WEEK 3 | Chapter 3: Information Security Framework

Objectives

- Recognize the importance of the CIA security model and describe the security objectives of confidentiality, integrity, and availability
- Discuss why organizations choose to adopt a security framework
- Recognize the values of NIST resources
- Understand the intent of ISO/IEC 27000-series of information security standards
- Outline the domains of an information security program

الأهداف

- التعرف على أهمية النموذج الأمني لـ CIA ووصف الأهداف الأمنية للسرية والتكامل والتوافر
- مناقشة لماذا تختار المنظمات اعتماد إطار عمل أمني
- التعرف على قيم موارد NIST
- فهم نية سلسلة معايير أمن المعلومات ISO / IEC 27000
- الخطوط العريضة لنطاقات برنامج أمن المعلومات

CIA

- The CIA Triad or CIA security model
  - Stands for Confidentiality, Integrity, and Availability
  - An attack against either or several of the elements of the CIA triad is an attack against the Information Security of the organization
  - Protecting the CIA triad means protecting the assets of the company

CIA

- النموذج الأمني CIA أو الثلاثي CIA
  - تقف على السرية والتكامل ، والتوافر
  - الهجوم على أي من عناصر CIA أو عدة عناصر منها هو الهجوم على أمن المعلومات في المنظمة
  - حماية CIA يعني حماية أصول الشركة

CIA

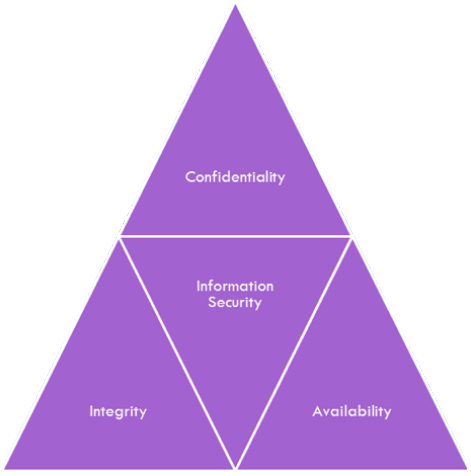
The Federal Information Security Management Act (FISMA) defines the relationship between information security and the CIA triad as follows:

- "information security" means protecting information and information systems in order to provide
  - integrity
  - confidentiality
  - availability
- Organizations may consider all three components of the CIA triad equally important, in which case resources must be allocated proportionately

العلاقة بين IS و CIA

يعرف القانون الفيدرالي لإدارة أمن المعلومات (FISMA) العلاقة بين أمن المعلومات و CIA triad على النحو التالي:

- "أمن المعلومات" حماية المعلومات ونظم المعلومات من الوصول غير المصرح به أو الاستخدام أو الكشف أو التعطيل أو التعديل أو التدمير من أجل توفير:
  - سلامة البيانات او النزاهه
  - السرية
  - التوافر
- قد ترى المنظمات أن العناصر الثلاث لثالث السي آي إيه لها نفس الأهمية ، وفي هذه الحالة يجب تخصيص الموارد بطريقة تناسبية



What Is Confidentiality?

- Not all data owned by the company should be made available to the public
- Failing to protect data confidentiality can be disastrous for an organization:
  - Dissemination of Protected Health Information (PHI) between doctor and patient
  - Dissemination of Protected Financial Information (PFI) between bank and customer
  - Dissemination of business-critical information to rival company
- Only authorized users should gain access to information
- Information must be protected when it is used, shared, transmitted, and stored
- Information must be protected from unauthorized users both internally and externally
- Information must be protected whether it is in digital or paper format
- The threats to confidentiality must be identified. They include:
  - Hackers and hacktivists
  - Shoulder surfing
  - Lack of shredding of paper documents
  - Malicious Code (Virus, worms, Trojans)
  - Unauthorized employee activity
  - Improper access control
- The information security goal of confidentiality is to protect information from unauthorized access and misuse
- The best way to do this is to implement safeguards and processes that increase the work factor and the chance of being caught
- A spectrum of access controls and protections as well as ongoing monitoring, testing, and training

