LECTURE SLIDES FOR CSS 410

COURSE TITLE: INFORMATION SYSTEMS SECURITY MANAGEMENT

Lecturer: Dr. Olusegun D. Ilesanmi

Department of Criminology and Security Studies

COURSE OUTLINE

- Introduction to Information System Security Management
- Overview of Information Security Management.
- Importance of Information Security in the 21st Century.
- Basic Concepts of Computer Security.
- Information gathering
- Methods for Information Gathering in Security Management.
- Identifying and Assessing Information Security Risks.
- Risk Assessment Tools and Techniques
- Introduction to system analysis and design
- Information system security:
- Ethics of information communication technology (ICT)
- Identity and information security integration
- Integrating information assurance into system administration
- Management information systems useability and associated risk
- The information systems and the economics of innocent fraud management

- An overview of information security as a risk management function
- Risk assessment
- Risk mitigation options
- Mitigating economic risk through security technology
- Information age militaries
- Information technology impacts on war fighters
- Information technology and nature of future war
- Difficulties in information security
- The economics of information security investment

Introduction

- In today's interconnected world, safeguarding sensitive data and protecting digital assets has become paramount for organizations across all sectors. This course will serve as your comprehensive guide to understanding the fundamental principles, strategies, and best practices essential for effective information systems security management. Through a blend of theoretical concepts and practical applications, you will gain insights into threat detection, risk assessment, access control, encryption techniques, and incident response protocols.
- By the end of this course, you will be equipped with the knowledge and skills necessary to navigate the evolving landscape of cybersecurity and contribute to the resilience of organizational IT infrastructures.

Information Gathering

- The primary objective of information gathering is to ascertain the information needs of an organization. Frequently, management does not express these needs with precision. Hence, it falls upon the analyst to compile a detailed Systems Requirements Specifications (SRS) document that is readily comprehensible to users. This SRS document plays a crucial role as it serves as a foundational document prior to commencing a project.
- An analyst should constantly have a strategy in place for gathering information. This strategy entails identifying information sources, devising a methodology for extracting information from these identified sources, and employing an organizational information flow model.

INFORMATION SOURCES

- The main sources of information are users of the system, forms and documents used in the organization, procedure manuals, rule books etc, reports used by the organization and existing computer programs

INFORMATION GATHERING METHODS

- Collecting data entails interviewing individuals across different management tiers, spanning from top-level executives to middle management and operational personnel.
- Besides interviews, group discussions also prove invaluable for analysts in acquiring information. Given the breadth of information required, conducting multiple interviews is often imperative rather than solely depending on a single session.

Methods if Information gathering

- Interview
- Questionnaire
- Studying systems utilized by similar organizations.
- Observing workflow processes in the workplace.
- Exploring repositories of systems developed for comparable organizations.

Information Gathering Techniques

a. Open Source Intelligence (OSINT): Leveraging publicly accessible information from platforms such as the internet, social media, public records, and newspapers.

b. Human Intelligence (HUMINT): Acquiring data through interpersonal communication, interviews, and engagements with individuals.

c. Signals Intelligence (SIGINT): Gathering data from electronic signals, encompassing telecommunications, radio transmissions, and digital communications.

d. Geospatial Intelligence (GEOINT): Examining data derived from satellite imagery, maps, and geographic information systems to procure intelligence.

e. Cyber Intelligence (CYBINT): Extracting information from digital origins, involving activities like malware analysis, network traffic analysis, and monitoring the dark web.

INTERVIEW TECHNIQUE

- Effective interviews hinge on clear protocols: Arrange the interview beforehand and meet the interviewee promptly as agreed.
- Familiarize yourself with pertinent background information and come equipped with a checklist.
- Communicate the interview's purpose clearly and maintain punctuality while attentively listening to the interviewee's answers.
- Steer clear of technical jargon and aim to collect both quantitative and qualitative data. Avoid extending the interview unnecessarily and summarize the gathered data for validation.

Tools for Information Collection

a. Search Engines: Platforms like Google, Bing, and specialized search engines such as Shodan for IoT devices.

b. Social Media Monitoring Tools: Solutions like Hootsuite, Buffer, and Mention for monitoring mentions and discussions across various social media platforms.

c. Data Analysis Tools: Tools like Excel, Python, and R for processing and analyzing extensive datasets.

d. Network Monitoring Tools: Software such as Wireshark, Nmap, and Snort for capturing and analyzing network traffic.

e. Open Source Intelligence Tools: Applications like Maltego, the Harvester, and Spider Foot for gathering information from open sources.

