01- Comparing Security Roles and Security Controls

مقارنة قواعد الأمن وضوابط الأمن

Ahmed Sultan
Senior Technical Instructor
ahmedsultan.me /about

Outlines

1.1- Compare and Contrast Information Security Roles

1.2- Compare and Contrast Security Control And Framework Types

1.1- Compare and Contrast Information Security Roles

1.2- Compare and Contrast Security Control And Framework Types

INFORMATION SECURITY

Information Security (or infosec) refers to the protection of data resources from unauthorized access, attack, theft, or damage.Data may be vulnerable because of the way it is stored, the way it is transferred,or the way it is processed.

يشير أمان المعلومات (أو infosec) إلى حماية موارد البيانات من الوصول غير المصرح به أو الهجوم أو السرقة أو التلف.
قد تكون البيانات عرضة للخطر بسبب طريقة تخزينها أو طريقة نقلها أو طريقة معالجتها.

Secure information has three properties, often referred to as the CIA Triad:

المعلومات الآمنة لها ثلاث خصائص ، يشار إليها غالبًا باسم CIA Triad :

Confidentiality: means that certain information should only be known to certain people.

السرية: تعني أن بعض المعلومات يجب أن تكون معروفة لأشخاص معينين

Integrity: means that the data is stored and transferred as intended and that any modification is authorized.

النزاهة: تعني أن البيانات يتم تخزينها ونقلها على النحو المنشود كالتعديل مصرح به.

Availability: means that information is accessible to those authorized to view or modify it

التوافر: يعني أن المعلومات يمكن الوصول إليها من قبل المصرح لهم بمشاهدتها أو تعديلها.

INFORMATION SECURITY (cont.)

- Some security models and researchers identify other properties that secure systems should exhibit.
- تحدد بعض نماذج الأمان والباحثين الخصائص الأخرى التي يجب أن تظهرها الأنظمة الآمنة.
- The most important of these is **non-repudiation**. وأهمها عدم الإنكار
- **Non-repudiation** means that a subject cannot deny doing something, such as creating, modifying, or sending a resource.
- عدم الإنكار يعني أن الشخص لا يمكنه إنكار القيام بشيء ما ، مثل إنشاء أو تعديل أو إرسال مورد.
- **For Example:** a legal document, such as a will, must usually be witnessed when it is signed.If there is a dispute about whether the document was correctly executed, the witness can provide evidence that it was.
- على سبيل المثال: الوثيقة القانونية ، مثل الوصية ، يجب أن تشهد عادة عند توقيعها.إذا كان هناك نزاع حول ما إذا تم تنفيذ المستند بشكل صحيح ، يمكن للشاهد تقديم دليل على ذلك.

INFORMATION SECURITY COMPETENCIESكفاءات أمن المعلومات

- IT professionals working in a role with security responsibilities must be competent in a wide range of disciplines, from network and application design to procurement and human resources (HR).
يجب أن يكون محترفو تكنولوجيا المعلومات الذين يعملون في دور بمسؤوليات أمنية أكفاء في مجموعة واسعة من التخصصات ، من تصميم الشبكة والتطبيق إلى المشتريات والموارد البشرية (HR).

- The following activities might be typical of such a role:

Participate in risk assessments and testing of security systems and make recommendations. ✓

✓ المشاركة في تقييمات المخاطر واختبار أنظمة الأمان وتقديم التوصيات.

Specify, source, install, and configure secure devices and software ✓

✓ تحديد الأجهزة والبرامج الآمنة ومصدرها وتثبيتها وتكوينها.

Manage security-related incident response and reporting ✓

✓ إدارة الاستجابة للحوادث المتعلقة بالأمن والإبلاغ عنها..

Create and test business continuity and disaster recovery plans and procedures ✓

✓ إنشاء واختبار خطط وإجراءات استمرارية الأعمال والتعافي من الكوارث.

Participate in security training and education programs ✓

المشاركة في برامج التدريب والتعليم الأمني..

INFORMATION SECURITY ROLES AND RESPONSIBILITIES

- A **Security Policy** is a formalized statement that defines how security will be implemented within an organization. It describes the means the organization will take to protect the confidentiality, availability, and integrity of sensitive data and resources.

سياسة الأمن هي بيان رسمي يحدد كيفية تنفيذ الأمن داخل المؤسسة.ويصف الوسائل التي ستتخذها المنظمة لحماية سرية وتوافر وسلامة البيانات والموارد الحساسة.

- The implementation of a security policy to support the goals of the CIA triad might be very different for a school, a multinational accountancy firm, or a machine tool manufacturer.

قد يكون تنفيذ سياسة أمنية لدعم أهداف (سي آي أي) مختلفًا تمامًا بالنسبة لمدرسة، أو شركة محاسبة متعددة الجنسيات، أو شركة تصنيع الأدوات الآلية.

- However, each of these organizations, or any other organization should have the same interest in ensuring that its employees, equipment, and data are secure against attack or damage.

- ومع ذلك ، يجب أن يكون لكل من هذه المؤسسات أو أي مؤسسة أخرى نفس المصلحة في ضمان حماية موظفيها ومعداتها وبياناتها من الهجوم أو التلف.

INFORMATION SECURITY ROLES AND RESPONSIBILITIES

- As part of the process of adopting an effective organizational security posture, employees must be aware of their responsibilities. كجزء من عملية تبني موقف أمان تنظيمي فعال ، يجب أن يكون الموظفون على دراية بمسؤولياتهم
- The structure of security responsibilities will depend on the size and hierarchy ofan organization, but these roles are typical .
- سيعتمد هيكل المسؤوليات الأمنية على حجم المؤسسة وتسلسلها الهرمي ، ولكن هذه الأدوار نموذجية.

Overall internal responsibility for security might be allocated to a dedicated department, run by a **Director of Security, Chief Security Officer (CSO)**, or **Chief Information Security Officer (CISO)**. ✓
قد يتم تخصيص المسؤولية الداخلية العامة للأمن إلى إدارة مخصصة ، يديرها مدير الأمن ، أو كبير مسؤولي الأمن (CSO، أو كبير مسؤولي أمن المعلومات CISO).

Managers may have responsibility for a domain, such as building control, ICT, or accounting ✓
قد يتحمل المديرون مسؤولية مجال ما ، مثل مراقبة البناء أو تكنولوجيا المعلومات والاتصالات أو المحاسبة.

Technical and specialist staff have responsibility for implementing, maintaining, and monitoring the policy. ✓
يتحمل الموظفون الفنيون والمتخصصون مسؤولية تنفيذ السياسة والحفاظ عليها ✓

Non-technical staff have the responsibility of complying with policy and with any relevant legislation ✓
يتحمل الموظفون غير الفنيين مسؤولية الامتثال للسياسة وأي تشريعات ذات صلة... ✓

INFORMATION SECURITY BUSINESS UNITS

Security Operations Center (SOC)1.

- A **security operations center (SOC)** is a location where security professionals monitor and protect critical information assets across other business functions, such as finance, operations, sales/marketing, and so on.
- مركز عمليات الأمان (SOC) هو موقع يقوم فيه متخصصو الأمن بمراقبة أصول المعلومات الهامة وحمايتها عبر وظائف العمل الأخرى ، مثل التمويل والعمليات والمبيعات / التسويق وما إلى ذلك.

INFORMATION SECURITY BUSINESS UNITS (cont.)

2. Incident Response الاستجابة للحادث

- A dedicated **cyber incident response team (CIRT)/computer security incident response team (CSIRT)/computer emergency response team (CERT)** as a single point-of-contact for the notification of security incidents.
- This function might be handled by the **SOC**, or it might be established as an independent business unit.

(CERT فريق الاستجابة للطوارئ على الكمبيوتر / (CSIRT فريق الاستجابة لحوادث أمن الكمبيوتر / (CIRT فريق الاستجابة للحوادث السيبرانية)
، أو قد يتم تأسيسها كوحدة أعمال مستقلة. SOC كنقطة اتصال واحدة للإخطار بالحوادث الأمنية.قد يتم التعامل مع هذه الوظيفة بواسطة

1.1- Compare and Contrast Information Security Roles

1.2- Compare and Contrast Security Control And Framework Types

SECURITY CONTROL CATEGORIES فئات الضوابط الأمنية

- Information and cybersecurity assurance is usually considered to take place within an overall process of **business risk management**.

عادةً ما يتم اعتبار ضمان أمن المعلومات والأمن السيبراني يتم ضمن عملية شاملة لإدارة مخاطر الأعمال

Implementation of cybersecurity functions is often the **responsibility of the IT department**.

غالبًا ما يكون تنفيذ وظائف الأمن السيبراني من مسؤولية قسم تكنولوجيا المعلومات

- Some organizations have developed IT service frameworks to provide best practice guides to implementing IT and cybersecurity.
- طورت بعض المنظمات أطر عمل لخدمات تكنولوجيا المعلومات لتوفير أدلة أفضل الممارسات لتنفيذ تكنولوجيا المعلومات والأمن السيبراني

These frameworks can shape company policies and provide checklists of procedures, activities, and technologies that should ideally be in place.

يمكن لهذه الأطر أن تشكل سياسات الشركة وتوفر قوائم مرجعية للإجراءات والأنشطة والتقنيات التي يجب أن تكون في مكانها المثالي.

SECURITY CONTROL CATEGORIES (cont.)

- A **Security Control** is something designed to give a system or data asset the properties of **confidentiality**, **integrity**, **availability**, and **non-repudiation**.
- الضوابط الأمنية هو شيء مصمم لمنح نظام أو أصل بيانات خصائص السرية والتكامل والتوافر وعدم التنصل.
- Controls can be divided into three broad categories, representing the way the control is implemented: يمكن تقسيم الضوابط إلى ثلاث فئات عريضة ، تمثل طريقة تنفيذ الضوابط :

Technical—the control is implemented as a system (hardware, software, or firmware), For example, firewalls, antivirus software, and OS access control models are technical controls. Technical controls may also be described as logical controls ✓

فني - يتم تنفيذ الضوابط كنظام (جهاز أو برنامج أو برنامج ثابت) ، على سبيل المثال ، تعد جدران الحماية وبرامج مكافحة الفيروسات ونماذج التحكم في الوصول إلى نظام التشغيل عناصر الضوابط الفنية.

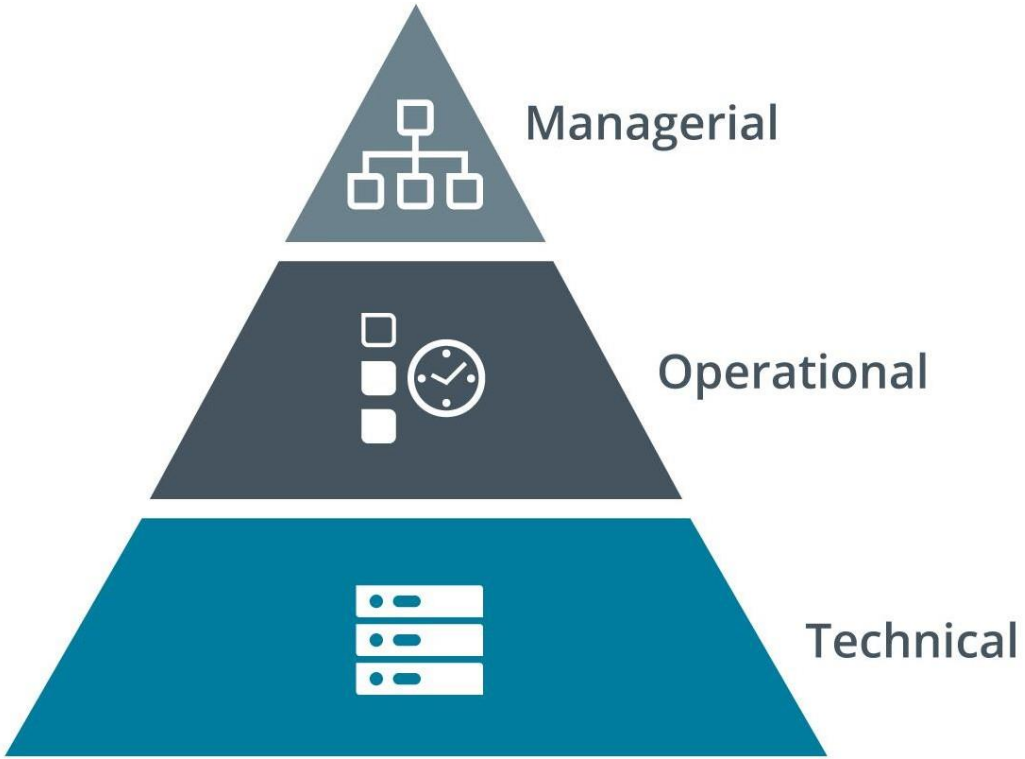
Operational—the control is implemented primarily by people rather than systems, For example, security guards and training programs are operational controls rather than technical controls. تشغيلي ✓

- يتم تنفيذ الضوابط بشكل أساسي من قبل الأشخاص بدلاً من الأنظمة ، على سبيل المثال ، حراس الأمن وبرامج التدريب عبارة عن ضوابط تشغيلية وليست ضوابط تقنية.

Managerial—the control gives oversight of the information system, Examples could include risk identification or a tool allowing the evaluation and selection of other security controls ✓

إداري - يوفر عنصر التحكم الإشراف على نظام المعلومات ، ويمكن أن تشمل الأمثلة تحديد المخاطر أو أداة تسمح بالتقييم واختيار عناصر ضوابط امنية اخرى.. ✓

SECURITY CONTROL CATEGORIES (cont.)



SECURITY CONTROL FUNCTIONAL TYPES

- Security controls can also be classified in types according to the **goal** or **function** they perform: يمكن أيضًا تصنيف عناصر التحكم في الأمان إلى أنواع وفقًا للهدف أو الوظيفة التي تؤديها:

✓ Preventive—the control acts to eliminate or reduce the likelihood that an attack can succeed, A preventative control **operates before an attack can take place**, Access control lists (ACL) configured on firewalls and file system objects are preventative-type controls, Anti-malware software also acts as a preventative control, by blocking processes identified as malicious from executing.

✓ وقائي - يعمل عنصر التحكم على القضاء على احتمالية نجاح الهجوم أو تقليله ، ويعمل عنصر التحكم الوقائي قبل حدوث هجوم ، وقوائم التحكم في الوصول (ACL) التي تم تكوينها على جدران الحماية وكائنات نظام الملفات هي عناصر تحكم من النوع الوقائي ، ومكافحة البرامج الضارة يعمل البرنامج أيضًا كعنصر تحكم وقائي ، عن طريق منع العمليات التي تم تحديدها على أنها ضارة من التنفيذ.

Detective—the control may not prevent or deter access, but it will identify and record any attempted or successful intrusion, A detective control **operates during the progress of an attack**, Logs provide one of the best examples of detective-type controls. الكشف - قد لا يمنع عنصر التحكم الوصول أو يردعه ، ولكنه سيحدد ويسجل أي محاولة اقتحام ناجح أو محاولة اقتحام ناجحة ، ويعمل عنصر تحكم الكشف أثناء تقدم الهجوم ، وتوفر السجلات أحد أفضل الأمثلة على عناصر التحكم من نوع المخبر.

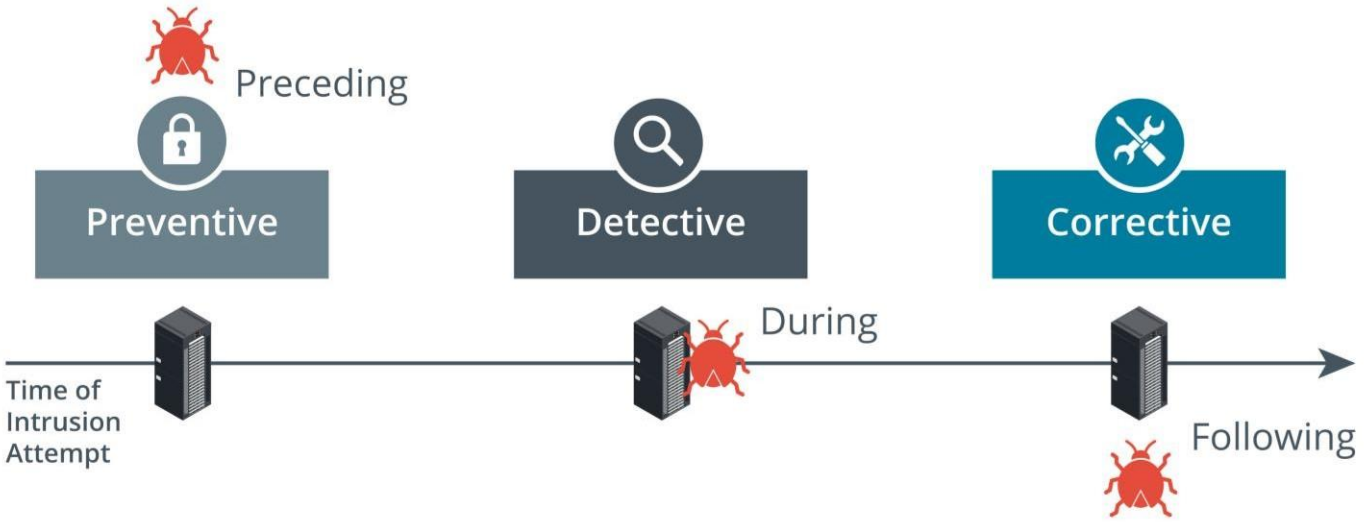
SECURITY CONTROL FUNCTIONAL TYPES (cont.)

- Security controls can also be classified in types according to the **goal** or **function** they perform (cont.)

Corrective—the control acts to eliminate or reduce the impact of an intrusion event, ✓
A corrective control is **used after an attack**, A good example is a backup system that can restore data that was damaged during an intrusion, Another example is a patch management system that acts to eliminate the vulnerability exploited during the attack.

✓ تصحيحي - يعمل عنصر التحكم على القضاء على تأثير حدث التسلل أو تقليله ، ويتم استخدام عنصر تحكم تصحيحي بعد الهجوم ، ومن الأمثلة الجيدة على ذلك نظام النسخ الاحتياطي الذي يمكنه استعادة البيانات التي تعرضت للتلف أثناء التطفل ، ومثال آخر هو نظام إدارة التصحيح يعمل على القضاء على الثغرة الأمنية التي تم استغلالها أثناء الهجوم

SECURITY CONTROL FUNCTIONAL TYPES (cont.)



Other Control Functional Types:

- Physical
- Compensating
- Deterrent

SECURITY CONTROL FUNCTIONAL TYPES (cont.)

- While most controls can be classed functionally as preventative, detective, or corrective, a few other types can be used to define other cases:
- يمكن تصنيف معظم عناصر الضوابط وظيفيًا على أنها وقائية أو استقصائية أو تصحيحية ، يمكن استخدام بعض الأنواع الأخرى لتحديد الحالات الأخرى:

Physical—controls such as alarms, gateways, locks, lighting, security cameras, and guards that deter and detect access to premises and hardware are often classed separately. ✓

✓ المادية — عناصر التحكم مثل أجهزة الإنذار ، والبوابات ، والأقفال ، والإضاءة ، وكاميرات الأمان ، والحراس الذين يردع ويكتشفون الوصول إلى المباني والأجهزة ، غالبًا ما يتم تصنيفهم بشكل منفصل.

Deterrent—the control may not physically or logically prevent access, but psychologically discourages an attacker from attempting an intrusion, This could include signs and warnings of legal penalties against trespass or intrusion. ✓

✓ الرادع - قد لا يمنع عنصر التحكم الوصول ماديًا أو منطقيًا ، ولكنه لا يشجع المهاجم نفسيًا على محاولة التطفل ، وقد يشمل ذلك إشارات وتحذيرات من عقوبات قانونية ضد التعدي أو التطفل.

Compensating—the control serves as a substitute for a principal control, as recommended by a security standard, and affords the same (or better) level of protection but uses a different methodology or technology ✓

التعويض - تعمل أداة التحكم كبديل لعنصر تحكم رئيسي ، على النحو الموصى به في معيار الأمان ، وتوفر نفس مستوى الحماية (أو أفضل منه) ولكنها تستخدم منهجية أو تقنية مختلفة..