ما هي السرية؟

- يجب ألا تكون جميع البيانات التي تمتلكها الشركة متاحة للعامة
- قد يكون عدم حماية سرية البيانات كارثياً بالنسبة للمؤسسة:
  - نشر المعلومات الصحية المحمية (PHI) بين الطبيب والمريض (قانون حصانة -الطبيب-المريض)
  - نشر المعلومات المالية المحمية (PFI) بين البنك والعميل
  - نشر المعلومات الهامة للأعمال لشركة منافسة
- يجب فقط للمستخدمين المصرح لهم الوصول إلى المعلومات
- يجب حماية المعلومات عند استخدامها ومشاركتها ونقلها وتخزينها
- يجب حماية المعلومات من المستخدمين غير المصرح بهم داخليًا وخارجيًا
- يجب حماية المعلومات سواء كانت بتنسيق رقمي أو ورق
- يجب تحديد التهديدات للسرية. يشملوا:
  - Hackers و hacktivists (يعرف الشخص الذي ينفذ فعل hacktivism بأنه hacktivist .. والهاكتفزم هو استخدام أجهزة الحاسوب والشبكات الحاسوبية لتعزيز أجندة سياسية. وغالبا ما ترتبط أهدافه بحرية التعبير، حقوق الإنسان أو حرية المعلومات)
  - Shoulder surfing (مصطلح يستخدم لوصف الشخص الذي ينظر إلى كتف شخص آخر عند إدخال البيانات في جهاز كمبيوتر أو جهاز آخر. يمكن استخدام Shoulder surfing عند إدخال كلمة مرور الكمبيوتر أو رقم التعريف الشخصي للصراف الآلي أو رقم بطاقة الائتمان)
  - عدم تمزيق الوثائق الورقية
  - الشفرة الخبيثة (الفيروس ، الديدان ، حصان طروادة)
  - نشاط موظف غير مصرح به
  - تحكم غير صحيح في الوصول
- إن هدف سرية أمن المعلومات هو حماية المعلومات من الوصول غير المصرح به وسوء الاستخدام
- أفضل طريقة للقيام بذلك هي تنفيذ الضمانات والعمليات التي تزيد عامل العمل وفرصة الامساك بهم
- مجموعة من عناصر التحكم في الوصول والحماية بالإضافة إلى المراقبة المستمرة والاختبار والتدريب

What Is Integrity?

- Protecting data, processes, or systems from intentional or accidental unauthorized modification
  - Data integrity- A requirement that information and programs are changed only in a specified and authorized manner
  - System integrity- A requirement that a system “performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system
- A business that cannot trust the integrity of its data is a business that cannot operate
- An attack against data integrity can mean the end of an organization’s capability to conduct business
- Threats to data integrity include:
  - Human error
  - Hackers
  - Unauthorized user activity
  - Improper access control
  - Malicious code
  - Interception and alteration of data during transmission
- Controls that can be deployed to protect data integrity include:
  - Access controls:
    - Encryption
    - Digital signatures
  - Process controls
    - Code testing
  - Monitoring controls
    - File integrity monitoring
    - Log analysis
  - Behavioral controls:
    - Separation of duties
    - Rotation of duties
    - End user security training

ماهي السلامة ؟

- حماية البيانات أو العمليات أو الأنظمة من التعديل غير المصرح به عن قصد أو عن غير قصد
  - سلامة البيانات - شرط أن يتم تغيير المعلومات والبرامج فقط بطريقة محددة ومصرح بها
  - سلامة النظام- - اشتراط أن يقوم النظام "بأداء وظيفته المقصودة بطريقة موثوقة ، خالية من التلاعب غير المصرح به أو غير المقصود من النظام
- الأعمال التي لا تثق في سلامة بياناتها هي الأعمال التي لا يمكنها العمل
- يمكن أن يعني الهجوم على سلامة البيانات نهاية قدرة المؤسسة على إدارة العمل
- تتضمن التهديدات لسلامة البيانات:
  - الخطأ البشري
  - القراصنة
  - نشاط المستخدم غير المصرح به
  - تحكم غير صحيح في الوصول
  - كود خبيث
  - اعتراض وتعديل البيانات أثناء الإرسال
- تتضمن عناصر التحكم التي يمكن نشرها لحماية سلامة البيانات:
  - عناصر التحكم في الوصول:
    - التشفير
    - التوقيعات الرقمية
  - ضوابط العملية
    - اختبار الكود
  - ضوابط المراقبة
    - مراقبة سلامة الملف
    - تحليل السجل
  - الضوابط السلوكية: - توزيع وفصل المهمات - تناوب في المهمات - تدريب أمان المستخدم النهائي

