

PMG 611

Enterprise Risk Management

Prepared by Dr. Abdullah Jameel Halawany

جامعة الجميع الذكية

تسعى لتكون الكيان الأول الذي يتبنى مبدأ المجتمع التعليمي
التعاوني ويقدم العلم مقابل العمل لتنمية وبناء المجتمعات.

Lecture 10

Cybersecurity and Information
Technology and ERM



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

Lecture 10

Session Outline

IT And The
ERM
Framework

IT Application
Systems Risks

Effective IT
Continuity
Planning

Worms,
Viruses, And
System
Network Risks



Lecture 10

Introduction



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

- IT is so pervasive in all business and operations processes.
- IT is also a challenging area for understanding risks and developing appropriate risk responses.
- As has been the pattern over the years, no matter how strong are the designed and implemented internal controls—particularly those that are software based—someone will find a way to violate and get around them.

- Because of the complexity in building and maintaining Information Technology (IT) systems, their network interconnections, and all types of applications, Risk Management has been a very important consideration in all aspects of IT processes.
- One does not have to have been a participant or observer of IT hardware and software projects for that many years to have observed many IT projects that were launched with high expectations but subsequently failed for any of a variety of reasons.

- Just as people involved in marketing often have overly high expectations that some new initiative will succeed, IT processes often have high, positive expectations but ignore the many business and technology risks associated with IT systems.
- Digital transformation era.

- 90% of organizations in North American that are engaged in Digital Transformation acknowledge their risk profiles have expanded due to their digital initiatives.
- Managing *Cybersecurity Risks* is the top risk management objective for decision makers at organizations engaged in Digital Transformation.

- On any given day, there are numerous media reports about significant cyber incidents.
- Organizations of all types and sizes are susceptible to cyber attacks.
- Which data, systems, and assets are of value at any particular point in time depends on the cyber attacker's motives.

- As long as cyber incidents continue to have a negative impact on the reputation and financial well-being of victim companies and continue to draw *additional regulatory* and legal scrutiny, cyber breaches will continue to be high profile events that draw a substantial amount of negative press.

- Digital incidents are now costing small businesses \$200,000 on average, according to insurance carrier Hiscox, and 60% going out of business within six months of being victimized.
- The frequency with which these attacks are happening is also increasing, with more than half of all small businesses having suffered a breach and 4 in 10 having experienced multiple incidents.

Lecture
10

IT And The COSO Erm Framework



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

- Information systems general controls include hardware, software, and administrative control procedures that apply to all systems and applications, including:
 - Reliability of information systems processing
 - Integrity of programs, including configuration management
 - Controls of the proper development and implementation of systems.
 - Continuity of processing
 - Controls of Application Inputs
 - Self-balancing and other financial and data controls
 - Application output components

Lecture 10

IT And The COSO Erm Framework

ENTERPRISE RISK MANAGEMENT



Source: COSO

- *Governance and Culture* (sets the entity's tone, reinforcing the importance of cyber vigilance and establishing oversight responsibilities for the entity)
- *Strategy and Objective-Setting* (Cyber risk management should integrated)
- *Performance* (identifies and assesses cyber risks that may affect the achievement of that strategy and business objectives)
- *Review and Revision* (reviewing cyber risk management capabilities and practices, and the entity's performance relative to its targets)
- *Information, Communication, and Reporting*

- *Governance and Culture* (sets the entity's tone, reinforcing the importance of cyber vigilance and establishing oversight responsibilities for the entity)
- *Strategy and Objective-Setting* (Cyber risk management should integrated)
- *Performance* (identifies and assesses cyber risks that may affect the achievement of that strategy and business objectives)
- *Review and Revision* (reviewing cyber risk management capabilities and practices, and the entity's performance relative to its targets)
- *Information, Communication, and Reporting*

