Co-funded by the Erasmus+ Programme of the European Union

InCyT Training Modules

Information Security for Employees Unit 1 Week 2 Unit name: Introduction into Information Security, internal control systems	
Learning Activities	❑ **Webinar** ❑ **Exercises** ❑ **Workshop** ❑ **Presentation** ❑ **Other**
Learning Responsible	• Gabriel Vladut • Valentin Istratie
Learning Activity Goals	1. Introduction about Erasmus+ InCyT project 2. Cyber-security 3. Concepts, definitions and terms 4. Internal Control Standard 5. Elaboration of cyber security controls
Skills to be Gained	• TS3 Network Security • TS4 Penetration (exploitable vulnerabilities) testing • SS3 Cognitive and behaviour analysis
Duration of Learning activity	2 weeks
Learning requirements	***What is needed?*** • Gain Cyber-security awareness and learn what is a Cyber-security attacks • Learn methods to prevent data breaches used by attackers to access sensitive data and exploit organizational vulnerabilities • Learn how to proceed in case of a Cyber-security attack

Co-funded by the
Erasmus+ Programme
of the European Union

Brief information about the module

Description
Information Security, internal control systems are important and verry often threat to cyber – security The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security. Also called INFOSEC. See also communications security; computer security; information security; information system. Internal controls are used by management, IT security, financial, accounting, and operational teams to achieve the following goals: 1. Ensure the reliability and accuracy of financial information – Internal controls ensure that accurate, up to date and complete information is reflected in accounting systems and financial reports. The learners could be informed about such aspects by reading the corresponding text, watching streaming webinars and solving exercises at own pace. All these documents are on the digital interactive project platform. The learners can test their answers on self-assessment exercises. The answers on other exercises should be saved on the corresponding discussion forum and discuss with the mentor at the common organised meeting once a week. Learner can work cooperatively with other ones and mentor particularly during the meetings. They will be supported to develop e-portfolio important for reflection and evaluation of the training.

Content of the Learning Material

Co-funded by the Erasmus+ Programme of the European Union

Cyber attacks and the competence framework

A competency framework is regularly used by companies to understand their skill-based requirements, required competencies, employee skills, and gaps.

When a competency framework is developed taking into account the company's profile and employee interests, it can improve performance and provide clarity for each individual role requirement and develop talent in the workplace. In recent years, due to many cyber attacks, cyber security frameworks are mainly adopted by large organizations (businesses, NGOs and other entities) or by state actors.

A successful cyber attack can cause major damage to a company's business. It can affect its bottom line as well as the company's business status and consumer confidence. The impact of a security breach can be divided into three categories: financial, reputational and legal.

Cyber attacks

Cyber-attacks often result in substantial financial loss resulting from the theft of corporate information, financial information (eg bank details or payment card details), money, transaction disruptions (eg inability to transact online), loss of business or of the contract. Businesses that have suffered a cyber breach will generally spend money associated with repairing affected systems, networks and devices.

Cyber attacks can damage a company's reputation and the trust customers have in the company. This could lead to lost customers, lost sales and reduced profits. The effect of reputational damage can even affect the company's suppliers or affect relationships with partners, investors and other third parties involved in the company's business.

So data protection and privacy laws require the security management of all personal data held by the company (of its own staff or customers). If this data is accidentally or deliberately compromised and the company does not implement adequate security measures, it may face regulatory penalties.

Risks in the company

It is important to manage your risks accordingly. After an attack occurs, an effective cyber security tool or incident response plan, i.e. using a cyber consultant, can help to:

- reduce the impact of the attack
- report the incident to the appropriate authority
- clean up the affected systems
- get your company business up and running in the shortest possible time.

It is necessary to invest in training and educating users in the field of cyber security in order to avoid attacks and continuously develop awareness for a cyber strategy in one's organization.

Cyber Security Framework

A cybersecurity framework is a set of best practices and documented processes that are used to develop IT security policies within an organization. But unlike traditional policy strictly related to the legal domain, a cybersecurity framework should also include documented examples of problems to be avoided by those policies and of the appropriate processes and ways to implement the security policies described in the framework.

It is both a guide for employees and users as well as a compelling compendium of security best practices that can be consulted by authorized external parties (such as authorities). A cybersecurity competency framework can also help better assess the competencies needed to avoid attacks, gaps, and remediation measures.

Cyber security

Despite increased awareness and bold efforts, the highly significant and growing shortage of cybersecurity professionals in the European Union and the knowledge and skills of employees to avoid cyber-attacks worldwide is known, and these shortages continue to present major problems for the public and private sector.

The 2019 CYBERSECURITY WORKFORCE 2019 Strategies for Building and Growing Strong Cyber Security Teams (ISC) study estimates that there are 2.8 million cybersecurity professionals globally, while the gap is actually 4.07 million.

The study notes that the current gap in Europe is 291,000, and this number has doubled from previous years. Many countries with highly developed expertise prefer to create their own set of regulations and documents, but many countries and small and medium-sized companies (SMEs) need help in this context.

Social engineering

- it means manipulating human beings, (often using psychological methods), to gain access to data, documents and information of interest to the attacker.
- is one of the main threats to information security today and is an effective form of cybercrime.
- could have dangerous repercussions, for example, data breaches, more than any other type of attack.
- the attacks have a financial purpose and thus organizations have lost considerable amounts of money.

- it is particularly dangerous because it relies more on human error than on vulnerabilities in software and operating systems.

The companies:

- they could suffer lost productivity, a drop in employee morale, and difficulties in recovery.
- they have reputational damage because customers are not convinced that the organization can protect itself.
- often need to trigger an old incident response.
- should provide security software to help prevent future attacks.
- they would often have to retrain employees to be ready for attacks.

Social engineering; Training (cyber awareness)

- of employees and managers for whom it is important to recognize social engineering attacks because the risk of becoming a victim is high.
- could be included in community, individual and citizen security awareness programs and protect individuals and their organization.
- is particularly lacking in SMEs that have fewer resources, so they should be helped to take cyber awareness training seriously and provide opportunities for employees to take it.

Training and mentoring

Entrepreneurs, including future ones, need complex ways of thinking and the ability to understand and integrate knowledge from different sectors, which requires interdisciplinary learning. Complex engineering problems require creating an interdisciplinary situation in an almost natural way.

In an interdisciplinary approach, learners should integrate information from different disciplines and fields. They develop an interdisciplinary understanding, learn to integrate areas of expertise and discipline-specific ways of thinking.

This increases cognitive skills and critical thinking more than through single disciplinary means.

Entrepreneurial skills and mentoring

Assessing learners' performance in developing entrepreneurial skills can take a holistic view, including a look at the learning environment and learning outcomes, and facilitate interactive, effective and active learning.

Mentoring is an experienced method to support more individual learning and to gain personal and career skills for new professions. There is research on the outcomes of mentoring in general, but there is little research on mentoring.

Mentoring offers a number of benefits for employees who train in companies. Interdisciplinary team mentoring has gained importance in recent years, reflecting the need for a change in the orientation of mentoring as various entrepreneurial developments and fields are increasingly multidisciplinary.

Interdisciplinary mentoring and networks of mentors can produce synergy in groups, generate innovative ideas and complex solutions to challenges, and create opportunities for collaboration and work.

Concepts, definitions and terms

The term "**cyberspace**" was coined in 1982 by William Gibson. The term entered everyday life in the 1990s with the advent of the World Wide Web

cyber infrastructures - information and communications technology infrastructures, consisting of IT systems, related applications, networks and electronic communications services;

cyber space - the virtual environment, generated by cyber infrastructures, including the informational content processed, stored or transmitted, as well as the actions carried out by users in it;

cyber security - the state of normality resulting from the application of a set of proactive and reactive measures that ensure the confidentiality, integrity, availability, authenticity and non-repudiation of information in electronic format, of public or private resources and services, in cyber space.

Proactive and reactive measures may include security policies, concepts, standards and guidelines, risk management, training and awareness activities, implementation of technical solutions to protect cyber infrastructures, identity management, consequence management;

cyber defense - actions carried out in cyber space for the purpose of protecting, monitoring, analyzing, detecting, countering aggressions and ensuring a timely response against threats to cyber infrastructure specific to national defense;

operations in computer networks - the complex process of planning, coordinating, synchronizing, harmonizing and carrying out actions in cyberspace for the protection, control and use of computer networks in order to obtain informational superiority, simultaneously with the neutralization of the adversary's capabilities;

cyber threat - circumstance or event that constitutes a potential danger to cyber security;

cyber attack - hostile action carried out in cyber space likely to affect cyber security;

cyber incident - event occurring in cyber space, the consequences of which affect cyber security;

cyber terrorism - premeditated activities carried out in cyberspace by politically, ideologically or religiously motivated individuals, groups or organizations that can cause material destruction or victims, likely to cause panic or terror;

cyber espionage - actions carried out in cyber space, with the aim of obtaining unauthorized confidential information in the interest of a state or non-state entity;

computer crime - all the acts provided for by the criminal law or other special laws that present a social danger and are committed with guilt, through or on cyber infrastructures;

vulnerability in cyber space - weakness in the design and implementation of cyber infrastructures or related security measures that can be exploited by a threat;

security risk in cyber space - the probability that a threat will materialize, exploiting a specific vulnerability specific to cyber infrastructures;

risk management - a complex, continuous and flexible process of identifying, evaluating and countering cyber security risks, based on the use of complex techniques and tools, to prevent losses of any kind;

identity management - methods of validating the identity of people when they access certain cyber infrastructures;

The components of internal control

According to the INTOSAI GOV 9100 Standard "Guidelines for Internal Control Standards". In 2001, at the Congress of the International Organization of Supreme Audit Institutions (INCOSAI), it was decided to update the INTOSAI Guidelines for internal control standards in the public sector, originally issued in 1992, by introducing into the document all aspects of recent developments in the field internal control and to integrate a series of elements of the COSO model (Internal Control – Integrated Framework).

By integrating it into the Guidelines - an activity carried out by the operative group of the Internal Control Standards Committee of INTOSAI - an attempt was made to obtain a unified understanding of how the new internal control system works, by the representatives of the Supreme Audit Institutions.

The "INTOSAI Guidelines for Internal Control Standards in the Public Sector" are part of the INTOSAI GOV category (good governance guidance) and are considered extremely useful both for public sector managers who have to implement the internal control system and external public auditors,

who must know this system and evaluate it.

Internal control standards

According to the INTOSAI GOV 9100 Guidelines), internal control consists of five interdependent components (identical to those of the COSO model):

- Control Environment
- Risk evaluation
- Control activities
- Information and communication
- Monitoring

Internal control is designed to provide reasonable assurance regarding the achievement of the institution's overall objectives. Objectives clearly established by the heads of the entity and the appropriate planning of the budget are a mandatory condition for an effective internal control.

Control environment

The control environment encompasses the general attitude, awareness and actions taken by management and those charged with governance regarding the internal control system and its importance within the entity. The control environment sets the tone of the organization, influencing the control consciousness at the staff level.

It represents the basis of all other components of internal control, ensuring a discipline within the organization that must be respected and a structure of the entity, so that the internal control system can be effectively applied. The internal control environment is an effective tool in preventing corruption and fraud.

The elements that define the control environment are:

- personal and professional integrity, the ethical values established by management for all staff, including a permanent supportive attitude towards internal control;
- a continuing management concern for staff competence;
- "the tone given from above" (the philosophy and activity style of management);
- the organizational structure of the entity;
- HR policy and practices.

Types of Cyber Security Controls

Cybersecurity controls are mechanisms used to prevent, detect and mitigate cyber threats and attacks. Mechanisms range from physical controls such as security guards and surveillance cameras to technical controls including firewalls and multi-factor authentication.

A one-sided approach to cyber security is simply outdated and ineffective. And because it is impossible to prevent all attacks in today's threat landscape, organizations should evaluate their assets based on their importance to the business and establish controls accordingly.

Adding to the challenge is that employees are unlikely to follow compliance rules if stringent controls are implemented across all company assets. The severity of a control should directly reflect the asset and threat landscape.

The consequences of a hacker exposing thousands of personal customer data through a cloud database, for example, can be far greater than if an employee's laptop is compromised.

Cyber security controls

"There are many different ways to apply controls based on the nature of what you're trying to protect," said Joseph MacMillan, author of Infosec Strategies and Best Practices and cybersecurity global black belt at Microsoft.

"What is the nature of the threat you are trying to protect against?

Is it a malicious actor?

Or is it a devastating attack?"

Securing information assets

It refers to the implementation of appropriate information security controls for assets. We want to ensure that we focus on strong and effective ideologies to understand to select the appropriate controls, which means that the asset is considered "safe enough" based on its criticality and classification. There are different classes that divide the types of controls:

- Administrative/managerial controls are the firm's policies and procedures. They're not as "cool" as a new software control, but they exist to provide structure and guidance to individuals and other members of the organization, ensuring that no one gets fined or causes a breach.
- Physical controls that limit access to systems in a physical way.
- Technical / logical controls are those that limit access based on hardware or software, such as encryption, fingerprint readers, authentication or trusted platform modules (TPM).

They do not limit access to physical systems as physical controls do, but rather access to data or content. Operational controls are those that involve people carrying out processes on a day-to-day basis. Examples might include awareness training, asset classification, and log file review.

Types of controls

Preventive controls exist to prevent an action and include firewalls, fences, and access permissions.

Detective commands are only triggered during or after an event, such as video surveillance or intrusion detection systems. Deterrents discourage threats from trying to exploit a vulnerability, such as a "Watchdog" or dogs sign. Corrective controls are capable of taking action from one state to another. The fail open and fail closed commands are addressed here.

Recovery commands get something back from a loss, such as recovering a hard drive. Compensating controls are those that attempt to compensate for deficiencies in other controls, such as regularly reviewing access logs. This example is also a detective control, but compensation controls can be of different types.

Order of controls

It discourages actors from trying to access something they shouldn't be. Deny/Prevent Access through a preventive control such as access permissions or authentication.

Detect risk by making sure to record detection, such as with endpoint protection software. Delay the process from repeating the risk again, such as with a "too many attempts" feature for entering a password.

Correct the situation by responding to the compromise, such as with an incident response plan. Recover from a compromised state, such as a backup generator that restores availability to a server.

In addition, in the field of continuous improvement, we should monitor the value of each asset for any changes. The reason is that we may need to rethink our controls for protecting those assets if they become more or less valuable over time or during certain major events in your organization.

Controls and recovery

When we look at controls we should also think about recovery, we want to be able to recover from any adverse situations or changes in assets and their value. Just as examples, we are talking about backups, redundancy, restoration processes and the like.

A concept to remember, especially in the era of cloud, SaaS, PaaS, IaaS, third-party solutions and all other forms of "someone else's computer" is to ensure that Service Level Agreements (SLAs) are clearly defined and have maximum allowable downtime agreements, as well as penalties for non-compliance with these agreements. This is an example of compensatory control.

Questions:

Questions Discussion Forum to be answered with a short explanation. Answers will be discussed with the mentor during the mentoring sessions

1. Witch are the risks in the company for cyber attacks?
2. Call some types of cyber security controls
3. Witch are internal control standards
4. How to Control and recover informations

Self-assessment questions. After answering the learner can see the results and compare them with these saved on the platform

- Risks in the company for cyber attacks
- Internal control standards and rouls
- Control environment

Attachments

PowerPoint presentation
Video movies

References:

- Cyber Attacks on Companies: Are You at Risk?
- The rising strategic risks of cyberattacks
- 10 Common Cyber Security Risks For Businesses
- Internal Controls and Data Security: How to Develop Controls That Meet Your IT Security Needs
- Internal Controls Over Information Systems