What Is Availability?

- Availability: The assurance that the data and systems are accessible when needed by authorized users
- The Service Level Agreement (SLA) is a type of agreement between a service provider and a customer that specifically addresses availability of services
- What is the cost of the loss of data availability to the organization?
- A risk assessment should be conducted to more efficiently protect data availability

- Threats to data availability include:
  - Natural disaster
  - Hardware failures
  - Programming errors
  - Human errors
  - Distributed Denial of Service attacks
  - Loss of power
  - Malicious code
  - Temporary or permanent loss of key personnel

ما هو التوافر؟

- الإتاحة: التأكد من أن البيانات والأنظمة يمكن الوصول إليها عند الحاجة من قبل المستخدمين المصرح لهم
- اتفاقية مستوى الخدمة (SLA) هي نوع من الاتفاقية بين مزود الخدمة والعميل الذي يتناول تحديدا توافر الخدمات
- ما هي تكلفة فقدان إتاحة البيانات للمؤسسة؟
- يجب إجراء تقييم للمخاطر لتوفير حماية البيانات بشكل أكثر كفاءة

- تتضمن التهديدات لتوفر البيانات ما يلي:
  - كارثة طبيعية
  - فشل الأجهزة
  - أخطاء البرمجة
  - أخطاء بشرية
  - هجمات للحرمان من الخدمة الموزعة
  - فقدان الطاقه
  - كود خبيث
  - فقدان مؤقت أو دائم للموظفين الاساسيين

The Five A's of Information Security

Supporting the CIA triad of information security are five key information security principles, commonly known as the Five A's.

- Accountability
- Assurance
- Authentication
- Authorization
- Accounting

الخمسة A's من أمن المعلومات

- دعم CIA من أمن المعلومات هي خمسة مبادئ أمن المعلومات الرئيسية ، والمعروف باسم الخمسة A's.
- المسؤليه
- الضمان
- الهويه - المصادقه عليها
- الصلاحيه
- التتبع

Accountability

- All actions should be traceable to the person who committed them
- Logs should be kept, archived, and secured
- Intrusion detection systems should be deployed
- Computer forensic techniques can be used retroactively
- Accountability should be focused on both internal and external actions

المسئوليه

- يجب أن تكون جميع الإجراءات عائدة إلى الشخص الذي ارتكبها
- يجب حفظ السجلات وأرشفتها وتأمينها
- ينبغي نشر أنظمة كشف التسلل
- يمكن استخدام تقنيات قضاڈيه الحاسوبية بأثر رجعي
- يجب أن تركز المسئوليه على كل من الإجراءات الداخلية والخارجية

Assurance

- Security measures need to be designed and tested to ascertain that they are efficient and appropriate
- The knowledge that these measures are indeed efficient is known as assurance
- The activities related to assurance include:
  - Auditing and monitoring
  - Testing
  - Reporting

الضمان والتأكيد

- يجب تصميم إجراءات الأمن واختبارها للتأكد من أنها فعالة ومناسبة
- تُعرف معرفة أن هذه الإجراءات فعالة بالفعل كضمان
- الأنشطة المتعلقة بالضمان تشمل:
  - التدقيق والمراقبة
  - الاختبارات
  - التقارير

Authentication

- Authentication is the cornerstone of most network security models
- It is the positive identification of the person or system seeking access to secured information and/or system
- Examples of authentication models:
  - User ID and password combination - Tokens - Biometric devices

