SORSOGON STATE UNIVERSITY
BULAN CAMPUS
COLLEGE OF INFORMATION AND COMMUNICATION TECHNOLOGY
Bachelor of Science in Information Technology

BAGONG PILIPINAS

ICT

Module 1

- *INTRODUCTION TO INFORMATION ASSURANCE AND SECURITY 2*

BSIT 4

Learner's Reference Number (LRN)

Name of Student Strand/Year Address

Contact No.

RICHARD G. RABULAN, MIT
INSTRUCTOR II

RICHARD RABULAN | 0977-357-1407 | richard.rabulan@sorsu.edu.ph

HOW TO USE THIS MODULE

Before starting the module, I want you to set aside other tasks that will disturb you while enjoying the lessons. Read the simple instructions below to successfully enjoy the objectives of this kit. Have fun!

1. Follow carefully all the contents and instructions indicated in every page of this module.
2. Write on your notebook the concepts about the lessons. Writing enhances learning that is important to develop and keep in mind.
3. Perform all the provided activities in the module.
4. Let your facilitator/guardian assess your answers using the answer key card.
5. Analyze conceptually the posttest and apply what you have learned.
6. Enjoy studying!

Lesson 1 – Introduction to Information Assurance and Security 2

Information assurance and security is a rapidly growing field, but what's it all about? How can you start working in information security? Do you have the right skills and education? Information security conferences are key to staying on top of this rapidly evolving industry. If you're looking to grow your career in a new direction and turn your love of computer science into a lucrative paycheck, you've come to the right place. Keep reading to learn more about this exciting field and whether it's a good fit for you.

"Information is data endowed with relevance and purpose. Converting data into information thus requires knowledge. Knowledge by definition is specialized." (Blyth and Kovacich, 2023)

How does information differ from data? And what characteristics should information possess to be useful?

It should be: accurate, timely, complete, verifiable, consistent, available.

According to Raggad, the following are all distinct conceptual resources:

Noise: raw facts with an unknown coding system

Data: raw facts with a known coding system

Information: Collected and processed data that have a structure and organized

Knowledge: accepted facts, principles, or rules of thumb that are useful for specific domains. Knowledge can be the result of inferences and implications produced from simple information facts.

What about "assurance"? What does that mean? Assurance from what or to do what? Is it context-dependent?

According to the U.S. Department of Defense, IA involves:

"Actions taken that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities."

Information Assurance (IA) is the study of how to protect your information assets from destruction, degradation, manipulation and exploitation. But also, how to recover should any of those happen. Notice that it is both proactive and reactive.

In this chapter, we introduce the essential concepts behind Information Assurance and Security. We start with a description of typical IAS that are found in contemporary organizations and the Difference of Information Assurance and Information Security. Next, we discuss the Proactive and Reactive Cybersecurity Approach. In order to place IAS in a broader perspective, we then provide an overview of the SSDLC discipline.

INFORMATION ASSURANCE AND SECURITY

Information assurance and cybersecurity is the management and protection of knowledge, information and data. It combines two fields: Information assurance, which focuses on ensuring the availability, integrity, authentication, confidentiality and nonrepudiation of information and systems.In our lessons, we will be using a concrete example of a procure-to-pay process for renting construction equipment, as described below.

Information assurance includes protection of the integrity, availability, authenticity, non-repudiation and confidentiality of user data. Undetected loopholes in the network can lead to unauthorized access, editing, copying or deleting of valuable information. This is where information assurance plays a key role on which the following measurements are needed in this area, You might want:

- **Privacy of your data**
- **Protection against phishing**
- **Integrity of your data**
- **Authentication**
- **Authorization**
- **Confidentiality**
- **Non-repudiation**
- **Availability**

According to the DoD definition, these are some aspects of information needing protection:

- **Availability**: timely, reliable access to data and information, services for authorized users;

- **Integrity**: protection against unauthorized modification or destruction of information;

- **Confidentiality**: assurance that information is not disclosed to unauthorized persons;

- **Authentication**: security measures to establish the validity of a transmission, message, or originator.

- **Non-repudiation**: assurance that the sender is provided with proof of a data delivery and recipient is provided with proof of the sender’s identity, so that neither can later deny having processed the data

The quality of a system is the degree to which the system satisfies the stated and implied needs of its various stakeholders, and thus provides value. Those stakeholders' needs (functionality, performance, security, maintainability, etc.) are precisely what is represented in the quality model, which categorizes the product quality into characteristics and sub-characteristics.

According to ISO/IEC Standard 9126-1 (Software Engineering Product Quality), the following are all aspects of system quality:

- functionality
- reliability
- usability
- efficiency
- maintainability
- portability

Which of these do you think apply to IA?

All aspects are applicable to Information Assurance on which each aspects plays a vital role on the quality of the software system. All aspects should met the quality standard in order for the developer to gain the trust of the client.

Businesses that store and exchange critical data over information networks need to be mindful of how vulnerable each individual machine can be. Whether you're supporting existing systems or designing and implementing new ones, your organization should aim to reduce the exposure to and impact of cyber risk by working within the frameworks of compliance, industry regulations, risk management and organizational policies, aka information assurance.

As network security issues become more prevalent, information assurance (IA) has grown to be a nuanced and essential part of information security. However, implementing sound information assurance management is difficult.

Adding to the challenge is a variety of confusing terms and misnomers. Even seasoned IT pros can get confused between information assurance, cyber assurance, cybersecurity and information security. Often, these terms are used interchangeably, leading to IA bad practices.

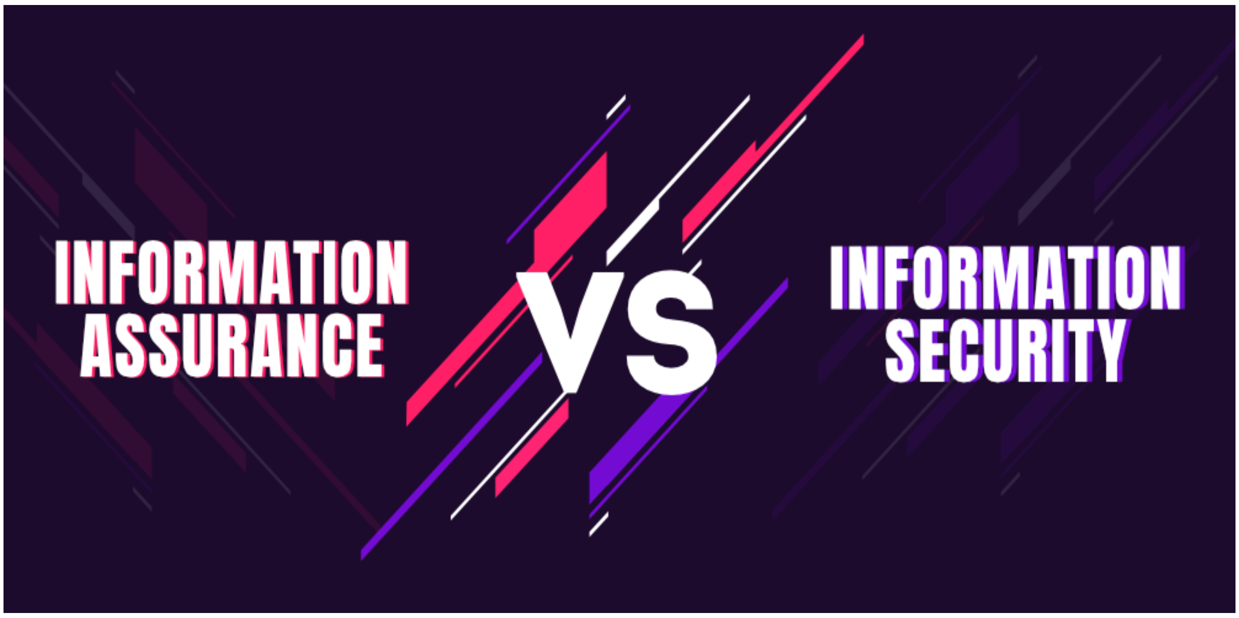
Let's simplify IA in order for you to evaluate your framework with ease.

Information assurance vs. information security

What Is the Difference Between Information Assurance and Information Security?

The NIST defines information security as the process of protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability.

In short, information assurance focuses on gathering data. Information security is about keeping that data safe. In most organizations, these two jobs are combined into one department or even one worker. You'll need to understand cyber security, database management and security engineering to succeed in this field. A relevant master's or bachelor's degree is highly recommended to ensure you learn the broad range of skills necessary to work as a cyber security officer. Don't be confused: Although you'll be responsible for storing customer data, algorithm outputs or protected health information, you won't actually be in charge of gathering the data yourself. You'll be more like the owner of a long-term storage facility, and your company's users will be the tenants who actually bring you items -- meaning data -- for safeguarding.



The differences between information assurance and information security are more than just semantics. Let's break it down:

Focus

Information assurance focuses on quality, reliability and restoration of information. Information security focuses on deploying security solutions, encryption, policies and procedures to secure information.

Approach

IA is not concerned with the specific technology or tools used to protect information. Rather, it is centered around developing policies and standards. Information security directly deals with tools and technologies used to protect information. It's a hands-on approach that safeguards data from cyberthreats.

Scope

IA stresses organizational risk management and overall information quality. As a result, IA has a broad scope. Information security stresses risk control and agreement. As a result, information security has a detailed scope.

GOAL OF INFORMATION ASSURANCE

The purpose of IA is to reduce information risks by ensuring the information on which the business makes decisions is reliable. This purpose is achieved by following:

Risk management: Businesses face legal fines and penalties if the information in the network is compromised. IA enables risk assessment to identify vulnerabilities and the potential impact on the business in terms of compliance, cost and operational continuity. The goal is to mitigate potential threats.

Encryption at rest and in transit: IA mandates end-to-end encryption to protect privacy by ensuring no human or computer can read data at rest and in transit except the intended parties. The goal is to help businesses stay compliant with regulatory requirements and standards.

Data integrity: Bad business decisions usually stem from bad data. IA focuses on auditing data collection and tracking process, improving transparency in the organizational process. The goal is to manage data in a way that a future audit can retrace the process, leading to better decision-making.

Why do we need information assurance?

Your organization needs assurance services to ensure compliance with laws and regulations, identify weaknesses in internal controls, enhance credibility with stakeholders, provide assurance on financial statements' accuracy, and facilitate informed decision-making on financial performance and risk management.

IA aims to maintain integrity through anti-virus software on all computer systems and ensuring all staff with access know how to appropriately use their systems to minimize malware, or viruses entering information systems.

While, Information security protects sensitive information from unauthorized activities, including inspection, modification, recording, and any disruption or destruction. The goal is to ensure the safety and privacy of critical data such as customer account details, financial data or intellectual property.

Adopting good IA best practices provides several benefits:

- Operational benefits:
- Resilient business processes
- Improved customer service
- Better information usage
- Improved responsiveness

Tactical benefits:

- Easy compliance
- Better understanding of business opportunities
- Commitment from business partners and customers
- Strategic benefits:
- Better governance
- Cheaper equity
- More sales
- Lower costs

Organizational benefits:

- Improved shareholder value
- Gain competitive advantage
- License to operate

How does information assurance work?

Information assurance is a strategic endeavor that extends beyond simply IT. The reality is that the legal and reputational ramifications that ensue from a data breach affect the entire organization. A proper security framework helps protect your organization and customers. IA is a work in progress that includes:

Strategy: Develop Governance, Risk and Compliance (GRC) readiness by evaluating maturity as compared to your peers. Utilize key use cases to identify gaps and build roadmaps. Rationalize and prioritize GRC initiatives by aligning the essential requirements of your information and infrastructure with the organization's objectives.

Design: Design GRC programs and models to align with organizational policies. Exposures and risks should be quantified and classified to evaluate defined metrics. Once established, use these findings to define mitigation steps to manage risk and optimize speed, accuracy and efficiency of resolution.

Implementation: Implement processes, policies, controls and technology that monitor operations against key metrics. Measure potential exposures in personnel, processes and technology controls in the context of IT infrastructure interdependencies.

Operations: Mitigate exposures through continuous enforcement of policies. Detect violations and measure outcomes in comparison to your desired state. Use these learnings to continuously improve processes to maximize synergies and optimize outcomes.

Who is responsible for information assurance?

Conventionally, IA is seen as an incoherent function that is solely exclusive to the IT department. The reality is that the legal and reputational ramifications that ensue from a data breach affect the entire organization. It is essential to create a security-centric culture from top to bottom, with a focus on complying with information security regulations.

Information security, or infosec, is not just a concern for IT departments or cybersecurity professionals – it's a collective responsibility that permeates every level of an organisation. From top management to frontline employees, everyone has a role to play in protecting sensitive data and mitigating risks.

Anyone in an organization has a responsibility to uphold data protection compliance. This should be outlined in an organization's Data Protection Policy, and in short, all persons who handle personal data in some way have some level of responsibility for making sure that this data is handled safely and correctly.

Everyone is responsible for Information Security. It can't be done in isolation, or have one person named as responsible. We're in this together and if each one of us was a little more aware of the positive impact our behavior can have on the security of our organizations, then people might just start taking notice.

What are the five pillars of information assurance?

The CIA triad is considered the first model of information assurance introduced to define effective practices of assuring information security and integrity. Here are the following five pillars of IA that make information networks safe against all threats:

- Integrity (protection of information systems and assets)
- Availability (dependable access to information systems by authorized users)
- Authentication (the process of restricting access and confirming the identity of users)
- Confidentiality (restriction of access to authorized users only)
- Non-repudiation (forensic tracking to create a reliable "paper trail" of all actions)

INTEGRITY

Information sent should always remain in its original state. Integrity means tampering or modification by bad actors should not occur. Therefore, the primary goal of this pillar is to set up safeguards to deter threats.

AVAILABILITY

Easy data access helps users seamlessly access important information to perform critical tasks. Availability means those who need access to information can do so. Therefore, the primary goal of this pillar is to ensure systems always remain fully functional.

AUTHENTICITY

Verify the identity of a user (device) before allowing them to access data with methods like two-factor authentication, password management, biometrics and other devices. Authenticity means ensuring that those who have access to information are who they say they are. The primary goal of this pillar is to prevent identity theft.

CONFIDENTIALITY

Protect private information from getting exposed by any unauthorized users, systems or networks. Confidentiality means data should be accessed only by those who have proper authorization. Therefore, the primary goal of this pillar is to avoid IP theft or the compromise of Personal Identifiable Information (PII) of customers.

NON-REPUDIATION

It is important that the information system is able to provide proof of delivery to confirm that the data was properly transmitted. Non-repudiation means someone with access to your organization's information system cannot deny having completed an action within the system, as there should be methods in place to prove that they did make said action. The primary goal of this pillar is to guarantee that the digital signature is that of the intended party, thereby granting authorization to the protected information.

CEOS ARE ALSO TRYING TO SECURE NETWORKS

Businesses have to look at the risks and benefits before diving in. The Gartner 2023 Board of Directors Survey revealed that boards are now more open to taking risks. This only increases the need for better cybersecurity measures on executive levels.

A Gartner study found that 60% of boards have achieved their digital business optimization goals. Businesses are willing to pay for new technologies to stay ahead. However, a surprising number of them do not have the right cybersecurity measures in place to protect these investments.

The security and reputation of a company are worth the expense of improved cybersecurity. The global cybersecurity market size is already forecast to grow to US$ 266.2 billion by 2027.

The main goal of **cybersecurity** is to protect a network from cyber-attacks, data breaches, or any cyber threat. The cybersecurity measures used can often be neatly divided into proactive and reactive strategies.

A Proactive Cybersecurity Approach

A **proactive approach** uses active measures to prevent attacks before they take place. This type of security focuses on identifying potential weaknesses in a network well before they can be exploited.

Examples of proactive cybersecurity measures include the use of firewalls and threat detection. It also involves regular vulnerability assessments and employee training on proper cyber hygiene.

A Reactive Cybersecurity Approach

Reactive cybersecurity involves the actions after a cyber-attack has taken place. These are usually just quick-fix solutions for damage assessments and recovery. They do not always focus on data or money loss.

Examples of reactive cybersecurity include disaster recovery solutions, vulnerability patching, and updates to security software.

Proactive vs. Reactive Security Measures

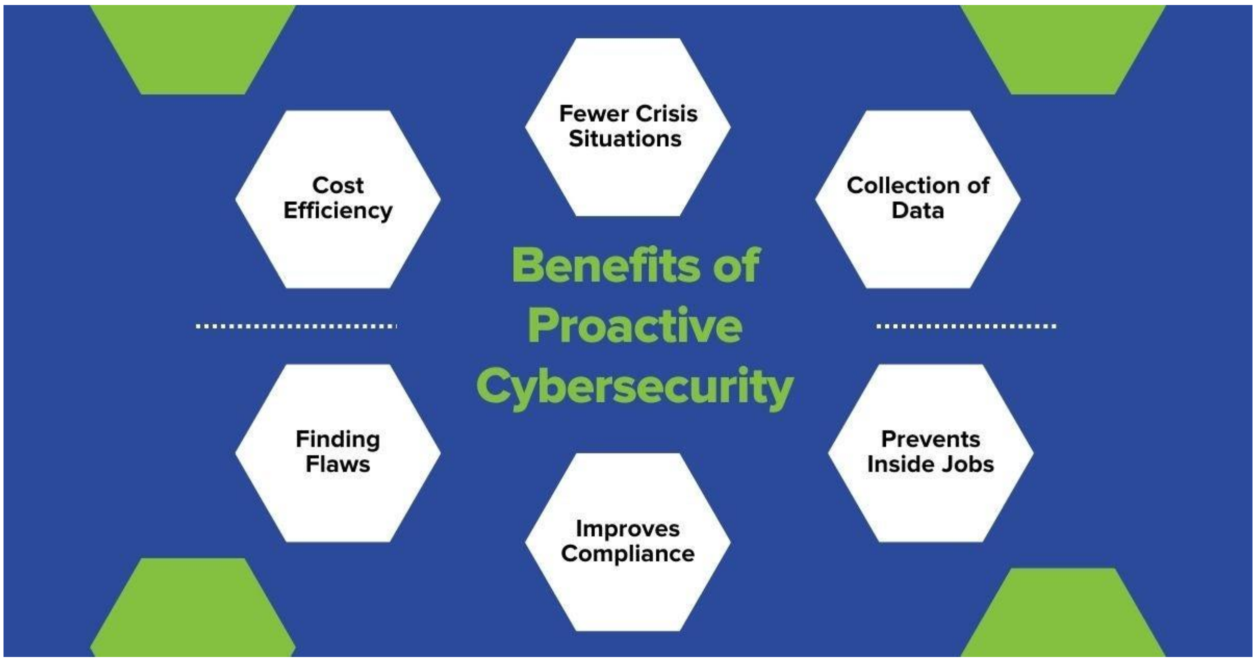
The question then begs, which approach is the better solution?

Proactive cybersecurity helps to identify, isolate, and eliminate any threats. This happens before an attack can take place while still looking for weak spots.

Reactive approaches, however, focus on fixing immediate incidents and preventing repeat attacks from happening. This is done through log monitoring, patching, and SIEM solutions. However, prevention will always be better than cure.

Proactive cybersecurity outweighs the reactive approach by covering more ground. A proactive approach prevents cyber threats before they can cause damage.

WHY YOU SHOULD CHOOSE PROACTIVE CYBERSECURITY



Proactive cybersecurity is better than relying on the damage control of a reactive solution. Companies have resources and data that need to be protected as best as possible.
Proactive approaches create a basic level of security for your company to build on. We've created a list of some of the benefits of a proactive approach to cybersecurity:

- **Cost Efficiency**: Proactive solutions usually involve more steps, which might mean more money spent. However, these measures ensure a better return on investment than a reactive solution. The costs of a cyber-attack can cause damage to any organization. Brand damage alone can have lasting effects on business growth. Proactively defending your company ensures that your network - and bottom line - are always safe.
- **Fewer Crisis Situations**: Cyber-attacks are happening more each day - forcing companies to lose lots of money and data. Proactive security ensures that your IT team is always one step ahead.
- **Evolved Thinking**: Proactive cybersecurity relies on the ability to identify and quickly get rid of new cyber threats. This means that these solutions are always improving to adapt to new threats.
- **Prevents Inside Jobs**: A proactive approach gives you a simple and open view of your entire network. This helps you quickly find any odd behavior or files that could be harmful.
- **Improves Compliance**: Regulations ask for a high level of cybersecurity. Many countries have issued hefty fines to companies for data breaches. Proactive solutions use a risk analysis and offer layered protection to avoid any data breaches.
- **Finding Flaws**: A proactive approach scans your entire network to show you areas that need to be improved. All cybersecurity solutions need the right tools and specialists. Sangfor Technologies uses innovative platforms and services to help you create the best proactive cybersecurity for your company.