Lecture
10

IT Application Systems Risks



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

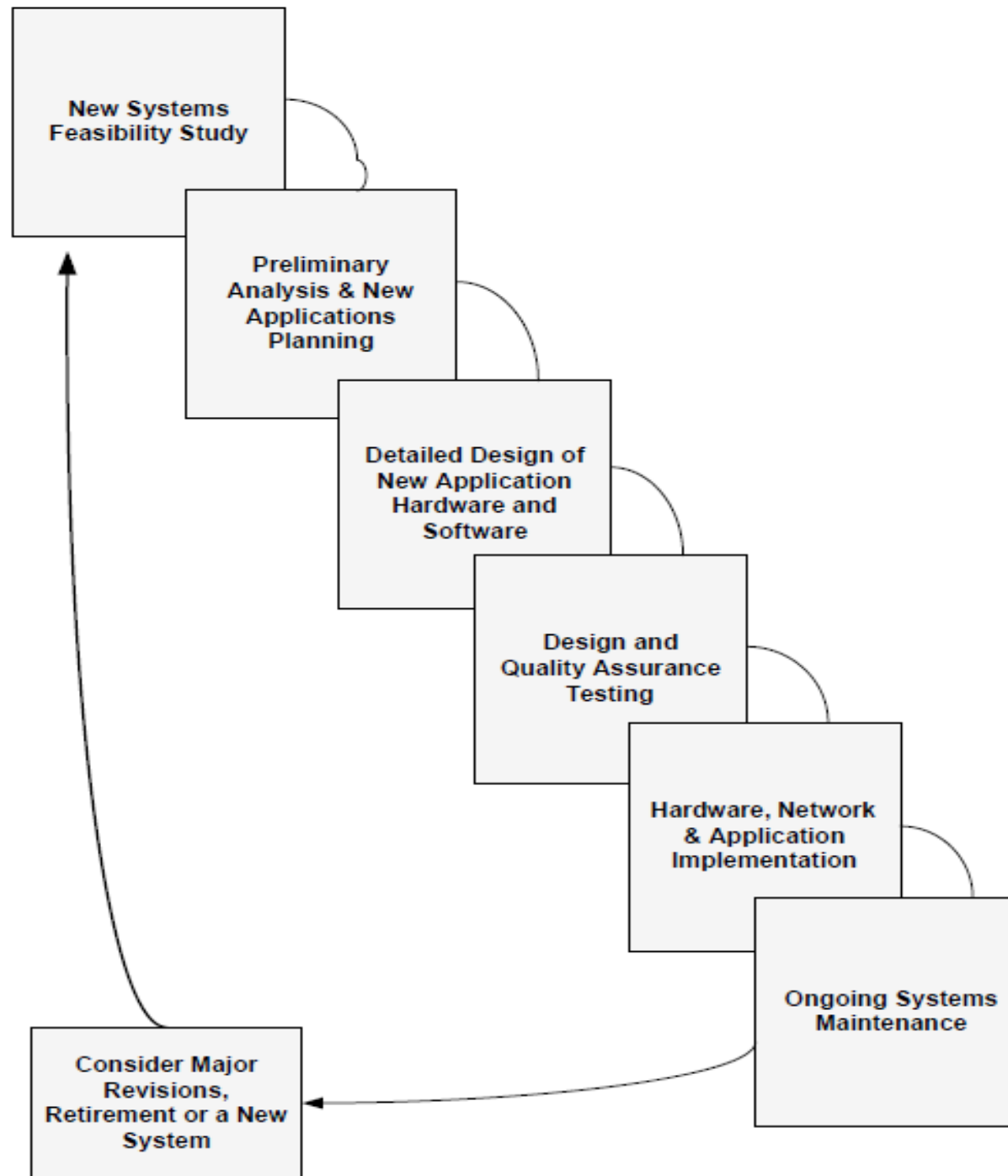
- IT applications are pervasive and can contain many risks.
- They may represent software routines that have been custom developed by an enterprise, purchased software products, or software that is embedded in many other tools and products.
- Some of the areas where an enterprise faces risks with its application systems include situations when a project is poorly planned and misses schedule or budget targets.
- Other risk areas are when there are integrity and performance problems, or when there are just “bugs” in the application.

