Computer-Based Information Systems Auditing

الاستاذ المساعد الدكتور
اسعد محمد علي وهاب العواد

Learning Objectives

- Describe the threats to an AIS and discuss why these threats are growing.
  - وصف تهديدات نظم معلومات المحاسبة ومناقشة لماذا هذه التهديدات المتزايدة.
- Explain the basic concepts of control as applied to business organizations.
  - شرح المفاهيم الاساسية للرقابة على النحو المطبق في منظمات الاعمال.
- Describe the major elements in the control environment of a business organization.
  - وصف العناصر الرئيسية للرقابة في بيئة منظمات الأعمال التجارية.

Introduction

- This part discusses the types of threats a company faces.
  - يناقش هذا الجزء انواع التهديدات التي تواجهها الشركة.

Learning Objectives, continued

- Describe control policies and procedures commonly used in business organizations.
- وصف سياسات الرقابة والإجراءات التي تستخدم عادة في منظمات الاعمال.
- Evaluate a system of internal accounting control, identify its deficiencies, and prescribe modifications to remedy those deficiencies.
- تقييم نظام الرقابة المحاسبيه الداخلية ، وتحديد أوجه القصور ، وفرض تعديلات لتداركها.
- Conduct a cost-benefit analysis for particular threats, exposures, risks, and controls.
- اجراء تحليل للتكلفة والعائد للتهديدات والتعرض للمخاطر.

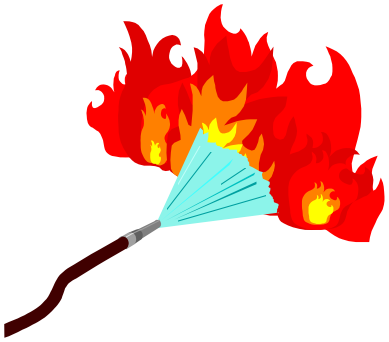
Learning Objective 1

Describe the threats to an AIS and discuss why these threats are growing.

Threats to Accounting Information Systems
الاخطار التي تهدد نظم المعلومات المحاسبية

- What are examples of *natural and political disasters*?
- ما هي الامثلة على الكوارث الطبيعية والسياسية؟

  - fire or excessive heat
  - الحرائق
  - Floods
  - الفيضانات
  - Earthquakes
  - الزلازل
  - high winds
  - الاعصار
  - War
  - الحروب



Threats to Accounting Information Systems

- What are examples of *software errors and equipment malfunctions*?
  - ما هي الامثلة على مشاكل البرمجيات و اعطال المعدات؟

  - hardware failures
    - فشل الاجهزة
  - power outages and fluctuations
    - انقطاع وتقلبات التيار الكهربائي
  - undetected data transmission errors
    - عدم اكتشاف اخطاء تراسل البيانات

Threats to Accounting Information Systems

- What are examples of *unintentional acts*?
  - ما هي الامثلة على الافعال غير مقصودة؟
    - accidents caused by human carelessness
    - الحوادث الناجمة عن اهمال الانسان
    - innocent errors of omissions
    - أخطاء السهو
    - lost or misplaced data
    - فقدان البيانات
    - logic errors
    - الاخطاء المنطقية
    - systems that do not meet company needs
    - النظم التي لا تلبي احتياجات الشركة

Threats to Accounting Information Systems

- What are examples of *intentional acts*?
- ما هي امثلة على الافعال المقصودة؟
  - Sabotage
  - التخريب
  - computer fraud
  - الاحتيال
  - Embezzlement
  - الاختلاس

انواع الهجمـات والاعتداءات وأساليبها التقنية

- **التهديد Threats :** ويعني الخطر المحتمل الذي يمكن ان يتعرض له نظام المعلومات وقد يكون شخصا ، كالمتجسس او المجرم المحترف او الهاكرز المخترق ، او شيئا يهدد الاجهزة او البرامج او المعطيات ، او حدثا كالحريق وانقطاع التيار الكهربائي والكوارث الطبيعية .
- **نقاط الضعف او الثغرات Vulnerabilities :** وتعني عنصر او نقطة او موقع في النظام يحتمل ان ينفذ من خلاله المعتدي او يتحقق بسببه الاختراق وتعتبر نقاط الضعف هي الأسباب المحركة لتحقيق التهديدات او المخاطر . ويرتبط بهذا الاصطلاح اصطلاح **وسائل الوقاية Countermeasures :** وتعني التكنيك المتبع لحماية النظام ككلمات السر والأقفال ووسائل الرقابة والجدران النارية وغيرها .

تابع .. انواع الهجمـات والاعتداءات وأساليبها التقنية

- **المخاطر Risks :** فانها تستخدم بشكل مترادف مع تعبير التهديد ، مع انها حقيقة تتصل بأثر التهديدات عند حصولها ، وتقوم استراتيجية أمن المعلومات الناجحة على تحليل المخاطر Risk analysis ، وتحليل المخاطر هي عملية Process وليست مجرد خطة محصورة ، وهي تبدأ من التساؤل حول التهديدات ثم نقاط الضعف واخيرا وسائل الوقاية المناسبة للتعامل مع التهديدات ووسائل منع نقاط الضعف .
- **اما الحوادث Incident :-** فهو اصطلاح متسع يشمل المخاطر ويشمل الأخطاء ، وهو بالمعنى المستخدم في دراسات أمن المعلومات التقنية يشير الى الأفعال المقصودة او غير المقصودة.
- **اما الهجمات Attacks** فهو اصطلاح لوصف الاعتداءات بنتائجها او بموضع الاستهداف ، فنقول هجمات انكار الخدمة ، او هجمات إرهابية ، او هجمات البرمجيات ، او هجمات الموظفين الحاقدة او الهجمات المزاحية . ويستخدم كاصطلاح رديف للهجمات اصطلاح الاختراقات او الاخلالات Breaches، وهو اصطلاح توصف به مختلف انماط الاعتداءات التقنية ، وبالتالي يكون مرادفا أيضا للاعتداءات.

Why are AIS Threats Increasing?

- Increasing numbers of client/server systems mean that information is available to an unprecedented number of workers.
  - نمو الانظمة على نموذج الشبكات العملاء / خادم يعني ان نظم المعلومات متاحة للعدد كبير من المستخدمين.
- Because LANs and client/server systems distribute data to many users, they are harder to control than centralized mainframe systems.
  - نسبة لتوزيع البيانات للعديد من المستخدمين في نطاق الشبكات المحلية وشبكة العميل / الخادم من الصعوبة التحكم والرقابة على تدفق البيانات مقارنة بالمركزية في نظم الحاسوب المركزي.
- WANs are giving customers and suppliers access to each other's systems and data, making confidentiality a concern.
  - الشبكات الواسعة تتيح للزبائن والموردين وصول كل منهما الى النظم والبيانات ، مما يزيد القلق في مسائل السرية والموثوقية.

Learning Objective 2

Explain the basic concepts of control as applied to business organizations.

Overview of Control Concepts

What is the traditional definition of internal control?

ما هو التعريف التقليدي للرقابة الداخلية؟

Internal control is the plan of organization and the methods a business uses to safeguard assets, provide accurate and reliable information, promote and improve operational efficiency, and encourage adherence to prescribed managerial policies.

الرقابة الداخلية هي خطة منظمة وأساليب تجارية تستخدم لحماية الاصول ، وتوفير معلومات دقيقة وموثوقة ، وتعزيز وتحسين الكفاءة التشغيلية ، والحث على التقييد بنصوص السياسات الادارية.

Overview of Control Concepts

- What is management control? ما هى الرقابة الادارية؟
- Management control encompasses the following three features:
- الرقابة الادارية تشمل السمات الثلاثة التالية :

1. It is an integral part of management responsibilities.
1. هى جزء لا يتجزأ من مسؤوليات الادارة.
2. It is designed to reduce errors, irregularities, and achieve organizational goals.
2. وهى مصممة للحد من الأخطاء ، والمخالفات ، وتحقيق الأهداف التنظيمية للمؤسسة.
3. It is personnel-oriented and seeks to help employees attain company goals.
3. ومن منظور شئون العاملين تسعى الى مساعدة الموظفين على تحقيق أهداف المؤسسة.

Internal Control Classifications

- The specific control procedures used in the internal control and management control systems may be classified using the following four internal control classifications:
- اجراءات الرقابة المستخدمة في الرقابة الداخلية وإدارة نظم المراقبة ويمكن تصنيفها وفق تصنيفات للرقابة الداخلية التالية :

1. Preventive, detective, and corrective controls
2. General and application controls
3. Administrative and accounting controls
4. Input, processing, and output controls

Learning Objective 2

Describe the major elements in the control environment of a business organization.

The Control Environment

- The control environment consists of many factors, including the following:
- بيئة المراقبة تتكون من عدة عوامل ، بما في ذلك ما يلي :

1. Commitment to integrity and ethical values
1. الالتزام والنزاهة والقيم الاخلاقية
2. Management's philosophy and operating style
2. فلسفة الادارة وأسلوب التشغيل
3. Organizational structure
3. الهيكل التنظيمي للمؤسسة

The Control Environment

4 The audit committee of the board of directors

4 لجنة مراجعة الحسابات من مجلس الادارة

5 Methods of assigning authority and responsibility

5 اساليب اسناد السلطة والمسؤولية

6 Human resources policies and practices

6 الموارد البشرية والسياسات والممارسات

7 External influences

7 التأثيرات الخارجية

Learning Objective 3

Describe control policies and procedures commonly used in business organizations.

Control Activities

- Generally, control procedures fall into one of five categories:
- وبصفة عامة ، اجراءات الرقابة تندرج في واحدة من خمس فئات هي :

1. Proper authorization of transactions and activities
1. الترخيص اللازم للمعاملات والأنشطة
2. Segregation of duties
2. الفصل بين الواجبات
3. Design and use of adequate documents and records
3. تصميم واستخدام ما يكفي من الوثائق والسجلات
4. Adequate safeguards of assets and records
4. ضمانات كافية من الاصول والسجلات
5. Independent checks on performance
5. الاستقلالية في مراقبة الاداء

Proper Authorization of Transactions and Activities

- *Authorization* is the empowerment management gives employees to perform activities and make decisions.
  - اذن هو تمكين الادارة ويعطي الموظفين صلاحيات اداء انشطة واتخاذ القرارات.
- *Digital signature* or fingerprint is a means of signing a document with a piece of data that cannot be forged.
  - بصمات الاصابع او التوقيع الرقمي هو وسيلة من التوقيع على وثيقة بيانات لا يمكن تزويرها.
- *Specific authorization* is the granting of authorization by management for certain activities or transactions.
  - اذن محدد هو منح الترخيص من قبل الادارة لأنشطة معينة او المعاملات.

Segregation of Duties

- Good internal control demands that no single employee be given too much responsibility.
- المراقبة الداخلية الجيدة عدم تحميل الموظف الكثير من المسؤوليات.
- An employee should not be in a position to perpetrate and conceal fraud or unintentional errors.
- الموظف لا ينبغى ان يكون فى وضع يمكنه من اخفاء أو ارتكاب الغش او الاخطاء غير المقصودة.

Segregation of Duties

Custodial Functions
Handling cash
Handling assets
Writing checks
Receiving checks in mail

Recording Functions
Preparing source documents
Maintaining journals
Preparing reconciliations
Preparing performance reports

Authorization Functions
Authorization of transactions

Segregation of Duties

- If two of these three functions are the responsibility of a single person, problems can arise.
- اذا كانت اثنتان من هذه الوظائف الثلاث هي من مسؤولية شخص واحد ، يمكن ان تنشأ مشاكل.
- Segregation of duties prevents employees from falsifying records in order to conceal theft of assets entrusted to them.
- يجب الفصل بين الواجبات ويمنع الموظفين من تزوير في السجلات بغية اخفاء سرقة الاصول الموكلة اليهم.

Segregation of Duties

Segregation of duties prevents an employee from falsifying records to cover up an inaccurate or false transaction that was inappropriately authorized.

الفصل بين الواجبات يمنع موظف من تزوير السجلات للتغطية على وجود صفقة غير دقيقة أو كاذبة.

قوائم المراجعة والتدقيق وإطار بناء خطط واستراتيجيات الأمن

هناك العديد من قوائم التدقيق والمراجعة حول مسائل أمن المعلومات ومتطلبات سياسات واستراتيجيات أمن المعلومات والنظم والاتصالات ، وتقوم بالأساس على توفير نوع من دليل المراجعة الذي يساعد المؤسسات او الافراد في بناء أسس الأمن وتحديد اطار عام لواجبات الموظفين والمستشارين و المعنيين بشؤون ادارة نظم المعلومات والاتصال وتطبيقاتهما وبنفس الوقت تقدم هذه القوائم او ادلة المراجعة للمؤسسات والأفراد اطار عاما لفهم عناصر ومتطلبات بناء نظم الأمن الخاصة بالكمبيوتر والشبكات .

المسائل التي تعالجها عادة هذه القوائم

- مسائل **واجبات جهات الادارة** للتحقق من وجود سياسة أمن المعلومات موثقة ومكتوبة والتحقق من وجود عمليات تحليل المخاطر وخطة الأمن وبناء الأمن التقني وسياسة ادارة الاتصالات الخارجية ، ومدى معرفة وإطلاع الموظفين على السياسة الأمنية ومعرفتهم بواجباتهم ، ومدى توفر تدريب على مسائل الأمن وما اذا كان يخضع الموظفون الجدد لتدريب وتعريف حول محتوى الخطة .
- مسائل **تنظيم شؤون ادارة الأمن** ، والتي تتعلق بوجود جهة مختصة بذلك في المؤسسة وما اذا كان هنالك دليل مكتوب ، وخطط ومسؤولية التعامل مع إجراءات التنفيذ والتعريف والتعامل مع الحوادث ومع خطط الطوارئ وغيرها.
- مسائل **الموظفين أنفسهم** من حيث مدى فحص التأهيل والكفاءة ومدى التزام الموظفين بتحقيق معايير الأمن على المستوى الشخصي او فيما يتعلق بواجباتهم ، وأغراضها المتصلة بالأمن لدى تعيين الموظفين وخلال عملهم ولدى انتهاء خدمتهم لأي سبب ، وتتصل أيضا بمدى توفر نصوص عقدية خاصة في عقود الموظفين ومدى توفر وصف دقيق بوجباتهم الوظيفية المتصلة بإلحاق المعلومات .
- مسائل **جهات تزويد الخدمة او المشورة** كالمستشارين والمدققين وغيرهم من حيث تغطية عقود التعامل معهم لمسائل الأمن المختلفة .