Information Assessment

a. **Credibility Assessment:** Evaluating the reliability and trustworthiness of sources based on factors like expertise, bias, and reputation.

b. **Corroboration:** Cross-referencing information from multiple sources to verify its accuracy and consistency.

c. **Contextual Analysis:** Understanding the broader context surrounding the information to interpret its significance accurately.

d. **Risk Assessment:** Assessing the potential impact and likelihood of different outcomes based on the gathered information.

e. Decision Support: Providing actionable insights and recommendations based on the assessed information to support decision-making processes.

Information Security In The 21st Century: Computer Security

- Information security involves numerous aspects of trust concerning information. Another commonly used term is information assurance, which goes beyond computer systems and covers information regardless of its electronic or machine-readable format.
- This practice pertains to all facets of safeguarding or protecting data in any form. An information security chain becomes crucial when information encounters threats, losses, or misuse.

Information Security

- Information security encompasses various dimensions of trust related to information. Another frequently used term is information assurance. Information security extends beyond computer systems and includes information in any form, regardless of whether it is electronic or machine-readable.
- It pertains to safeguarding or protecting information or data in all its manifestations. An information security chain is essential when information faces threats, losses, or misuse.

What is information security?

- Information security aims to safeguard the interests of those who depend on information, as well as the information systems and communication channels through which information is delivered, from potential harm arising from failures in availability, confidentiality, and integrity.
- Information security is a protection of the interests of those who rely on information, the information systems and communications that deliver the information from harm resulting from failures of availability, confidentiality, and integrity.

Reason for information security policy in organization

- Its information systems undergo thorough security assessments.
- The principles of confidentiality, integrity, and availability (CIA) are upheld, forming the cornerstone of nearly every security program, whether explicitly stated or implicitly practiced. These principles are often represented as a triangular framework, with each aspect directly impacting the other two. Confidentiality limits information access to authorized individuals, integrity ensures the accuracy and completeness of information, and availability ensures that authorized users can access information as required.
- Staff members are briefed on their responsibilities, roles, and accountability regarding information security.
- Established protocols for detecting and resolving security breaches.
- Consistent addressing of information security concerns across the organization.

