WEEK 4| Chapter 4: Governance and Risk Management

Objectives

- Explain the importance of strategic alignment
- Know how to manage information security policies
- Describe information security-related roles and responsibilities
- Identify the components of risk management
- Create polices related to information security policy, governance, and risk management

الأهداف

- شرح أهمية التوافق الإستراتيجي
- تعرف على كيفية إدارة سياسات أمان المعلومات
- وصف الأدوار والمسؤوليات المتعلقة بأمن المعلومات
- التعرف على مكونات إدارة المخاطر
- إنشاء سياسات مرتبطة بسياسة أمن المعلومات ، والحوكمة ، وإدارة المخاطر

Understanding Information Security Policies

- The goal of the information security policies is to protect the organization from harm
  - Policies should be written
  - Policies should be supported by management
  - Policies should be strategically aligned-ie the companies' security policy with business requirements and relevant laws and regulations
- ISO 27002:2013 can provide a framework for developing security policies

فهم سياسات أمن المعلومات

- الهدف من سياسات أمن المعلومات هو حماية المنظمة من الأذى
  - يجب كتابة السياسات
  - يجب دعم السياسات من قبل الإدارة
  - يجب أن تكون السياسات متماثلة استراتيجياً - أي سياسة أمن الشركات مع متطلبات العمل والقوانين واللوائح ذات الصلة
- يمكن أن توفر ISO 27002: 2013 إطارًا لتطوير سياسات الأمان

Understanding Information Security Policies cont

- Two approaches to information security
  - Parallel approach
    - assigns responsibility for being secure to the IT department, views compliance as discretionary, and has little or no organizational accountability
  - Integrated approach
    - recognizes that security and success are intertwined
- Policies can serve as teaching documents to influence behavior
  - Acceptable Use Policy
    - document and corresponding agreement should be developed specifically for distribution to the user community
  - Companies should create vendor versions of information security policies
  - Policies should be authorized by executive management
  - Policies should be updated on regular basis

فهم سياسات أمن المعلومات

- نهجان لأمن المعلومات
  - نهج متوازي
    - يعين المسؤولية عن كونها آمنة لقسم تكنولوجيا المعلومات ، ويراعي الامتثال على أنه تقديري ، ولديه مسؤولية تنظيمية قليلة أو منعدمة
  - نهج متكامل
    - يدرك أن الأمن والنجاح متشابكان
- يمكن للسياسات أن تكون بمثابة وثائق تعليمية للتأثير على السلوك
  - سياسة الاستخدام المقبول
    - يجب إعداد وثيقة والاتفاق المقابل خصيصا للتوزيع على مجتمع المستخدمين

- يجب على الشركات إنشاء إصدارات البائعين لسياسات أمان المعلومات
- يجب أن تكون السياسات معتمدة من الإدارة التنفيذية
- يجب تحديث السياسات على أساس منتظم

Evaluating Information Security Policies

- As applicable, standards, guidelines, plans, and procedures must be developed to support the implementation of policy objectives and requirements.
- Any information security policy distributed outside the organization must be sanitized.
- All documentation will be retained for a period of six years from the last effective date.

تقييم سياسات أمن المعلومات

- حسب الاقتضاء ، يجب تطوير المعايير والمبادئ التوجيهية والخطط والإجراءات لدعم تنفيذ أهداف السياسة والمتطلبات.
- يجب تطهير أي سياسة لأمن المعلومات يتم توزيعها خارج المنظمة.
- يتم الاحتفاظ بجميع الوثائق لمدة ست سنوات من تاريخ السريان الأخير.

Who Authorizes Information Security Policy?