تابع .. المسائل التي تعالجها عادة هذه القوائم

- مسائل **تصنيف المعلومات** من حيث توفرها ومعاييرها .
- مسائل **البرمجيات** من حيث سياسات شرائها واستخدامها وتنزيلها ومسائل الرخص المتصلة بها وآليات التعامل مع البرمجيات المطورة داخليا وحقوق الوصول اليها واستخدامها ، ومسائل حماية البرمجيات التقنية والقانونية .
- مسائل **الاجهزة والمعدات** من حيث توفر تصور للاحتياجات وتوفير المتطلبات ومعايير توظيف الاجهزة في العمل ، واستخداماتها وإلغاء استخدامها ومسائل صيانة والتدقيق .
- مسائل **التوثيق** ، وهي الذي تتعلق مدى توفر استراتيجية توثيق لكافة عناصر النظام ولكافة مرتكزات وعمليات خطط الأمن وسياساتها.
- المسائل المتصلة **بوسائط التخزين خارج النظام** من حيث تحديد وسائط التخزين المستخدمة وتبويبها وحفظها والوصول اليها وتبادلها وإتلافها .
- مسائل **التعريف والتوثق** من شخصية المستخدم وحدود صلاحيات والتفويض ، وتتعلق بالتحقق من توفر سياسة التحكم بهذه العناصر والوسائل المستخدمة في تحديد الهوية والتوثق من المستخدم ، واستراتيجيات حماية وسائل التعريف تقنيا وإداريا، ومدى صلاحية المستخدمين من الخارج او من داخل المؤسسة بشأن الوصول للمعلومات او قطاعات منها ، ومسائل التحقق من تصرفات المستخدم ، مسائل أمن النظام من حيث توفر وسائل التثبت من حيث وقت الاستخدام و المستخدمين .

تابع .. المسائل التي تعالجها عادة هذه القوائم

- مسائل **الاتصالات** من حيث السيطرة على وسائل وتطبيقات الاتصالات الداخلية والخارجية وتوثيق حركات الاتصال وحماية عمليات الاتصال والمعايير التقنية المستخدمة في ذلك واستراتيجيات سرية ورقابة وتتبع واستخدام البريد الإلكتروني .
- مسائل **ادارة الملفات وسجلات الأداء** واستخدام النظام من حيث توفر وسائل توثيقها وارشفتها والتثبت من جهات الانشاء والتعديل والتعامل مع الملفات وقواعد البيانات والبرامج التطبيقية .
- مسائل **النسخ الاحتياطية** من البيانات من حيث وقت عمل النسخ الاحتياطية وتخزينها واستخداماتها وتبويبها وتوثيقها وتشفيرها اذا كانت مما يتطلب ذلك .
- مسائل **الحماية المادية** من حيث التوثق من توفير وسائل وإجراءات الحماية للاجهزة الكمبيوتر والشبكات والبنى التحتية من ومسائل الطاقة والتوصيلات ومدى توفر وسائل الوقاية من الحوادث الطبيعة او المتعمدة اضافة الى وسائل حماية مكان وجود الاجهزة والوسائط وادلة الأمن المكتوبة ، والوسائل المادية للوصول الى الاجهزة واستخدامها من المخولين بذلك .
- مسائل **التعامل مع الحوادث والاعتداءات** ، من حيث توفر فريق لذلك وأغراضها التي يقوم بها الفريق لهذه الغاية اضافة الى وجود ارتباط مع جهات التحقيق الرسمية وجهات تطبيق القانون وجهات الخبرة المتخصصة بالمسائل المعقدة او التي لا تتوفر كفاءات للتعامل معها داخل المؤسسة .
- مسائل **خطط الطوارئ وخطط التعافي** لتخفيف الاضرار والعودة للوضع الطبيعي .
- مسائل **الاعلام** المتعلقة بالمعلومات المتعين وصولها للكافة او لقطاعات محددة والتحقق من وضوح استراتيجية التعامل الاعلامي مع الحوادث والاعتداءات المتحققة .