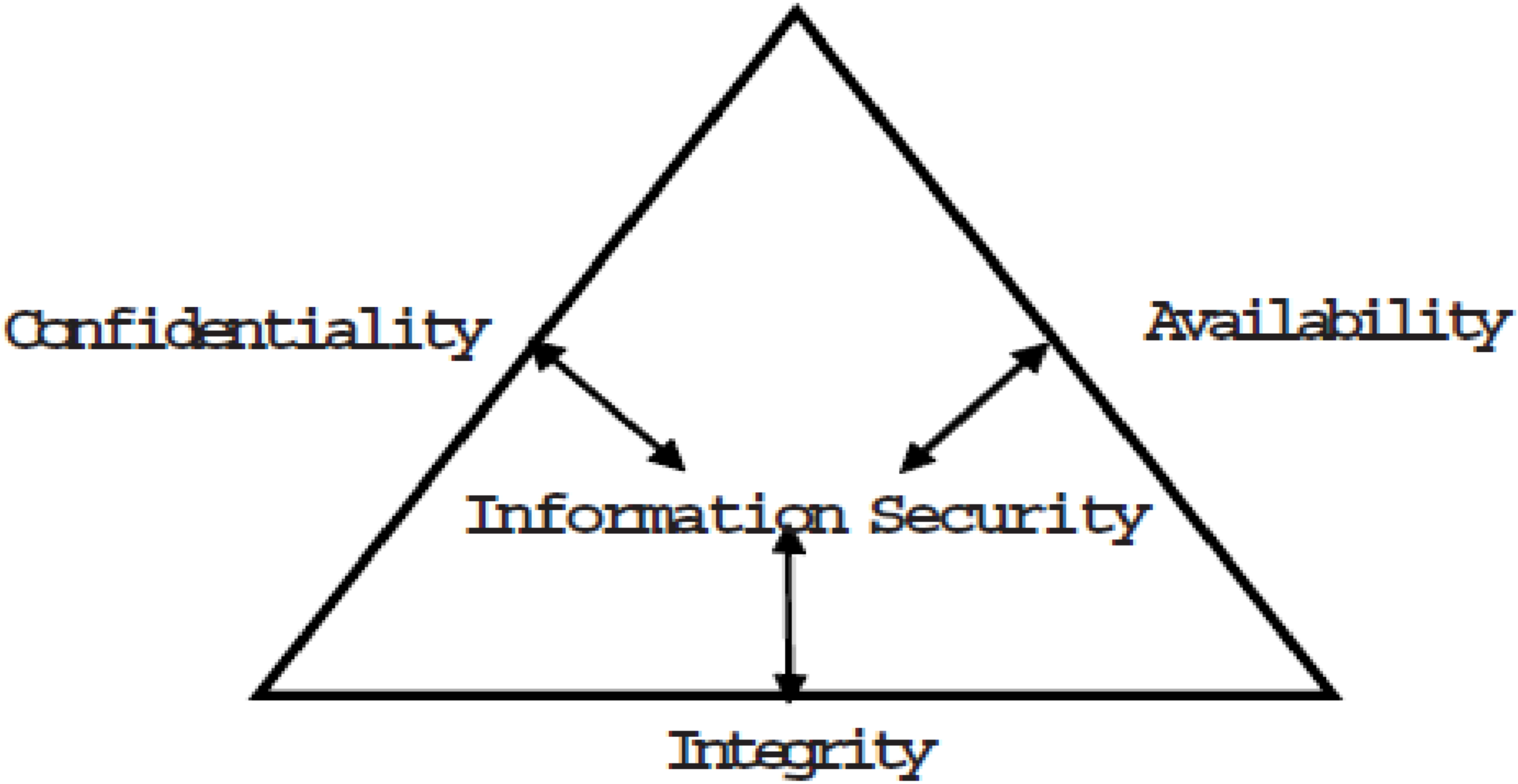


Figure 1: The CIA Relationship

Importance of Information Security

- Every organization, based on its resources and the type of data it manages, sets aside specific budgets and manpower for crafting information security protocols. Dr. Thomas V. Finne delineates twelve modules and eighty sub-modules within the information security framework, which include:

1. Computer Security
2. Operation Security
3. Protection against Burglary
4. Protection against Fire
5. Protection against Water Damage
6. Electricity Distribution
7. External and Internal Threats
8. Communication
9. Contingency Planning
10. Personnel Security
11. Attitudes toward Information Security (ISEC) Issues
12. Various Security Considerations

Understanding Information Security Risks

- Information security risks refer to potential vulnerabilities or threats that may compromise the confidentiality, integrity, or availability of information assets.
- **Types of Risks:** Risks can arise from various sources, including external threats (e.g., hackers, malware), internal threats (e.g., employee negligence, system failures), and environmental factors (e.g., natural disasters, power outages).

Risk Identification Techniques

a. **Asset Inventory:** Creating an inventory of all information assets, including hardware, software, data repositories, and network infrastructure.

b. **Threat Modeling:** Analyzing potential threats and vulnerabilities to identify potential attack vectors and weak points in the system.

c. **Vulnerability Assessments:** Conducting regular scans and assessments to identify known vulnerabilities in systems and applications.

d. **Security Audits:** Performing comprehensive audits of security controls, policies, and procedures to identify gaps and compliance issues.

e. **Stakeholder Interviews:** Engaging with key stakeholders to gather insights into their concerns, priorities, and perceived risks.

Risk Assessment Tools and Techniques

Risk assessment is a vital component of effective risk management, enabling organizations to identify, analyze, and mitigate potential threats to their assets and operations.

Quantitative vs. Qualitative Risk Assessment:

- **Quantitative Risk Assessment:** Involves assigning numerical values to risk factors, such as probability and impact, and using mathematical models to calculate risk levels.
- **Qualitative Risk Assessment:** Relies on subjective judgment and expert opinion to assess risks based on qualitative criteria, such as likelihood and severity.

Risk Assessment Techniques

a. **Failure Mode and Effects Analysis (FMEA):** Identifies potential failure modes in a system, assesses their impact, and prioritizes them based on severity.

b. **Bowtie Analysis:** Visualizes potential threats, consequences, and control measures in a diagram format, helping to identify critical control points and potential barriers.

c. **SWOT Analysis (Strengths, Weaknesses, Opportunities, Threats):** Assesses internal strengths and weaknesses along with external opportunities and threats to identify potential risks and strategic factors.

d. **Scenario Analysis:** Examines various hypothetical scenarios to assess their likelihood and potential impact on the organization, helping to prepare for different risk scenarios.

e. **Root Cause Analysis (RCA):** Investigates the underlying causes of risks and incidents to address fundamental issues and prevent recurrence.

Computer Security

- Computer security entails adopting measures, procedures, and controls to protect information resources from inadvertent or deliberate exposure, alteration, or destruction. Computer security includes;

a. Backup

b. Computer Viruses

c. Passwords

d. Data Encryption

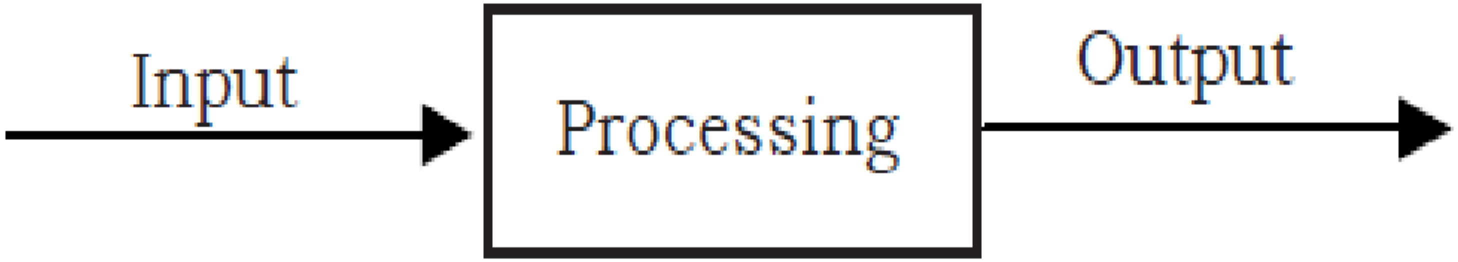
e. Biometric Methods

f. Computer Locks, among others.

System Analysis and Design

- System analysis and design play a crucial role in ensuring the security of information systems.

- A System is a collection of components that work together to realize some objectives forms a system. Basically there are three major components in every system, namely input, processing and output.



- **System Analysis:** The process of studying existing systems, identifying requirements, and proposing solutions to improve efficiency, functionality, and performance.

- **System Design:** The process of defining the architecture, components, and specifications of a system based on the identified requirements and objectives.

- The system design involves:
    a. Defining precisely the required system output
    b. Determining the data requirement for producing the output
    c. Determining the medium and format of files and databases
    d. Devising processing methods and use of software to produce output
    e. Determine the methods of data capture and data input
    f. Designing Input forms
    g. Designing Codification Schemes
    h. Detailed manual procedures
    i. Documenting the Design

Security Considerations in System Analysis and Design

- **Confidentiality:** Ensuring that sensitive information is only accessible to authorized users and protected from unauthorized access or disclosure.
- **Integrity:** Safeguarding the accuracy and completeness of data and preventing unauthorized modification, tampering, or corruption.
- **Availability:** Ensuring that systems and resources are accessible and operational when needed, mitigating the risk of disruptions or downtime.
- **Authentication and Authorization:** Verifying the identity of users and determining their privileges and access rights based on predefined roles and permissions.
- **Data Protection:** Implementing mechanisms such as encryption, and access controls to protect data from unauthorized access or theft.
- **Auditability:** Incorporating logging and monitoring capabilities to track system activities and detect security incidents or policy violations

Incorporating Security into System Development

- As cyber threats continue to evolve, the integration of security into every stage of system development has become imperative.

- The strategies, methodologies, and best practices for effectively incorporating security into system development processes becomes vital

Security by Design Principles

- **Proactive Approach:** Embedding security considerations from the initial stages of system development to anticipate and mitigate potential risks.
- **Defense in Depth:** Implementing multiple layers of security controls to provide redundancy and resilience against various threats.
- **Least Privilege:** Restricting user privileges to the minimum necessary level to perform their tasks, reducing the potential impact of security breaches.
- **Fail-Safe Defaults:** Configuring systems to operate securely by default, minimizing the risk of misconfigurations or insecure settings.
- **Secure Defaults:** Choosing secure settings and configurations for system components, applications, and services to minimize vulnerabilities.

Ethics of Information Communication Technology

- Globalization and digital convergence in the emerging knowledge society have introduced complex ethical, legal, and societal challenges. We now confront intricate questions about freedom of expression, access to information, the right to privacy, intellectual property rights, and cultural diversity.

- Information and Communication Technology (ICT) is essential for gathering information and knowledge, and should therefore be recognized as a basic human right. Despite existing legal protections, rights are frequently violated worldwide under the pretexts of economic progress, political stability, religious motivations, anti-terrorism efforts, or personal gain

- Information technology is influencing every aspect of life globally. Advances in ICT have enabled a shift in how information is stored, processed, and shared, moving from paper to digital formats and from physical atoms to digital bits.

- This transition has established new benchmarks for speed, efficiency, and accuracy in human endeavours. Extensive use of computerized databases to store confidential political, social, economic, and personal data supports numerous human activities and brings various benefits to society.

- Thus, there is a need for awareness, policy formation, and enactment of necessary legislation in all countries for the prevention of computer related crime. Globally, internet and computer-based commerce and communications cut across territorial boundaries, thereby creating a new realm of human activities, and undermining the feasibility and legitimacy of applying laws based on geographic boundaries.

- Cyber systems worldwide operate under diverse rules governing user behaviour. Users have the freedom to join or leave any system based on their comfort with its rules. However, this flexibility can sometimes result in improper conduct.
- Additionally, without an appropriate legal framework, system administrators may struggle to prevent fraud, vandalism, or other abuses, potentially making the online experience unpleasant for many users.
- This situation is alarming because any element of distrust for the internet may lead to people avoiding online transactions, thereby directly affecting the growth of e-commerce. The use or misuse of the internet as a medium of communication may in some situations lead to direct damage to real physical society

What is Ethics

- In the past decade, numerous ethics centres and programs focusing on business ethics, legal ethics, bioethics, medical ethics, engineering ethics, and computer ethics have emerged. These centres aim to explore the implications of moral principles and practices across all areas of human activity.
- Ethics can be understood from two perspectives: normative and prescriptive.

➢Normatively, ethics refers to well-founded standards of right and wrong that dictate what humans ought to do, typically regarding rights, obligations, societal benefits, fairness, and specific virtues.

➢Prescriptively, ethics encompasses standards that obligate individuals to refrain from actions like rape, theft, murder, assault, slander, and fraud, and to embody virtues such as honesty, compassion, and loyalty.

- Ethics refers to the study and development of personal ethical standards, as well as community ethics, in terms of behaviour, feelings, laws, and social habits and norms which can deviate from more universal ethical standards. So it is necessary to constantly examine one’s standards to ensure that they are reasonable and well-founded.

- Ethics also means, then, the continuous effort of studying of our own moral beliefs and conduct, and striving to ensure that we, and our community and the institutions we help to shape, live up to standards that are reasonable and solidly-based for the progress of human beings.

- “***Ethics** are moral standards that help guide behaviour, actions, and choices*. Ethics are grounded in the notion of responsibility (as free moral agents, individuals, organizations, and societies are responsible for the actions that they take) and accountability (individuals, organizations, and society should be held accountable to others for the consequences of their actions).

- In most societies, a system of laws codifies the most significant ethical standards and provides a mechanism for holding people, organizations, and even governments accountable.” (Laudon, et al, 1996).

ICT Ethics

- ICT ethics are not exceptional from the above-mentioned view of ethics. In a world where information and communication technology has come to define how people live and work, and has critically affected culture and values.

ICT Ethical Issues

- Analysing and evaluating the impact of a new technology, such as ICT, can be very difficult. ICT does not only involve technological aspects, but also epistemology since the main component of ICT is information which represents data, information, and knowledge. ICT assists and extends the ability of mankind to capture, store, process, understand, use, create, and disseminate information at a speed and scale which had never been thought possible before.

UNESCO's Info-Ethics Programme

- The development of digital technologies and their application in global information networks are creating vast new opportunities for efficient information access and use by all societies. Every nation can fully benefit from these opportunities, provided they can address the challenges posed by these information and communication technologies. To this end, UNESCO established the Info-Ethics Programme with the primary objective of reaffirming the importance of universal access to public domain information and defining ways to achieve and maintain this within the Global Information Infrastructure.
- The program seeks to address the ethical, legal, and societal challenges of cyberspace, as well as privacy and security concerns. It aims to foster international cooperation in the following areas:

- Promotion of the principles of equality, justice and mutual respect in the emerging Information Society;
- Identification of major ethical issues in the production, access, dissemination, preservation and use of information in the electronic environment; and
- Provision of assistance to Member States in the formulation of strategies and policies on these issues.