- Failures here can cause problems or even embarrassments for an enterprise.
- A new application may be launched where only a limited set of conditions may have been tested.
- Increased variation of transactions or volume of transactions.
- Whether it is a space launch rocket or a customer billing application, the causes for many if not most IT applications failures can be traced to poor design and testing processes.
- ***Adequate procedures and other good processes in place can limit those risks.***

- Enterprise management would decide they needed some type of specific application and would proceed to use their own in-house programming resources to build it.
- While some standard applications such as payroll and fixed asset applications have been offered by outside vendors and installed as purchased software for many years, many others have been built in-house by enterprise IT development resources.

- There are risks associated with any new application development effort along with a somewhat different set of risks, depending whether the application is based on essentially purchased software or built by in-house enterprise resources.
- Purchased applications typically take a large amount of tailoring work to install, and most in-house developed applications always use purchased software building blocks.
- With the possible exception of some desktop system applications, most require some degree of application development work.

Lecture 10



System
Development
Life Cycle
Waterfall
Development
Processes

- All-function applications called *Enterprise Resource Planning (ERP)* applications.
- The concept behind these applications is that a change to one module, such as an inventory adjustment, will be reflected in related applications such as the general ledger and the bill of material.
- These kinds of purchased ERP applications are not easy to install.
- They typically *require massive changes* to existing processes to better match business operations to the ERP software application as well as some parameter-driven changes to the ERP to make it a better business fit.

- An ERP system typically requires a long time period for its implementation with a need for specialized staff training and outside consultants.
- Failure to select the appropriate software vendors can present major risks to any contracted software product.

Lecture 10

Purchased Software Contract Guidelines to Reduce Risks

- Software Product Feasibility/Compatibility
- Product History
- Vendor Background
- Customer & Trade References
- Revision Practices
- Product Documentation & Training
- Product Customer Support

- Enterprises often decided they had to develop applications because of what they argued were their unique needs.
- There is not a strict dividing line between applications purchased from software vendors and those developed in-house.
- The reality is that the software development process does not fit totally on one side of this divide or the other.
- ***Risks can be limited through good SDLC procedures supported by strong project management practices.***

- It is necessary to test all new applications before placing them into production.
- An enterprise can face a major risk to the quality and integrity of its IT applications if new applications are not fully tested.
- This testing process should take place at an application level and for overall systems.
- IT testing required strong procedures in place for developing testing plans and for reviewing the results of those testing activities, including specified pass/fail criteria over the results of this testing.

- The type of testing performed will vary depending on the features, objectives, and controls of the application being reviewed.
- This testing should be performed by the application developers, or IT audit.
- *In order to provide sufficient testing activities to minimize risks, the results of the testing should be well documented so that any outside reviewers could assess the adequacy of this testing activity.*

Lecture
10

Effective IT Continuity Planning



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

- Just as we rely on electrical power and clean water resources to be in operation, an enterprise today depends on its IT systems to operate continuously and effectively.
- Enterprise is largely responsible for the operation of its own IT resources.
- An enterprise faces numerous risks around its IT assets.

- There typically is not one major or central computer facility for handling major automated applications but a wide range of desktop devices, servers, and other computer systems connected through often very complex wireless communications, storage management networks, and links to the Internet.

- An enterprise can face a major risk if they lose the ability to access and use their key IT systems for even a relatively short period of time.
- To limit those risks, there is a need to have procedures in place to promptly restore their operations.
- Systems today support many enterprise operations, and the concept of having tools and procedures in place to rapidly restore overall business operations is called ***Continuity Planning***.

- In the event of an unexpected outage, the IT systems should be restored and operating as quickly and efficiently as possible in order to support and *restore the business processes*.
- Enterprise should also be concerned about the continued and high availability of its IT resources.
- Any form of computer systems downtime can be very costly to an enterprise.