الهوية

- الهويه هو حجر الزاوية لمعظم نماذج أمن الشبكات
- إنه التعريف الإيجابي للشخص أو النظام الذي يسعى للوصول إلى المعلومات و / أو النظام الآمن (ID)
- أمثلة على نماذج الهوية:
  - هوية المستخدم وكلمة السر - الرموز(مثل جهاز يمرر عليه بطاقه للدخول) - الأجهزة البيومترية (مثل اجهزة البصمة)

Authorization

- Act of granting users or systems actual access to information resources
- Note that the level of access may change based on the user's defined access level
- Examples of access level include the following:
  - Read only
  - Read and write
  - Full

الصلاحية

- قانون منح المستخدمين أو الأنظمة الوصول الفعلي إلى موارد المعلومات
- لاحظ أن مستوى الوصول قد يتغير استنادًا إلى مستوى الوصول المحدد من قبل المستخدم
- تتضمن أمثلة مستوى الوصول ما يلي:
  - قراءة فقط - قراءة و كتابة - وصول كامل

Accounting

- Defined as the logging of access and usage of resources
- Keeps track of who accesses what resource, when, and for how long
- An example of use:
  - Internet café, where users are charged by the minute of use of the service
- CIA plus the Five A's are fundamental objectives and attributes of an information security program.

التتبع

- يتم تعريفه على أنه تسجيل الدخول إلى الموارد واستخدامها
- يتتبع من الذي يصل إلى الموارد ومتى ومدة ذلك الوقت
- مثال على الاستخدام:
  - مقهى الإنترنت ، حيث يتم محاسبة المستخدمين عن طريق استخدام الخدمة

تعد CIA بالإضافة إلى A الخمسة أهدافًا وسمات أساسية لبرنامج أمان المعلومات.

Who Is Responsible for CIA?

- Information owner
  - An official with statutory or operational authority for specified information
  - Has the responsibility for ensuring information is protected from creation through destruction
- Information custodian
  - Maintain the systems that store, process, and transmit the information

من هو المسؤول عن CIA ؟

- مالك المعلومات
  - مسؤول لديه سلطة قانونية أو تشغيلية للحصول على معلومات محددة
  - هل تتم حماية مسؤولية ضمان المعلومات من إنشائها حتى التدمير
- مسؤول المعلومات
  - الحفاظ على الأنظمة التي تقوم بتخزين ، ومعالجة ، ونقل المعلومات

Information Security Framework

- **Security framework** is a collective term given to guidance on topics related to
  - information systems security
  - predominantly regarding the planning,
  - implementing
  - managing, and auditing of overall information security practices.
- Two of the most widely used frameworks are:
  - Information Technology and Security Framework by NIST
  - Information Security Management System by ISO

إطار أمن المعلومات

- يُعد الإطار الأمني مصطلحًا جماعيًا يتم تقديمه للتوجيهات المتعلقة بالمواضيع ذات الصلة ب:
  - أمن نظم المعلومات
  - في الغالب فيما يتعلق بالتخطيط ،
  - تنفيذ
  - إدارة ومراجعة ممارسات أمن المعلومات بشكل عام
- اثنان من أكثر الأطر استخداما هي:
  - تقنية المعلومات وإطار الأمن من NIST
  - نظام إدارة أمن المعلومات حسب ISO

NIST Functions

- Founded in 1901
- Non regulatory federal agency
- Its mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve quality of life
- Published more than 300 information security-related documents including
  - Federal Information Processing Standards (FIPS)
  - Special Publication 800 series
  - ITL bulletins
- The mission of NIST's CSD is to improve information systems security as follows:
  - By raising awareness of IT risks, vulnerabilities, and protection requirements, particularly for new and emerging technologies.
  - By researching, studying, and advising agencies of IT vulnerabilities and devising techniques for the cost-effective security and privacy of sensitive federal systems.
  - By developing standards, metrics, tests, and validation programs
  - By developing guidance to increase secure IT planning, implementation, management, and operation.
- NIST defines information security as the protection of information and information systems from threats in order to provide CIA