Identity and Information Security Integration

Historically, in distributed computing, identity management and information security were often handled independently. While security teams collaborated with software developers and IT operations on aspects such as user authentication and password management, overall cooperation was limited. Generally, identity and security remained separate for the following reasons:

a. **Identity management focused on employee productivity**

b. **Security teams focused on IT infrastructure and security attacks**

c. **Need for Identity and Information Security Integration**

d. **Regulatory compliance requires strong access and security controls**

e. **Think Identity and Access Assurance**

f. **Data discovery, classification, and security policy enforcement**.

g. **Security monitoring and analysis**

h. **Authentication management**

i. **Access certification**

Management Information Systems Usability and Associated Risk

- A management information system (MIS) is a system or process that delivers the information needed to manage an organization effectively. MIS and the information it produces are widely regarded as crucial for making prudent and informed business decisions.
- Maintaining a consistent approach to developing, utilizing, and reviewing MIS systems is a continuous priority for both management and technical staff within any institution.
- MIS should have a clearly defined framework of guidelines, policies or practices, standards, and procedures for the organization. These should be followed throughout the institution in the development, maintenance, and use of all MIS.

Importance Management Information Systems

An institution's MIS should be designed to achieve the following goals:

- Enhance communication among employees.
- Deliver complex material throughout the institution.
- Provide an objective system for recording and aggregating information
- Reduce expenses related to labour-intensive manual activities.
- Support the organization's strategic goals and direction.

Risks Associated With Management Information Systems

- Risk represents the potential, likelihood, or expectation of events that could negatively impact earnings or capital. Management utilizes MIS to assess risk within an institution. Decisions based on ineffective, inaccurate, or incomplete MIS can elevate risk in various areas, such as credit quality, liquidity, market/pricing, interest rates, or foreign currency. A flawed MIS introduces operational risks and can impair an organization's ability to monitor its fiduciary duties, consumer practices, fair lending, Bank Secrecy Act compliance, and other regulatory obligations.
- Because management needs accurate information to evaluate and oversee performance at all organizational levels, MIS risks can permeate all operations. Additionally, poorly programmed or insecure systems, where data can be manipulated or require frequent repairs, can disrupt routine workflows and lead to incorrect decisions or compromised planning.

Assessing Vulnerability To Management Information Systems Risk

- To function effectively as an interacting, interrelated, and interdependent feedback tool for management and staff, MIS must be "useable." The five elements of a useable MIS system are:

a. Timeliness

b. Accuracy

c. Consistency

d. Completeness and

e. Relevance.

The usefulness of MIS is hindered whenever one or more of these elements are compromised.

The Information Systems and the Economics of Innocent Fraud Management

- In his work, John Kenneth Galbraith succinctly portrays the contemporary economic system as "the economics of innocent fraud" (Galbraith, 2004), encapsulating what could be regarded as a testament of intellectual insight. This characterization delineates an economy divorced from reality, where the private sphere dictates the public domain (particularly through the defense and arms industry) and corporations wield power undemocratically, with a minority of shareholders holding sway.

- It's a system where the impoverished struggle to access necessary funds for spending, while the affluent receive income they predominantly save (attributed by Galbraith to global tax cut policies). Moreover, it's an economy where a select elite profess to understand the uncertainties of economic change, often demanding exorbitant fees for their insights.
- In essence, this economy constitutes a significant deception against humanity. This deception can range from unwitting acceptance, ingrained as the norm and perpetuated with good intentions, especially by mass media which fail to condemn it, to instances laden with selfishness and malice.

The Role of ICT in fraud: The clearing case

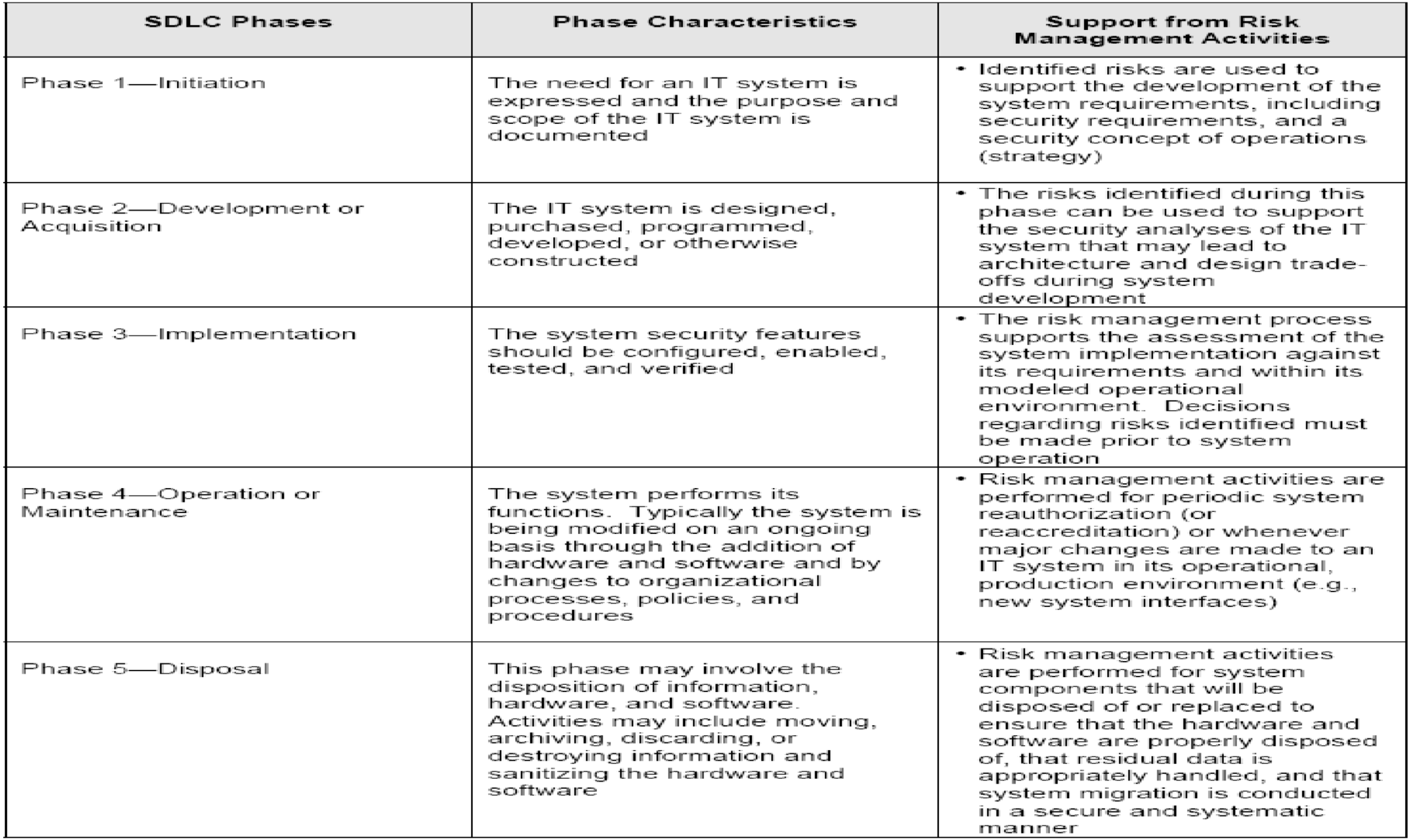
- It's not a paradox but rather a matter of common sense that the very technology enabling the existence of parallel opaque financial systems might hold the key to altering this state of affairs.
- This fundamental insight emerges from a significant investigation outlined in two books that have largely flown under the radar of public opinion: "Révélations" (Revelations) (2001) and "La boîte noire" (The Black Box) (2002). Authored by French researcher and journalist Denis Robert, these books chronicle a thorough and extensive investigation, demonstrating, among other findings, that the vulnerability of criminal financial systems arises from the very strength of the system itself—namely, the utilization of ICTs.

Information Security as a risk management function

- Risk management is the process enabling IT managers to strike a balance between the operational and economic costs of protective measures, thereby enhancing mission capability by safeguarding the IT systems and data crucial to their organizations' objectives.
- This process isn't exclusive to the realm of IT; it permeates decision-making in various facets of daily life. Consider home security: many opt to install home security systems and subscribe to monitoring services to enhance property protection.

- Presumably, homeowners assess the cost of system installation and monitoring against the value of their possessions and family's safety—a fundamental "mission" necessity. Similarly, organizational leaders must ensure their entities possess the requisite capabilities to fulfill their missions.
- These mission owners determine the security measures their IT systems require to deliver the desired level of mission support amidst real-world threats. Given tight IT security budgets, expenditure in this domain warrants scrutiny akin to other management decisions.
- A well-structured risk management approach, when employed effectively, aids management in identifying suitable controls to furnish essential security capabilities for the mission.

- Minimizing negative impact on an organization and need for sound basis in decision making are the fundamental reasons organizations implement a risk management process for their IT systems. Effective risk management must be totally integrated into the SDLC.
- An IT System Development Life Cycle (SDLC) has five phases: initiation, development or acquisition, implementation, operation or maintenance, and disposal. In some cases, an IT system may occupy several of these phases at the same time. However, the risk management methodology is the same regardless of the SDLC phase for which the assessment is being conducted. Risk management is an iterative process that can be performed during each major phase of the SDLC.