A policy is a reflection of the organization's commitment, direction, and approach and it has four essential practices:

- Place information security on the Board's agenda.
- Identify information security leaders, hold them accountable, and ensure support for them.
- Ensure the effectiveness of the corporation's information security policy through review and approval.
- Assign information security to a key committee and ensure adequate support for that committee

من يفوض سياسة أمن المعلومات؟

السياسة هي انعكاس لالتزام المنظمة وتوجيهها ونهجها ولها أربع ممارسات أساسية:

- ضع أمن المعلومات في جدول أعمال مجلس الإدارة.
- تحديد قادة أمن المعلومات ، وحملهم على المساءلة ، وضمان الدعم لهم.
- ضمان فعالية سياسة أمن معلومات الشركة من خلال المراجعة والموافقة.
- تعيين أمن المعلومات إلى لجنة رئيسية وضمان الدعم الكافي لهذه اللجنة

Revising Information Security Policies: Change Drivers:

- Organizations change over time, policies need to be revisited.
- Change drivers are events that modify how a company does business and they can be can be
  - Demographic
  - Economic
  - Technological, and regulatory or personnel related.
  - Examples of change drivers include company acquisition, new products, services or technology, regulatory updates, entering into a contractual obligation, and entering a new market.
- Why
  - Change can introduce new vulnerabilities and risks.
  - Change trigger internal assessments.

مراجعة ISP- تغييرالمشغلين :

- المؤسسات تتغير بمرور الوقت ، يجب إعادة النظر في السياسات.
- تغيير المشغلين هي الأحداث التي تقوم بتعديل كيفية قيام الشركة بأعمال تجارية ويمكن أن تكون كذلك
  - سكانية
  - اقتصادي
  - التكنولوجية والتنظيمية أو المتعلقة بالموظفين..
  - وتشمل أمثلة برامج التشغيل تغيير الشركات ، والمنتجات الجديدة ، والخدمات أو التكنولوجيا ، والتحديثات التنظيمية ، والدخول في التزام تعاقدي ، ودخول سوق جديدة.
- لماذا :
  - يمكن للتغيير إدخال نقاط ضعف ومخاطر جديدة.
  - تغيير التقييمات الداخلية المشغلة..

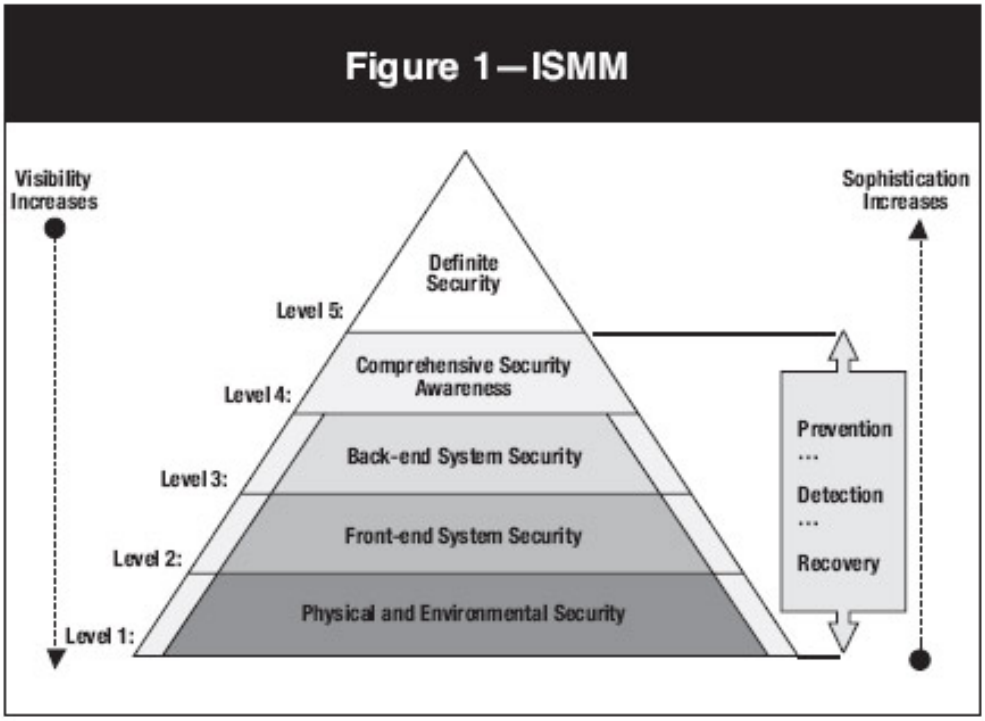
Evaluating Information Security Policies

- Policies can be evaluated internally or by independent third parties
- Audit
  - Systematic, evidence-based evaluation
  - Include interviews, observation, tracing documents to management policies, review or practices, review of documents, and tracing data to source documents
  - Audit report containing the formal opinion and findings of the audit team is generated at the end of the audit
- Capability Maturity Model (CMM)
  - Used to evaluate and document process maturity for a given area

تقييم سياسات أمن المعلومات

- يمكن تقييم السياسات داخليًا أو بواسطة طرف ثالث مستقل
- تدقيق
  - تقييم منهجي قائم على الأدلة
  - تضمين المقابلات والملاحظة وتعقب المستندات لسياسات الإدارة والمراجعة أو الممارسات ومراجعة المستندات وتتبع البيانات إلى الوثائق المصدر
  - يتم إنشاء تقرير التدقيق الذي يتضمن الرأي الرسمي والنتائج التي توصل إليها فريق التدقيق في نهاية عملية التدقيق
- نموذج نضج القدرات (CMM)
  - تستخدم لتقييم وتوثيق نضج العملية لمنطقة معينة

CMM example



Capability Maturity Model Scale

Level	State	Description
0	Non Existent	The organization is unaware of need for policies and processes المنظمة ليست على دراية بالحاجات للسياسات والعمليات
1	Ad-hoc	There are no documented policies or processes; there is sporadic activity. لا توجد سياسات أو عمليات موثقة. هناك نشاط متقطع.
2	Repeatable	Policies and processes are not fully documented; however, the activities occur on a regular basis. لا يتم توثيق السياسات والعمليات بشكل كامل ؛ ومع ذلك ، فإن الأنشطة تحدث على أساس منتظم.
3	Defined Process	Policies and processes are documented and standardized; there is an active commitment to implementation السياسات والعمليات موثقة وموحدة ؛ هناك التزام نشط بالتنفيذ
4	Managed	Policies and processes are well defined, implemented, measured, and tested. يتم تحديد السياسات والعمليات بشكل جيد وتنفيذها وقياسها واختبارها.
5	Optimized	Policies and process are well understood and have been fully integrated into the organizational culture. السياسات والعملية مفهومة بشكل جيد وتم دمجها بالكامل في الثقافة التنظيمية.

Information Security Governance

- The process of managing, directing, controlling, and influencing organizational decisions, actions, and behaviors
- The Board of Directors is usually responsible for overseeing the policy development
- Effective security requires a distributed governance model with the active involvement of stakeholders, decision makers, and users

حوكمة أمن المعلومات

- عملية إدارة وتوجيه ومراقبة والتأثير على القرارات والإجراءات والسلوكيات التنظيمية
- يكون مجلس الإدارة مسؤولًا عادة عن الإشراف على تطوير السياسة
- يتطلب الأمن الفعال نموذجًا لحوكمة موزعة مع المشاركة النشطة لأصحاب المصلحة وصانعي القرار والمستخدمين

Distributed Governance Model

- The foundation is the principle that stewardship is an organizational responsibility
- Effective security requires the
  - Active involvement
  - Cooperation
  - Collaboration of stakeholders
  - Decision makers, and the user community
- Chief information security officer (CISO)
- Information security steering committee
- Compliance officer
- Privacy officer
- Internal audit
- Incident response team
- Data owners
- Data custodians
- Data users

نموذج الحوكمه الموزعه

- الأساس هو مبدأ أن الإشراف مسؤولية تنظيمية
- يتطلب الأمن الفعال
  - المشاركة الفعالة
  - تعاون
  - تعاون أصحاب المصلحة
  - صناع القرار ، ومجتمع المستخدمين
- كبير ضباط أمن المعلومات (CISO)
- لجنة توجيه أمن المعلومات
- ضابط الامتثال
- ضابط الخصوصية
- التدقيق الداخلي
- فريق الاستجابة للحوادث
- أصحاب البيانات
- أمناء البيانات
- مستخدمو البيانات

Chief information security officer (CISO)

The CISO coordinates and manages security efforts across the company, including IT, human resources (HR), communications, legal, facilities management, and other groups.