وظائف NIST

- تأسست في عام 1901
- وكالة اتحادية غير تنظيمية
- وتتمثل مهمتها في تطوير وتعزيز المقاييس والمعايير والتكنولوجيا لتعزيز الإنتاجية وتسهيل التجارة وتحسين نوعية الحياة
- نشر أكثر من 300 وثيقة متعلقة بأمن المعلومات بما في ذلك
  - معايير معالجة المعلومات الفيدرالية (FIPS)
  - سلسلة النشر 800 الخاصة
  - نشرات ال ITL
- تتمثل مهمة CSD في NIST في تحسين أمان أنظمة المعلومات كما يلي:
  - من خلال زيادة الوعي بمخاطر تكنولوجيا المعلومات ومواطن الضعف ومتطلبات الحماية ، خاصة بالنسبة للتكنولوجيات الجديدة والناشئة.
  - من خلال البحث والدراسة وتقديم المشورة للوكالات من نقاط الضعف في تكنولوجيا المعلومات ووضع تقنيات للأمن وخصوصية فعالة من حيث التكلفة للأنظمة الفيدرالية الحساسة.
  - من خلال تطوير المعايير والمقاييس والاختبارات وبرامج التحقق من الصحة
  - من خلال تطوير إرشادات لزيادة أمن تخطيط تقنية المعلومات والتنفيذ والإدارة والتشغيل.
- تعرف NIST أمان المعلومات كحماية المعلومات ونظم المعلومات من التهديدات من أجل توفير CIA

ISO Functions

- A network of national standards institutes of 146 countries
- Nongovernmental organization that has developed more than 13,000 international standards
- The ISO/IEC 27000 series represents information security standards published by ISO and Electro-technical Commission (IEC)

وظائف ISO

- شبكة من المعاهد الوطنية للمعايير من 146 دولة
- منظمة غير حكومية وضعت أكثر من 13000 معيار دولي
- تمثل سلسلة ISO / IEC 27000 معايير أمن المعلومات التي نشرتها ISO واللجنة الفنية التقنية (IEC).

ISO 27002:2013 Code of Practice

- Comprehensive set of information security recommendations on best practices in information security
- In ISO 27002:2013 -the recommendations are organized in the following domains:

Information security policies (Section 5) – This domain focuses on information security policy requirements and the need to align policy with organizational objectives.	**سياسات أمن المعلومات (القسم 5)** - يركز هذا المجال على متطلبات سياسة أمن المعلومات والحاجة إلى مواءمة السياسة مع الأهداف التنظيمية.
Organization of information security (Section 6) – This domain focuses on establishing and supporting a management structure to implement and manage information security within, across, and outside the organization.	**تنظيم أمن المعلومات (القسم 6)** - يركز هذا المجال على إنشاء ودعم هيكل إداري لتنفيذ وإدارة أمن المعلومات داخل المنظمة وخارجها وخارجها.
Human Resources Security Management (Section 7) – This domain focuses on integrating security into the employee lifecycle, agreements, and training. Human nature is to be trusting	**إدارة أمن الموارد البشرية (القسم 7)** - يركز هذا المجال على دمج الأمن في دورة حياة الموظفين والاتفاقيات والتدريب. الطبيعة البشرية هي أن تكون على ثقة
Asset Management (Section 8) – This domain focuses on developing classification schema, assigning classification levels, and maintaining accurate inventories of data and devices	**إدارة الأصول (القسم 8) -** يركز هذا المجال على تطوير مخطط التصنيف وتعيين مستويات التصنيف والحفاظ على جرد دقيق للبيانات والأجهزة
Access Control (Section 9) – This domain focuses on managing authorized access and preventing unauthorized access to information systems and extends to remote locations, home offices, and mobile access	**التحكم في الوصول (القسم 9) -** يركز هذا المجال على إدارة الوصول المصرح به ومنع الوصول غير المصرح به إلى نظم المعلومات وتمتد إلى المواقع النائية والمكاتب المنزلية والوصول عبر الأجهزة المحمولة
Cryptography (Section 10) – This domain was added in the 2013 update and it focuses on proper and effective use of cryptography to protect the CIA of information	**التشفير (القسم 10)** - تمت إضافة هذا المجال في تحديث 2013 ويركز على الاستخدام السليم والفعال للتشفير لحماية CIA من المعلومات
Physical and Environmental Security (Section 11) – This domain focuses on designing and maintaining a secure physical environment to prevent unauthorized .access, damage, and interference to business premises	**الأمن المادي والبيئي (القسم 11)** - يركز هذا المجال على تصميم والحفاظ على بيئة فعلية آمنة لمنع الوصول غير المصرح به والأضرار والتدخل إلى المباني التجارية.
Operations Security (Section 12) – This domain focuses on data centre operations, integrity of operations, vulnerability management, protection .against data loss, and evidence-based logging	**أمان العمليات (القسم 12)** - يركز هذا المجال على عمليات مركز البيانات وسلامة العمليات وإدارة نقاط الضعف والحماية من فقد البيانات والتسجيل المستند إلى الأدلة.
Communications Security (Section 13) – This domain focuses on the protection of information in transit	**أمن الاتصالات (القسم 13)** - يركز هذا المجال على حماية المعلومات أثناء النقل
Information Systems Acquisition, Development, and Maintenance (Section 14) – This domain focuses on the security requirements of information systems, .applications, and code from conception to destruction	**استحواذ أنظمة المعلومات وتطويرها وصيانتها (القسم 14) -** يركز هذا المجال على المتطلبات الأمنية لأنظمة المعلومات والتطبيقات والمدونات من البدايه إلى التدمير.
Supplier Relationships (Section 15) – This domain was added in the 2013 update. The domain focuses on service delivery, third-party security requirements, .contractual obligations, and oversight	**علاقات الموردين (القسم 15) -** تمت إضافة هذا المجال في تحديث 2013. ويركز المجال على تقديم الخدمات ، ومتطلبات الأمن الخاصة بالأطراف الثالثة ، والالتزامات التعاقدية ، والإشراف.

Information Security Incident Management (Section 16) – This domain focuses on a consistent and effective approach to the management of information security incidents, including detection, reporting, response, escalation, and forensic practices	**إدارة حوادث أمن المعلومات (القسم 16)** - يركز هذا المجال على نهج متسق وفعال لإدارة حوادث أمن المعلومات ، بما في ذلك الكشف والإبلاغ والاستجابة والتصعيد وممارسات الطب الشرعي
Business Continuity (Section 17) – This domain focuses on availability and the secure provision essential services during a disruption of normal operating .conditions	**استمرارية الأعمال (القسم 17)** - يركز هذا المجال على التوافر وعلى الخدمات الأساسية الآمنة أثناء حدوث خلل في ظروف التشغيل العادية.
Compliance Management (Section 18) – This domain focuses on conformance with internal policy; local, national, and international criminal and civil laws; regulatory or contractual obligations; intellectual property rights (IPR); and copyrights	**إدارة الالتزام (القسم 18)** - يركز هذا المجال على التوافق مع السياسة الداخلية ؛ القوانين الجنائية والمدنية المحلية والوطنية والدولية ؛ التزامات تنظيمية أو تعاقدية ؛ حقوق الملكية الفكرية (IPR) ؛ وحقوق النشر

Summary

- The CIA triad is the blueprint of what assets needs to be protected to protect the organization.
- Protecting the organization's information security can seem vague and too conceptual. Protecting the confidentiality, integrity, and availability of the data is a concrete way of saying the same thing.
- Standards such as the ISO 27002 exist to help organizations better define appropriate ways to protect their information assets.

الملخص

- ثلاثي CIA هو مخطط لما تحتاجه الأصول لحماية المؤسسة.
- قد تبدو حماية أمن معلومات المنظمة غامضة ومفهومة أكثر من اللازم. إن حماية سرية البيانات وتكاملها وتوافرها هي طريقة ملموسة للقول بنفس الشيء.
- توجد معايير مثل ISO 27002 لمساعدة المؤسسات على تحديد الطرق المناسبة لحماية أصول معلوماتها بشكل أفضل.