SDLC Phases	Phase Characteristics	Support from Risk Management Activities
Phase 1—Initiation	The need for an IT system is expressed and the purpose and scope of the IT system is documented	• Identified risks are used to support the development of the system requirements, including security requirements, and a security concept of operations (strategy)
Phase 2—Development or Acquisition	The IT system is designed, purchased, programmed, developed, or otherwise constructed	• The risks identified during this phase can be used to support the security analyses of the IT system that may lead to architecture and design trade-offs during system development
Phase 3—Implementation	The system security features should be configured, enabled, tested, and verified	• The risk management process supports the assessment of the system implementation against its requirements and within its modeled operational environment. Decisions regarding risks identified must be made prior to system operation
Phase 4—Operation or Maintenance	The system performs its functions. Typically the system is being modified on an ongoing basis through the addition of hardware and software and by changes to organizational processes, policies, and procedures	• Risk management activities are performed for periodic system reauthorization (or reaccreditation) or whenever major changes are made to an IT system in its operational, production environment (e.g., new system interfaces)
Phase 5—Disposal	This phase may involve the disposition of information, hardware, and software. Activities may include moving, archiving, discarding, or destroying information and sanitizing the hardware and software	• Risk management activities are performed for system components that will be disposed of or replaced to ensure that the hardware and software are properly disposed of, that residual data is appropriately handled, and that system migration is conducted in a secure and systematic manner

Conclusion

- To minimize risk to the IT systems, it is essential that system and application users be provided with security awareness training. Therefore, the IT security trainers or security/subject matter professionals must understand the risk management process so that they can develop appropriate training materials and incorporate risk assessment into training programs to educate the end users.

Review of the Class Activities

- Students Project/ Assignment and Class Presentation

Reference

- Information Security Management Principles" by David Alexander and Amanda Finch
- K.E.Kendell and J.E.Kendell 2002. Systems Analysis and Design. Pearson Education Asia pp.117-196.
- Barwise, Jon and John Etchemendy. (2001). "Computers, Visualization, and the Nature of Reasoning." Accessible in PDF format via *http://morpheus.hartford.edu/~anderson/*
- Information Security Management Principles" by David Alexander and Amanda Finch.
- Risk Management in Information Security" by M. Kabay and D. Blyler.
- Security Engineering: A Guide to Building Dependable Distributed Systems" by Ross J. Anderson
- ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems -- Requirements" (International Standard).
- Water Quality: Guidelines, Standards, and Health" by World Health Organization.
- "Computer Ethics" by Deborah G. Johnson.

- "Security Culture: A How-To Guide for Improving Cybersecurity Culture and Dealing with People Risk in Your Organisation" by Kai Roer.
- "Principles of Information Security" by Michael E. Whitman and Herbert J. Mattord.
- Innovation and Its Enemies: Why People Resist New Technologies" by Calestous Juma.
- “Security Economics: A Guide for Decision Makers" by Ross Anderson, Tyler Moore, and Shishir Nagaraja.
- “Future Crimes: Everything Is Connected, Everyone Is Vulnerable, and What We Can Do About It” by Marc Goodman.
- Hoffman, L. (1995). Encryption Policy for the Global Information Infrastructure, in Information Security: the next Decade, J. Eloff and S. Von Solms, ed. proceedings of the IFIPTC11 Eleventh International Conference on Information Security, South Africa, May 9-12, 1995, pp 50-63.
- Managing security of information of information technology committee, website at www.ifac.org/new. (IFAC 1998. Exclusive Summary).

- Broadhurst, R. (2002). E-commerce & Cybercrime: issues, problems & prevention. AsiaPacific Conference on Cybercrime and Information Security, Seoul, Republic of Korea, 11-13 November 2002.
- Computer Security Institute. CSI. (2003). CSI/FBI Computer Crime and Security Survey.
- Johnson, D.G. (1994). *Computer Ethics,* second edition; Englewood Cliffs, NJ, Prentice Hall.
- Laudon, K. 1995. “Ethical Concepts and Information Technology,” Communications of the ACM, December 1995 p 33-40.
- Laudon, K.C., Traver, C.G. and Laudon J.P. (1996). Information Technology and Society, Pp.513.
- Comptroller’s Handbook. 1995. Management Information Systems. A Call to Action for Corporate Governance. IIA, AICPA, ISACA,NACD, www.theiia.org/eSAC/pdf/BLG0331.pdf; March 2000.
-