- The COO will appoint the CISO.
- The CISO will report directly to the COO.
- At his or her discretion, the CISO may communicate directly with members of the Board of Directors.
- The CISO will chair the Information Security Steering Committee.

كبير موظفين أمن المعلومات (CISO)

- تقوم CISO بتنسيق وإدارة الجهود الأمنية عبر الشركة ، بما في ذلك تكنولوجيا المعلومات والموارد البشرية (HR) والاتصالات والقانونية وإدارة المرافق والمجموعات الأخرى.
- الرئيس التنفيذي (COO) سيعين CISO.
- ستقوم CISO بالإبلاغ مباشرة إلى COO.
- وفقا لتقديره ، يجوز لـ CISO التواصل مباشرة مع أعضاء مجلس الإدارة.
- سيترأس CISO لجنة توجيه أمن المعلومات.

Information security steering committee

- The Information Security Steering Committee (ISC) is tasked with supporting the information security program
- serves in an advisory capacity
- provides an open forum to discuss business initiatives and security requirements
- Standing membership will include the CISO (Chair), the COO, the Director of Information Technology, the Risk Officer, the Compliance Officer, and business unit representatives.
- will meet on a monthly basis

لجنة توجيه أمن المعلومات

- تكليف اللجنة التوجيهية لأمن المعلومات (ISC) بدعم برنامج أمن المعلومات
- يخدم بصفة استشارية
- يوفر منتدى مفتوح لمناقشة مبادرات الأعمال والمتطلبات الأمنية
- ستشمل العضوية الدائمة CISO (رئيس) ، COO ، مدير تكنولوجيا المعلومات ، مسؤول المخاطر ، موظف الالتزام ، وممثلي وحدة الأعمال.
- سوف يكون الاجتماع على أساس شهري

Organization Roles and Responsibilities

In addition to the CISO and the Information Security Steering Committee, a variety of roles that have information security–related responsibilities.

- **Compliance Officer**—Responsible for identifying all applicable information security–related statutory, regulatory, and contractual requirements.
- **Privacy Officer**—Responsible for the handling and disclosure of data as it relates to state, federal, and international law and customs.
- **Internal audit**—Responsible for measuring compliance with Board-approved policies and to ensure that controls are functioning as intended.
- **Incident response team**—Responsible for responding to and managing security-related incidents.
- **Data owners**—Responsible for defining protection requirements for the data based on classification, business need, legal, and regulatory requirements; reviewing the access controls; and monitoring and enforcing compliance with policies and standards
- **Data custodians**—Responsible for implementing, managing, and monitoring the protection mechanisms defined by data owners and notifying the appropriate party of any suspected or known policy violations or potential endangerments.
- **Data users**—Are expected to act as agents of the security program by taking reasonable and prudent steps to protect the systems and data they have access to.

These responsibilities should be documented in policies, job descriptions, or employee manuals.

أدوار المنظمة ومسؤولياتها

بالإضافة إلى CISO ولجنة توجيه أمن المعلومات ، هناك مجموعة متنوعة من الأدوار التي لها مسؤوليات متعلقة بأمن المعلومات.

- مسؤول الالتزام - مسؤول عن تحديد جميع المتطلبات القانونية والتنظيمية والتعاقدية المتعلقة بأمن المعلومات المعمول به.
- مسؤول الخصوصية - مسؤول عن التعامل مع البيانات والكشف عنها من حيث صلتها بالقوانين والأعراف الحكومية والفدرالية والدولية.
- التدقيق الداخلي - مسؤول عن قياس الامتثال للسياسات المعتمدة من قبل مجلس الإدارة ولضمان عمل الضوابط على النحو المنشود.
- فريق الاستجابة للحوادث - مسؤول عن الاستجابة وإدارة الحوادث المتعلقة بالأمن.
- مالك البيانات - يكون مسؤولاً عن تحديد متطلبات الحماية للبيانات القائمة على التصنيف واحتياجات العمل والمتطلبات القانونية والمتطلبات التنظيمية ؛ مراجعة عناصر التحكم في الوصول ؛ ورصد وإنفاذ الامتثال للسياسات والمعايير
- مسؤولو البيانات - المسؤولون عن تنفيذ وإدارة ومراقبة آليات الحماية التي يحددها مالكو البيانات وإخطار الطرف المناسب بأي انتهاكات مشبوهة أو معروفة للسياسات أو تعرضهم لخطر محتمل.
- مستخدمو البيانات - من المتوقع أن يكونوا بمثابة وكلاء لبرنامج الأمان من خلال اتخاذ خطوات معقولة وحذرة لحماية الأنظمة والبيانات التي يمكنهم الوصول إليها.

يجب توثيق هذه المسؤوليات في السياسات أو توصيف الوظائف أو كتيبات الموظفين.

Information Security Risk

- Three factors influence information security decision making and policy creation
  - Guiding principles
  - Regulatory requirements
  - Risk associated with achieving business objectives
- **Risk**: The potential of undesirable or unfavorable outcome from a given action.
- **Risk tolerance:** How much undesirable outcome the risk taker is willing to accept
- **Risk appetite:** The amount of risk an entity is willing to accept in pursuit of its mission

مخاطر أمن المعلومات

- هناك ثلاثة عوامل تؤثر على صنع قرار أمن المعلومات وإنشاء السياسة
  - المبادئ التوجيهية
  - المتطلبات التنظيمية
  - المخاطر المرتبطة بتحقيق أهداف العمل
- **الخطر**: احتمال وجود (احتمال غير مرغوب فيه) أو (نتيجة غير مرغوب فيها) من إجراء معين.
- **تحمل المخاطر:** مقدار تحمل المخاطر مقابل الفوائد التي يحصل عليها
- **الرغبة في المخاطرة:** مقدار المخاطرة التي قد ترغب الجهه في قبولها لمتابعته

Risk Assessment

- Evaluate what can go wrong and the likelihood of a harmful event occurring
- Risk assessment involves
  - Identifying the inherent risk based on relevant threats, threat sources, and related vulnerabilities
  - Determining the impact of a threat if it occurs
  - Calculating the likelihood of occurrence
  - Determining residual risk

- **Inherent risk** - The level of risk before security measure are applied
- **Residual risk** - The level of risk after security measures are applied
- **Threat** - Natural, environmental, or human event that could cause harm
- **Vulnerability** - A weakness that could be exploited by a threat
- **Impact** - The magnitude of a harm

تقييم المخاطر

- تقييم ما يمكن أن يحدث بشكل خاطئ واحتمال وقوع حدث ضار
- يتضمن تقييم المخاطر
  - تحديد الخطر الكامن على أساس التهديدات ذات الصلة ومصادر التهديد ونقاط الضعف ذات الصلة
  - تحديد تأثير التهديد في حالة حدوثه
  - حساب احتمالية حدوثها
  - تحديد المخاطر المتبقية

- **الخطر المتأصل** - يتم تطبيق مستوى المخاطرة قبل إجراء التدبير الأمني
- **المخاطر المتبقية** - مستوى المخاطرة بعد تطبيق الإجراءات الأمنية
- **التهديد** - حدث طبيعي أو بيئي أو إنساني يمكن أن يتسبب في ضرر
- **الضعف** - الضعف الذي يمكن استغلاله من خلال التهديد
- **الأثر** - حجم الضرر

Risk Assessment Methodologies

- Components of a risk assessment methodology include
  - Defined process
  - Assessment approach
  - Standardized analysis
- Three well-known information security risk assessment methodologies
  - Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)
  - Factor Analysis of Information Risk (FAIR)
  - NIST Risk Management Framework (RMF)

منهجيات تقييم المخاطر

- تشمل مكونات منهجية تقييم المخاطر
  - تعريف العمليات
  - نهج التقييم
  - تحليل قائم على أسس
- ثلاث منهجيات لتقييم مخاطر أمن المعلومات المعروفة
  - التقييم التشغيلي الحرج للأصول ، وتقييم الأصول ، والضعف (OCTAVE)
  - تحليل عامل لمخاطر المعلومات (FAIR)
  - NIST إطار إدارة المخاطر (RMF)

Risk Management

- The process of determining an acceptable level of risk, calculating the current risk level, accepting the level of risk, or taking steps to reduce it to an acceptable level
- Risk acceptance
- Risk mitigation
  - Risk reduction
  - Risk transfer
  - Risk sharing
  - Risk avoidance

إدارة المخاطر

- عملية تحديد مستوى مقبول من المخاطر ، حساب مستوى المخاطر الحالي ، قبول مستوى المخاطرة ، أو اتخاذ خطوات لتخفيضه إلى مستوى مقبول
- قبول المخاطر
- تخفيف المخاطر
  - تقليل المخاطر
  - نقل المخاطر
  - تقاسم المخاطر
  - تجنب المخاطر

Risk Management

- **Risk Acceptance :** Risk acceptance indicates that the organization is willing to accept the level of risk associated with a given activity or process
- **Risk Mitigation :** The process of reducing, sharing, transferring or avoiding risk.
- **Risk Reduction :** Process of control to lower the residual risk
  - Offensive Control: reducing or eliminating the vulnerabilities by enhanced training or applying security patch
  - Defensive control :respond to threat source such as sensor sending an alert or detecting an intruder.
- **Risk Transfer :** shifts the entire risk responsibility or liability from one organization to another organization. This is often accomplished by purchasing insurance.
- **Risk sharing :** shifts a portion of risk responsibility or liability to other organizations.
- **Risk avoidance :** involves taking specific actions to eliminate or significantly modify the process or activities that are the basis for the risk.

- **قبول المخاطر:** يشير قبول المخاطر إلى أن المنظمة على استعداد لقبول مستوى المخاطر المرتبطة بنشاط أو عملية معينة
- **تخفيف المخاطر:** عملية تقليل أو مشاركة أو نقل أو تجنب المخاطر.
- **تقليل المخاطر:** عملية التحكم لخفض المخاطر المتبقية
  - السيطرة الهجومية: تقليل أو إزالة الثغرات من خلال تدريب محسّن أو تطبيق تصحيح الأمان
  - السيطرة الدفاعية: الاستجابة لمصدر التهديد مثل جهاز الاستشعار الذي يرسل إنذارًا أو يكتشف دخلاً.
- **نقل المخاطر:** ينقل كامل المسؤولية عن تحمل المخاطر من منظمة إلى منظمة أخرى. غالبا ما يتم ذلك عن طريق شراء التأمين.
- **تقاسم المخاطر:** ينقل جزء من مسؤولية المخاطرة أو المسئولية تجاه المنظمات الأخرى.
- **تجنب المخاطر**: ينطوي على اتخاذ إجراءات محددة للقضاء أو تعديل على العملية أو الأنشطة التي تشكل أساسًا للمخاطر.

Summary

- Information security policies should be reviewed at least annually to ensure they are relevant and accurate
- Information security audits should be conducted to ensure policies are accepted and integrated
- **Governance** is the process of managing, directing, controlling, and influencing organizational decisions, actions, and behaviors
- **Risk management** is the process of determining an acceptable level of risk, calculating the current risk level, accepting the level of risk, or taking steps to reduce it to an acceptable level