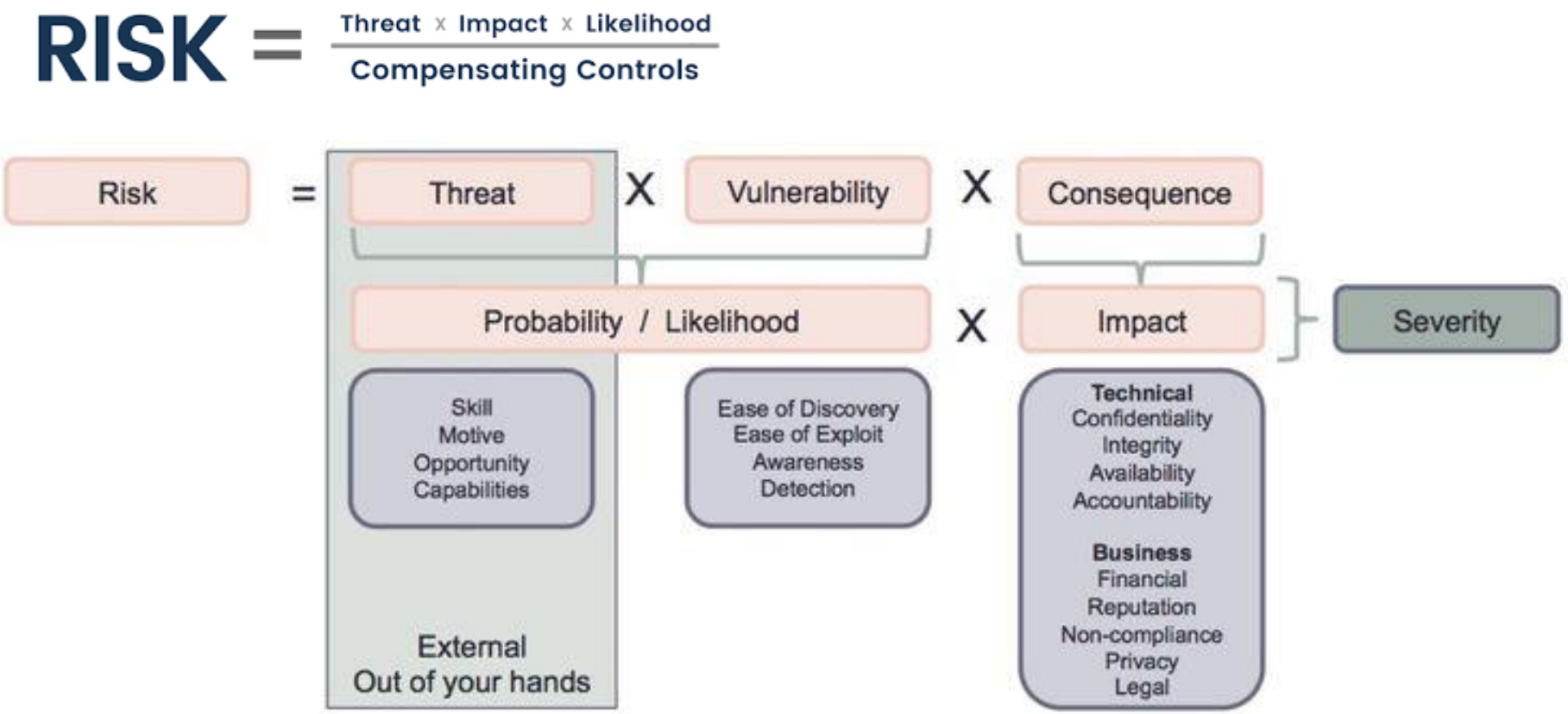
المخاطر المعلوماتية : هي حالة من الشك لاحتمالية تعرض البيانات او المعلومات للكشف أو التعديل او الحجب وعدم التوفر نتيجة لهجوم سيبراني أو وصول غير مصرح به لبيانات في المنظمة من خلال طرف خارجي أو داخلي عمدا أو من غير قصد بواسطة استغلال ضعف معين .

When Information Risk appear ؟ المعلوماتية متى تتكون المخاطر

إذا توفرت العناصر الأساسية الثلاث للخطر

- أصل حساس (ذو قيمة)
- تهديد (مؤثر حقيقي)
- ثغرات (نقاط ضعف)

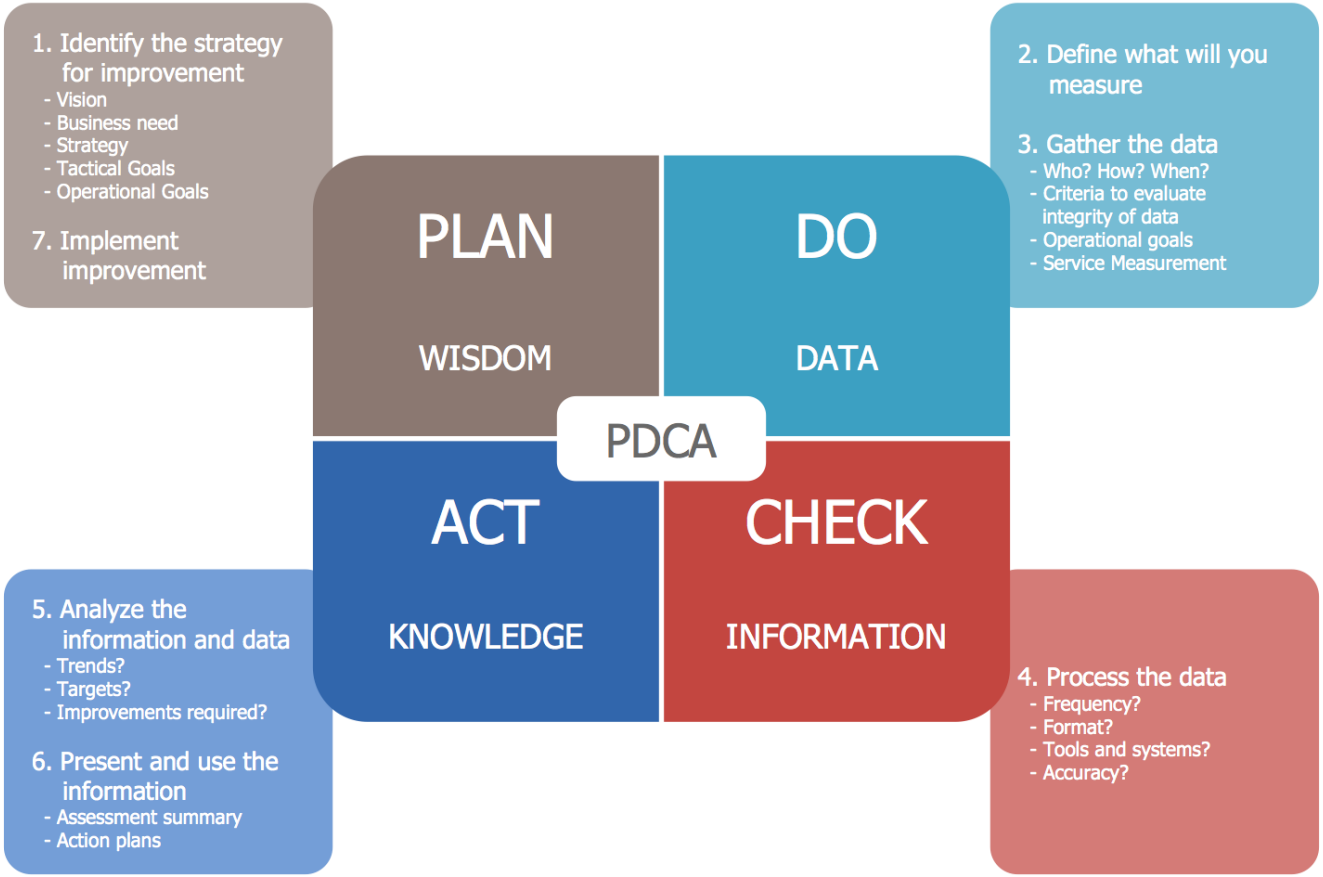
معادلة حساب قيمة المخاطر المعلوماتيه



مصطلحات هامة

	Vulnerability	Threat	Risk
Definition	Weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset.	Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.	The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability.

نموذج PDCA لعمليات تقييم المخاطر المعلوماتيه



أنواع تحليل المخطر المعلوماتيه

- Helps an entity identify risks & potential threats to its processes & operations
- Gives idea of their severity & likelihood of occurrence

TYPES

QUALITATIVE RISK ANALYSIS METHODS

1. **Bow Tie Analysis** – Spilt risk into two parts contributing factors and potential consequences
2. **The Delphi Technique** – Depends mainly on expert comments
3. **SWIFT Analysis** - Analyses how changes to new plan or design would impact potential project
4. **Fly Analysis** – Find causes and result of happening event

QUANTITATIVE RISK ANALYSIS METHODS

1. **Monte Carlo Simulation** - Determine chances of an event
2. **Decision Tree Analysis** - Graphical method where all possible scenarios are depicted visually
3. **Sensitivity Analysis** - Check impact of small change on final result
4. **Three-Point Estimate** -Estimation of cost and duration
5. **FMEA** – Failure modes and its determination

أشهر المنهجيات لعمليات تحليل المخاطر المعلوماتية

وفقا لـ PECB، فإن OCTAVE هي منهجية لتقييم المخاطر لتحديد وإدارة وتقييم مخاطر أمن المعلومات. تعمل هذه المنهجية على مساعدة المنظمة على:

- تطوير معايير تقييم المخاطر النوعية التي تصف مدى تحمل المنظمة للمخاطر التشغيلية

-تحديد الأصول التي تعتبر مهمة لمهمة المنظم

-تحديد نقاط الضعف والتهديدات التي تواجه تلك الأصول

-تحديد وتقييم العواقب المحتملة على المنظمة إذا تحققت التهديداتبدء إجراءات التحسين المستمر للتخفيف من المخاطر

According to the PECB , OCTAVE is a risk assessment methodology to identify, manage and evaluate information security risks. This methodology serves to help an organization to:

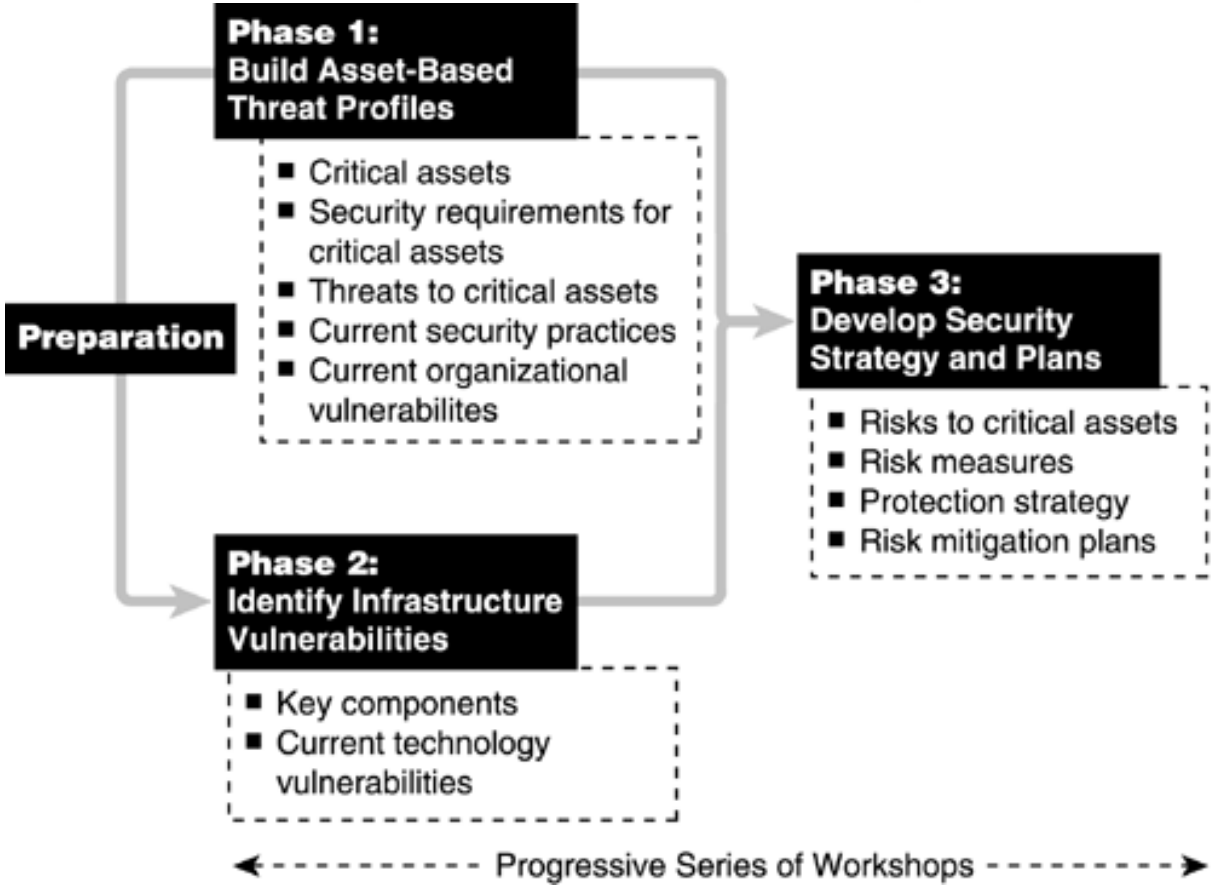
1- develop qualitative risk evaluation criteria that describe the organization's operational risk tolerances

2- identify assets that are important to the mission of the organization

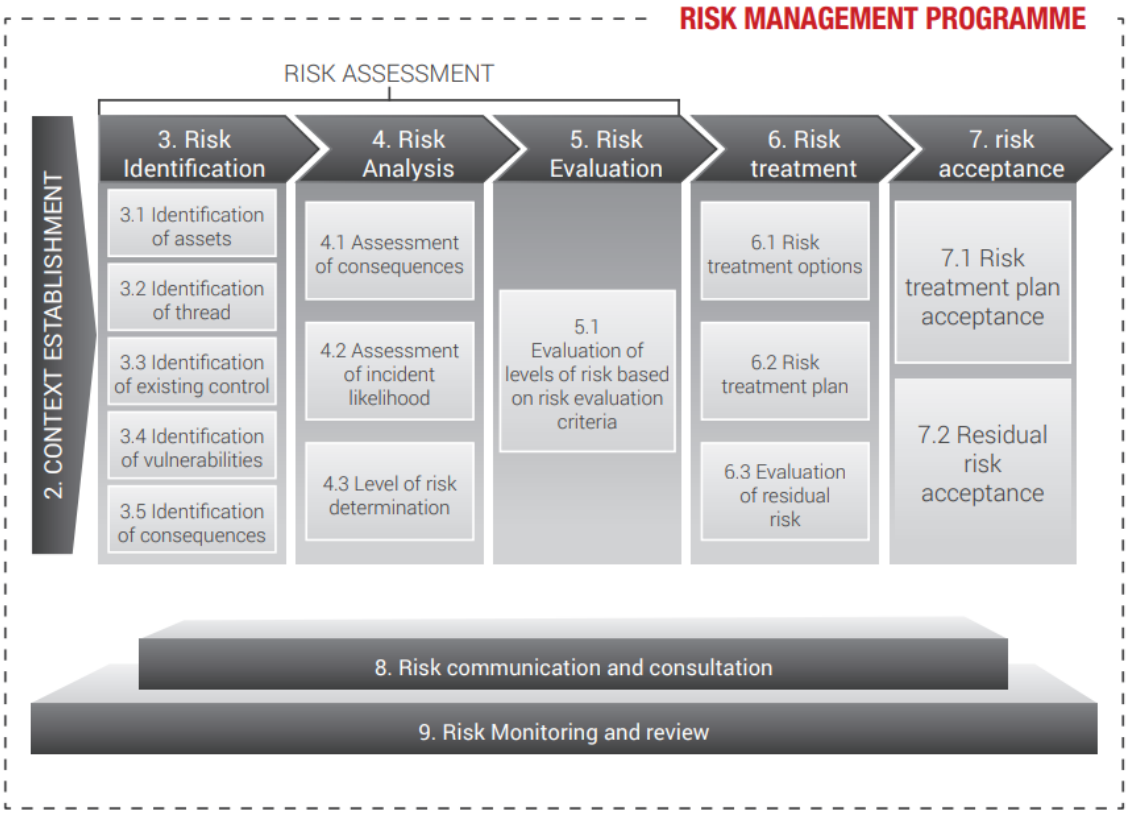
3- identify vulnerabilities and threats to those assets

4- determine and evaluate the potential consequences to the organization if threats are realized initiate continuous improvement actions to mitigate risks

The OCTAVE Method منهجية



إجراءات وعمليات تقييم المخاطر المعلوماتية



1- فهم السياق العام للمنظمة والخدمات

تحديد التقييم بمعرفة أهداف أعمال النطاق ومالكيها وأماكنها الجغرافية، و تحديد لأصول المعلومات المستخدمة لتخزين و/أو نقل و/أو تخزين المعلومات

ثم يتم تحديد الأطراف المعنية بتقييم مخاطر الأمن المعلوماتي بما فيه م مالكي الأصول والأوصياء على الأصول ومطبقي الضوابط على الأصول والخبراء وجميع المعنيين .

2- تحديد المخاطر المعلوماتية

1- تقييم الأصول التقنية

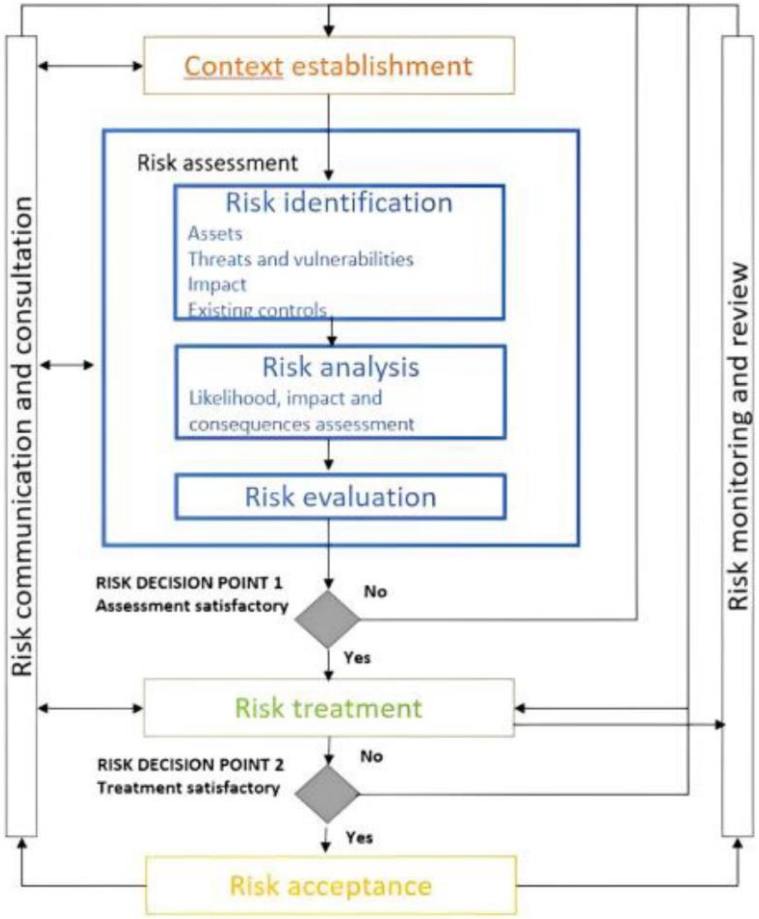
2- تقييم التهديدات

3- تقييم الضوابط الحالية

4- تقييم الثغرات

5- تقييم التأثير المحتمل في حال وقوع الخطر

شرح إجراءات وعمليات تقييم المخاطر المعلوماتية



- قياس وتقدير نسبة المخاطر

يتم تقدير المخاطر على مرحلتين:

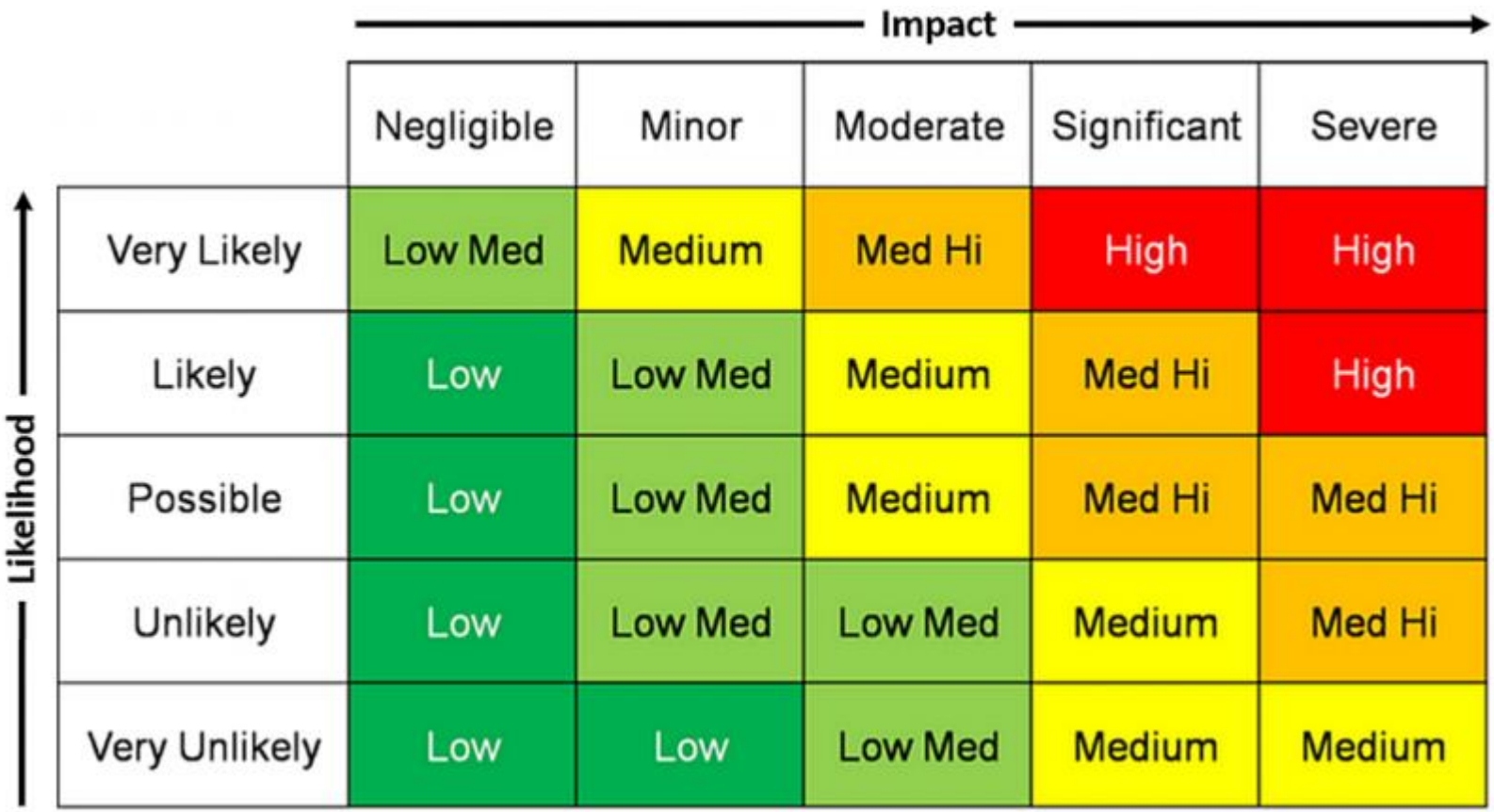
- درجة المخاطر الكامنة والأساسية Inherent Risk
- درجة المخاطر المتبقية Residual Risk

- معالجة المخاطر

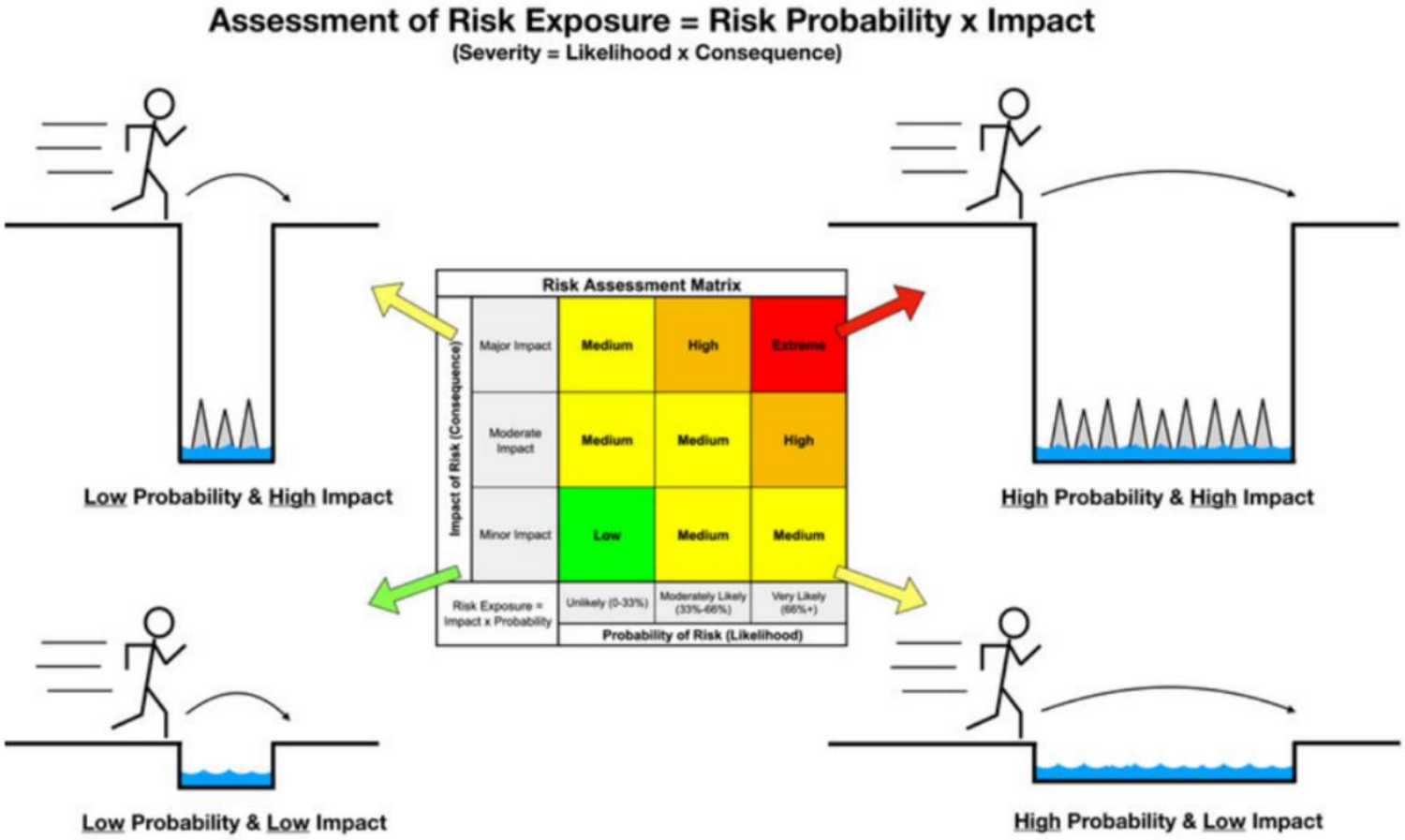
يتم معالجة المخاطر من خلال اربعة خيارات رئيسية :

- قبول
- تخفيف
- تحويل
- إنهاء

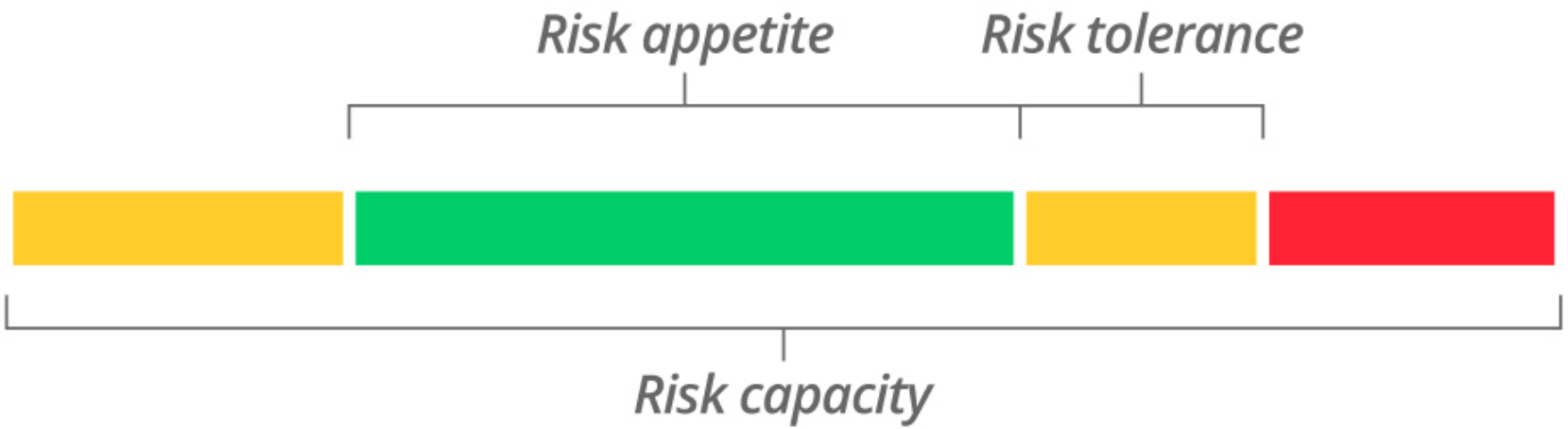
قياس وتقدير نسبة المخاطر من خلال Heat Map



شرح مبسط للتوضيح (Heat Map)

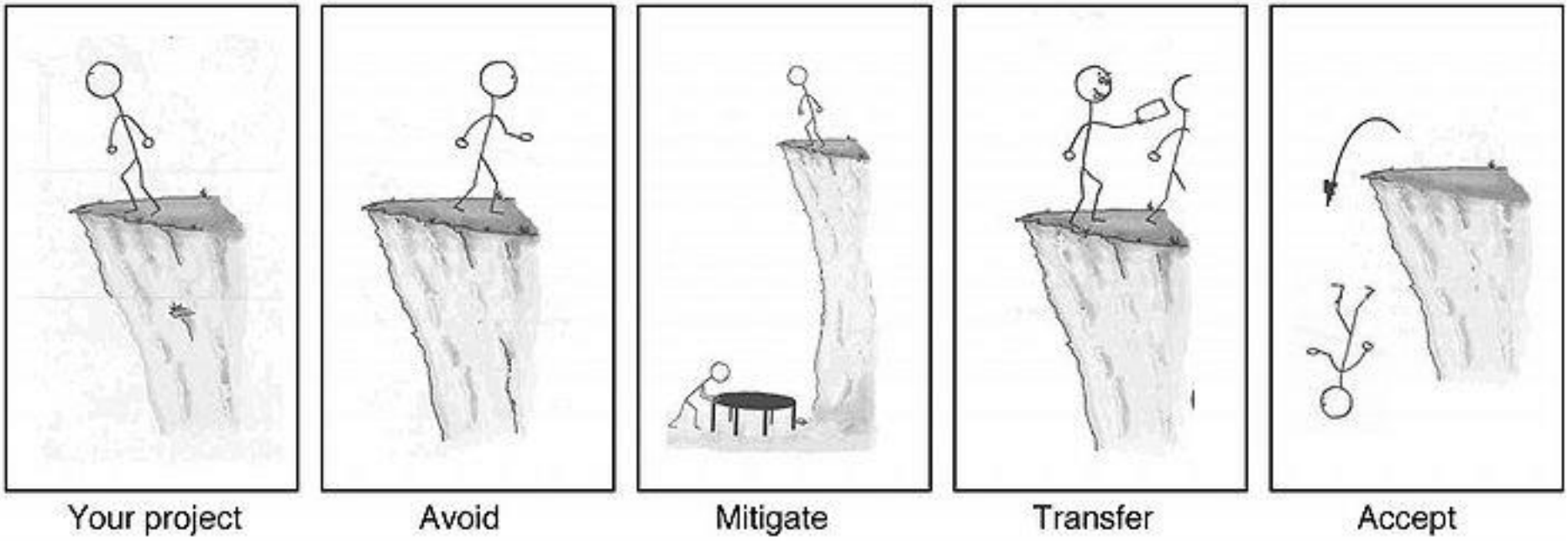


توضيح مبسط لمفهوم شهية المخاطرة

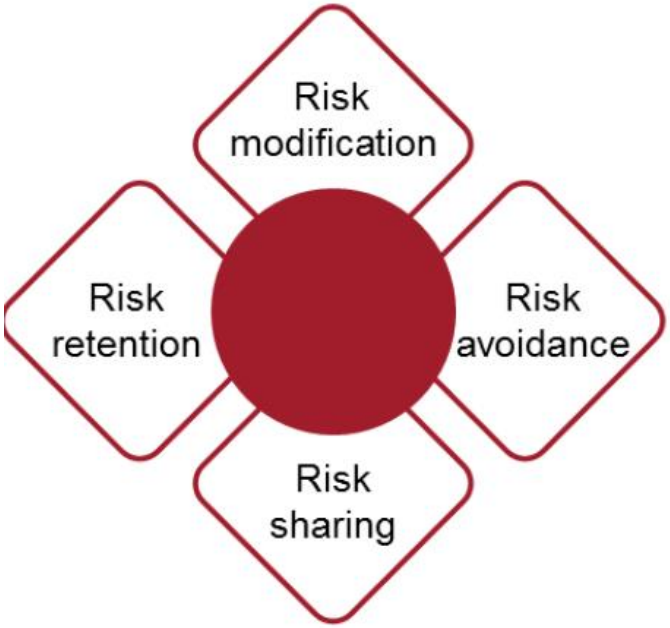


pirani

تبسيط لمفهوم خيارات المعالجة (Treatment Options)



شرح خيارات المعالجة لمخاطر أمن المعلومات



Risk modification

Introducing, removing or altering controls so that the residual risk can be reassessed as being acceptable

Risk avoidance

Cancellation or modification of an activity or set of activities related to risk

Risk retention

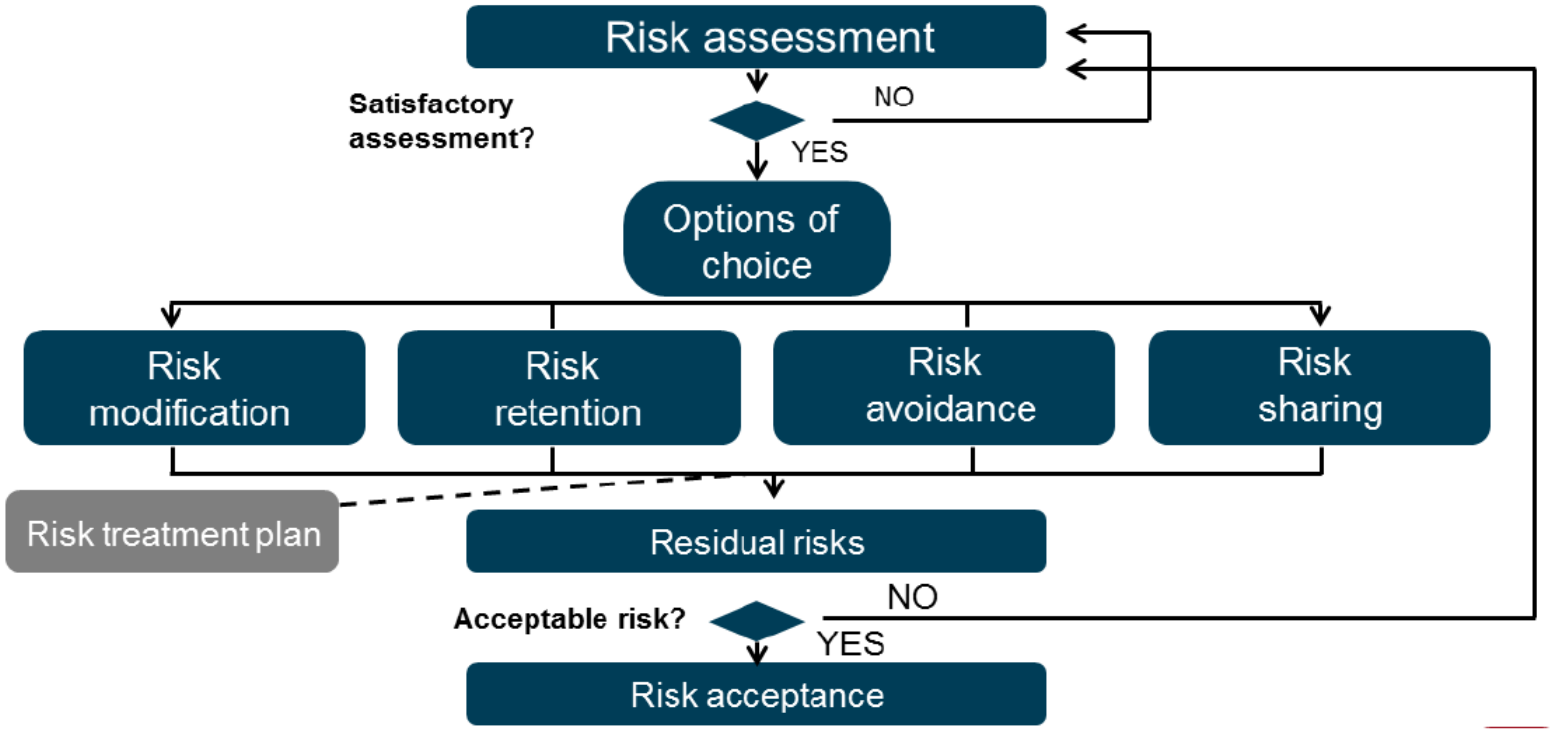
Decision to accept the actual level of risk

Risk sharing

Decision to share risks with external parties: insurance or outsourcing

عمليات معالجة مخاطر أمن المعلومات

Risk Treatment Activities



سجل المخاطر المعلوماتية

THE RISK REGISTER

Maintains the organization's overall risk profile

Includes:

- Summary of the risk based on threat type and associated event or actor
- Category and classification of the risk
- Risk owner

Also documents risk treatment choices

قالب سجل المخاطر

ACTIVITY: RISK REGISTER TEMPLATE

Part I—Summary Data				
Risk statement				
Risk owner				
Date of last risk assessment				
Due date for update of risk assessment				
Risk category	○ STRATEGIC (IT Benefit/Value Enablement)	○ PROJECT DELIVERY (IT Programme and Project Delivery)	○ OPERATIONAL (IT Operations and Service Delivery)	
Risk classification (copied from risk analysis results)	○ LOW	○ MEDIUM	○ HIGH	○ VERY HIGH
Risk response	○ ACCEPT	○ TRANSFER	○ MITIGATE	○ AVOID
Part II—Risk Description				
Title				
High-level scenario (from list of sample high-level scenarios)				
Part III—Risk Response				
Detailed scenario description—Scenario components	Actor			
	Threat Type			
	Event			
	Asset/Resource			
	Timing			
Other scenario information				

أشهر شهادات ادارة مخاطر أمن المعلومات

ISO 27005 Risk manger

- **ISO 27005 Risk manger**

تتيح الدورة التدريبية لمدير المخاطر الرئيسي
ISO/IEC 27005احيث أن اجتياز هذة الامتحان يؤكد على اكتساب الكفاءات
اللازمة لمساعدة المنظمة في إنشاء وإدارة وتحسين برنامج إدارة
مخاطر أمن المعلومات وتقييم المخاطر السيبرانية بشكل احترافي
استنادِا إلى إرشادات المعيار الدولي للمخاطر ISO/IEC 27005.

قيمة امتحان الشهادة ($500) دولار

رابط الدخول على موقع الامتحان: https://pecb.com/en/education-and-certification-for-individuals/iso-iec-27005/iso-iec-27005-risk-manager

أشهر شهادات ادارة مخاطر أمن المعلومات

CRISC from ISACA

- **CRISC from ISACA**

تمنح منظة ISACA الامريكية شهادة CRISC المعتمدة في إدارة المخاطر ونظم المعلومات لمختصين تقييم المخاطر الذين يحددون المخاطر ويديرونها من خلال تطوير وتنفيذ وصيانة ضوابط أنظمة المعلومات IS.

تم إطلاق شهادة CRISC في عام 2010 ، وهي معترف بها دوليا والحاصلين عليها أكثر من 17000 متخصص في تكنولوجيا المعلومات في جميع أنحاء العالم.

قيمة امتحان الشهادة (760$) دولار

رابط الدخول على موقع الامتحان: https://www.isaca.org/credentialing/crisc

Compliance الالتزام

تعريف الالتزام

يعرف بأنه مراجعة مفصلة وشاملة لوضع الأمن المعلوماتي والسيبراني للمنظمة ، بناءٍ على المعايير الدولية والمحلية مثل معايير الهيئة الوطنية للأمن السيبراني و البنك المركزي السعودي و ISOو PCI-DSSو COBITو GDPR وCyber Security Resilienceg، إلخ. يتطلب أي من هذه الأطر تحليلا منهجيا للمخاطر ، تحديد الضبط والتوثيق ، وكذلك مراقبةَ الامتثال والقياس. والتي يمكن استخدامها لتطوير واختبار خطط استمرارية الاعمال في الجهة .

إطار عمل الالتزام

COMPLIANCE - FRAMEWORK

إطار عمل إدارة الالتزام تعهد ب :

- ✓ الالتزام
- ✓ تنفيذ
- ✓ مراقبة
- ✓ وتطوير

أشهر المعايير والتشريعات الوطنية

1- الهيئة الوطنية للأمن السيبراني

- الضوابط الأساسية للأمن السيبراني
- ضوابط الأمن السيبراني للأنظمة الحساسة
- ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات
- وثيقة ضوابط الأمن السيبراني للعمل عن بعد
- ضوابط الأمن السيبراني للحوسبة السحابية
- وثيقة ضوابط الأمن السيبراني للأنظمة التشغيلية
- وثيقة ضوابط الأمن السيبراني للبيانات

2- هيئة الاتصالات وتقنية المعلومات

- الإطار التنظيمي للأمن السيبراني لمقدمي الخدمة في قطاع الاتصالات والفضاء والتقنية

3- مؤسسة النقد العربي السعودية (SAMA)

- إطار عمل الامن السيبراني الإلكتروني SAMA
- المعيار العالمي بأمان بيانات بطاقات الإئتمان

أهمية التنفيذ والالتزام بجميع الضوابط والتشريعات
The importance of implementation and compliance with all controls and legislation

تشير مواد الأنظمة والاوامر السامية على أنه يجب على جميع الجهات الحكومية وتشمل الوزارات والهيئات والمؤسسات والجهات والشركات التابعه لها وتطبق على جهات القطاع الخاص التي تمتلك بنى تحتية وطنية حساسة أو تقوم بتشغليها او استضافتها تنفيذ ما يحقق الالتزام الدائم والمستمر بهذة الضوابط وفقا لقابلية تطبيقها في الجهة بحسب طبيعة عملها .

The regulations and royal orders direct that all government agencies, including ministries, agencies, institutions, agencies and companies affiliated with them, must also be applied to private sector entities that own, operate, or host sensitive national infrastructure, implementing what achieves permanent and ongoing compliance with these controls according to their applicability. In the region, according to the nature of the work.

نموذج خطوط الدفاع الثلاثة

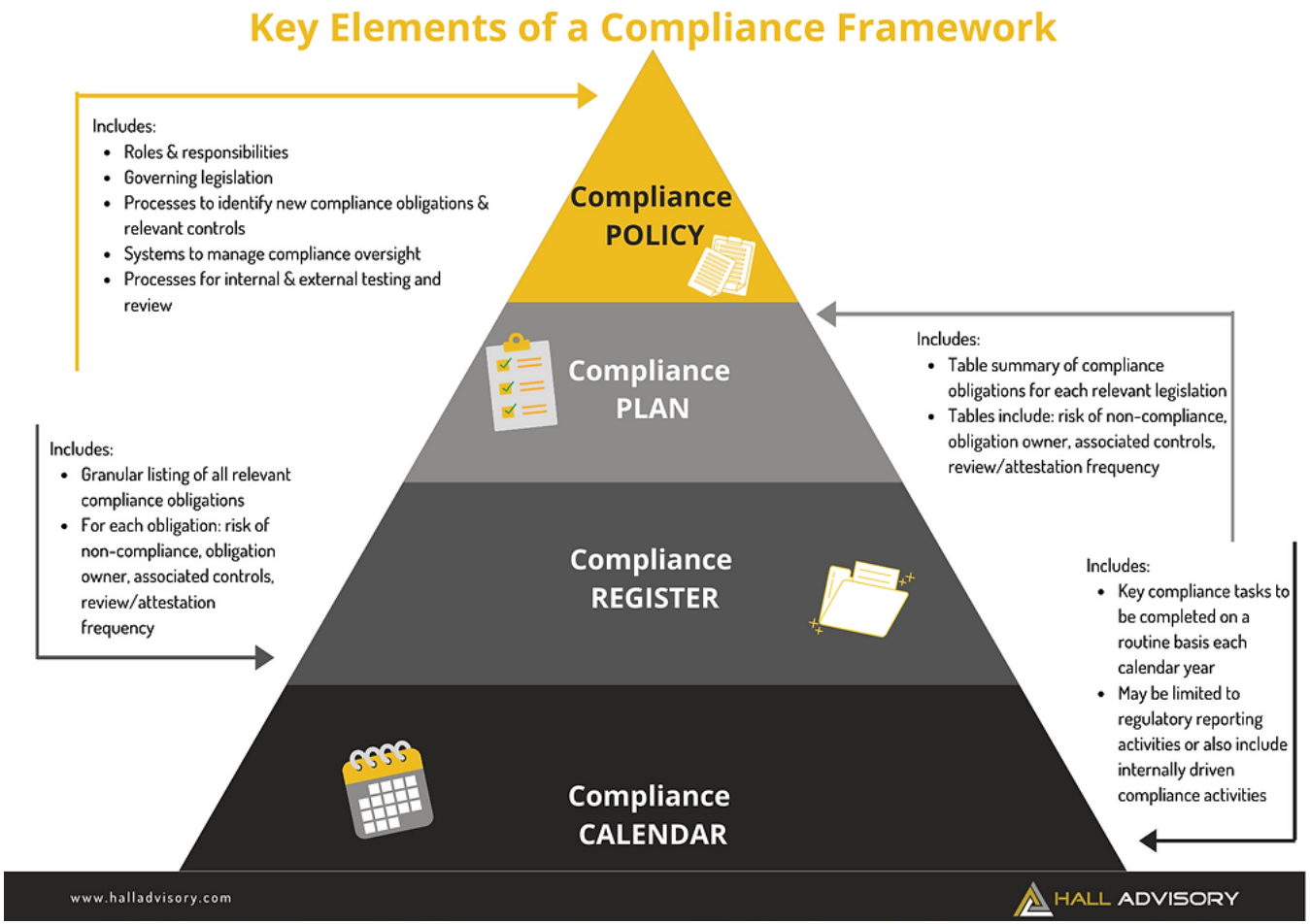
Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

الفرق بين التدقيق وتحقيق الالتزام

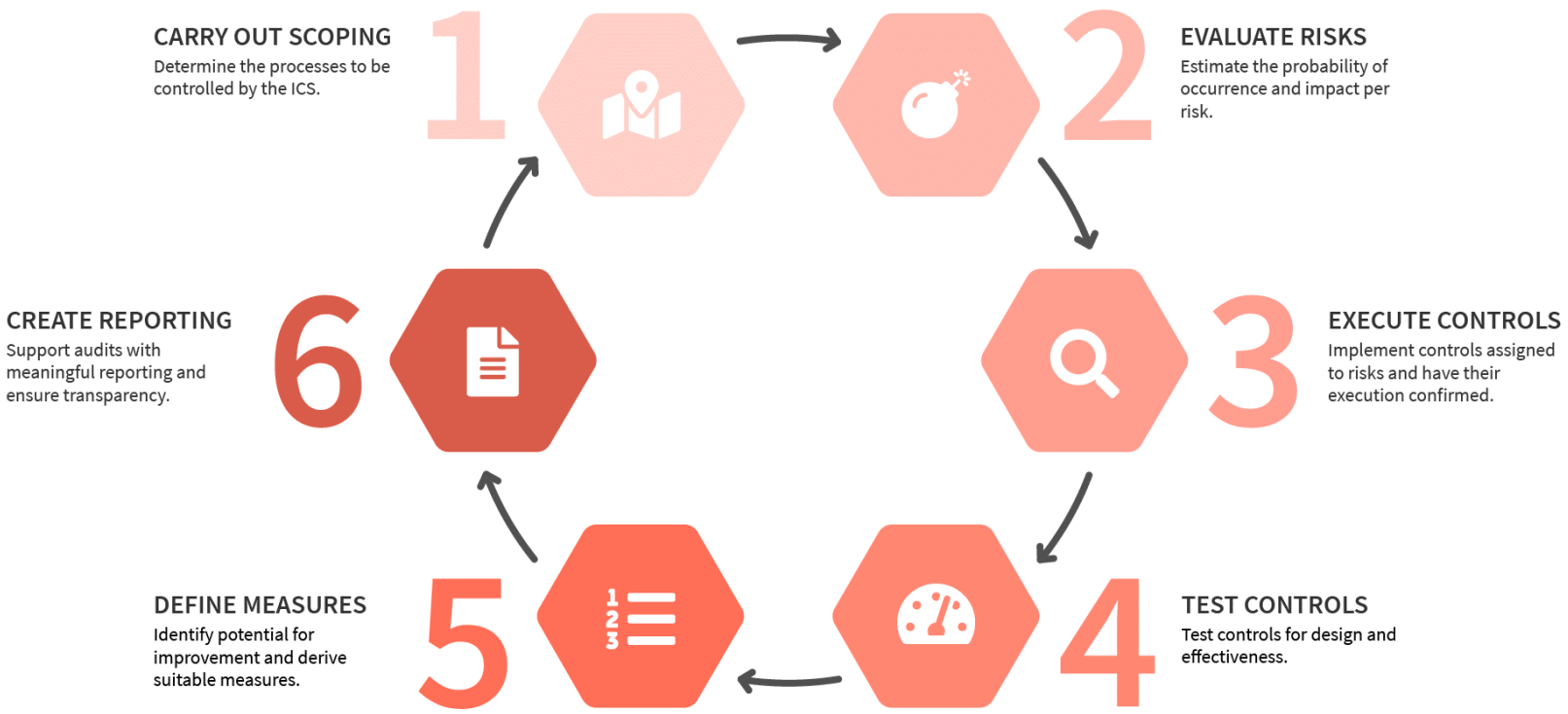
Difference Between Compliance and Internal Audit

Compliance Audit	Internal Audit
An external auditing body that ensures your company is adhering to the procedures, relevant laws, industry standards, and ethics.	An internal control team from your organization checks whether the internal procedures like code of conduct are followed.
They run audits for key areas where there are possibilities of fraudulent activities to occur. In addition, they may audit themselves or hire an external auditor.	They also carry out monitoring and evaluation of compliance from the company's side.

عناصر تحقيق الالتزام



Compliance Processes Steps
عمليات تحقيق الالتزام



أشهر شهادات التدقيق وتحقيق الالتزام

ISO 27001 Auditor

خلال هذه الدورة التدريبية، يكتسب المتدرب المعرفة والمهارات اللازمة

لتخطيط وتنفيذ عمليات التدقيق الداخلي والخارجي وفقا لعملية
اعتماد ISO 19011 و ISO/IEC 17021-1. بناءٍ على التمارين العملية، والمهارات

ويكون قادرا على إتقان تقنيات التدقيق و مؤهلا لإدارة برنامج تحقيق الالتزام
وفريق التدقيق . بعد اكتساب الخبرة والمهارات اللازمة لإجراء هذا التدقيق،

وتحقيق الاللتزام يمكن التقدم للاختبار والحصول على شهادة

"مدقق رئيسي معتمد لمعيار ISO/IEC 27001 من منظمة "PECB الامريكية .

قيمة امتحان الشهادة ($500) دولار

رابط الدخول على موقع الامتحان https://pecb.com/en/education-and-certification-for-individuals/iso-iec-27001/iso-iec-27001-lead-auditor

أشهر شهادات التدقيق وتحقيق الالتزام

CISA from ISACA

تساعدك هذة الدورة على اكتساب الخبرة في مجال تطوير واختبار وتنفيذ أنظمة المعلومات ومعرفة الإرشادات والمعايير وأفضل الممارسات لحمايتها. كذلك تعزز فهمك لعملية تدقيق نظام المعلومات وكيفية حمايتها بشكل مناسب.تعد شهادة CISA أحد أشهر الشهادات للمحترفين والحاصلين عليها بعد استيفاء سنوات الخبرة والمهارات المطلوبة تعطي قوة ودلاله على أن الحاصل عليها بجدارة وعلم يتمتع بمهارات احترافية في تدقيق أنظمة المعلومات ومراقبتها وأمنها.

قيمة امتحان الشهادة ($ 575.00) دولار

رابط الدخول على موقع الامتحان

https://www.isaca.org/credentialing/cisa?gad_source=1&gclid=CjwKCAiAsIGrBhAAEiwAEzMlC1-VynjbwMiSypAtzELAQ-shN_zLe0Et7-XTW82TqtMqBkjEeLvH2hoCGHAQAvD_BwE#schedule