- For example, the Disaster Recovery Institute⁵ estimated some years ago that the average hourly impact of an hour of systems downtime is \$89,500 for an airline reservations system or \$2.6 million for a credit card authorization provider, among others.
- Beyond just estimates, eBay's Internet auction site went down for 22 hours in August 1999.
- This caused \$4 million in lost fees and a \$5 billion drop in eBay's stock market value.

- To minimize risks, enterprises need to think through these various possible situations in advance.
- Two types of emergency incidents are significant.
- The first is the risk of a fire-in-the-building type of emergency incident.
- The supporting emergency response plan here would include posted fire exits and past experience with frequent fire drills.
- ***This type of emergency response plan should cover all enterprise operations, not just IT systems, and should be regularly tested.***

- The second level of emergency response plan covers specific individual incidents that ***may or may not turn out to be significant*** but must be corrected at once followed by an investigation and a plan of corrective action to prevent further incidents.
- These are called emergency incidents
 - Security Breaches or
 - Theft of hardware or software

- A good emergency incident response plan should be acted on quickly to minimize the effects of any further breaches.
- It should also be formulated to reduce any negative publicity and to focus attention on quick reaction time.
- *Rather than just an IT-related plan, all appropriate levels of enterprise operations should be covered.*

- An enterprise's risk management function should work with their IT operations to develop appropriate emergency response plans that will exist at a total facility level, such as a fire escape plan, and at an individual level, such as a plan to respond to a security breach. To reduce risks, these plans should be regularly updated and tested.

- Beyond an emergency response plan, an enterprise needs to develop a set of IT continuity plans.
- This type of plan is an outline of the steps necessary to help an enterprise recover from major service disruptions, whether a fire type of emergency, a computer or network equipment failure, or any other form of major disruption.
- The goal of such a plan is to help an enterprise reduce the risk of a disaster outage or extended service interruption to an acceptable level and to bring business operations back.

- This type of continuity plan represents a change in emphasis from what IT professionals once called disaster recovery plans.
- That older emphasis was to get data processing operations working while the continuity plan emphasizes needs of the business unit.
- Today, these plans have been redesigned to broaden them and to reduce risks.
- They are frequently called **Business Continuity Plans** (BCPs).

Lecture
10

Worms, Viruses, And System Network Risks



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

- An enterprise's IT operation today consists of much more than just its IT equipment and resources within offices and plants.
- It also includes a wide variety of other facilities connected through the Internet and other often-wireless networked resources.
- Even if an enterprise effectively prohibits the regular use of the Internet during regular working sessions, we are all effectively connected to these networks today.

- Communications with many banks, access to government reports, and even ordering certain parts and supplies requires Internet access.
- These interconnections contain many risks in terms of exposures to what have become known as worms, viruses, and other types of malignant software code threats that can cause peril for all types of programs and networked computer systems, ranging from a home office desktop to a large central system.

- An enterprise needs to recognize the threat of what is often called cybercrime and needs to take steps to protect from these threats.
- Establishing effective controls is a challenge.
- Enterprise can reduce its risks and the threat of cybercrime by:

- *Following “Best Practices” in Establishing and Maintaining an Effective IT Security System.*
- Regular systems of security maintenance should be established, including the regular updating of operating systems and software,
- Enforcement of password policies, disabling unnecessary services, installation and updating of antivirus software on a very frequent basis, and the use of intrusion detection systems and firewalls.
- *Prevention is always the best cure.*

- *Remaining on High Alert.*
- Frequent scanning of Internet logs and incoming and outgoing e-mail should be performed regularly, and any suspicious activity should be looked into and reported to the local authorities, if necessary.
- An emergency incident plan could be established as well, in case any system is temporarily or permanently disabled by a virus.

Lecture
10

Summary



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

- IT processes play a significant role in the operations of any enterprise and certainly are a major factor when assessing and understanding relative risks.
- This chapter has highlighted only three broad IT areas—the application development process, IT continuity plans, and malicious network programs—where an enterprise can face some significant IT risks.

Lecture 10

References

- COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance Processes. *Robert R. Moeller*.



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY