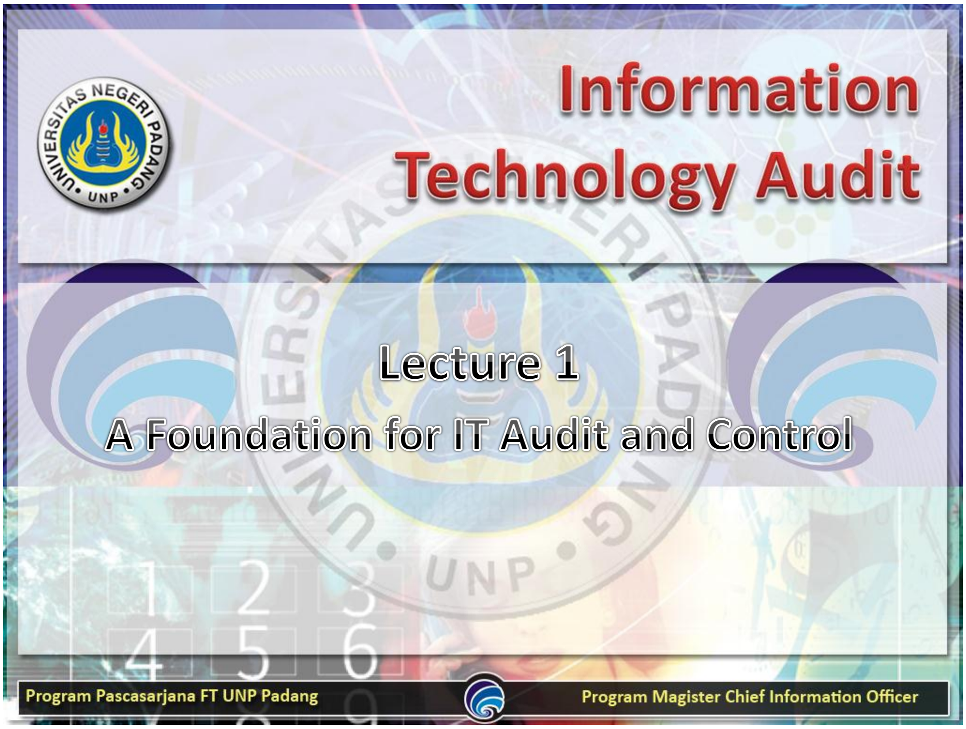
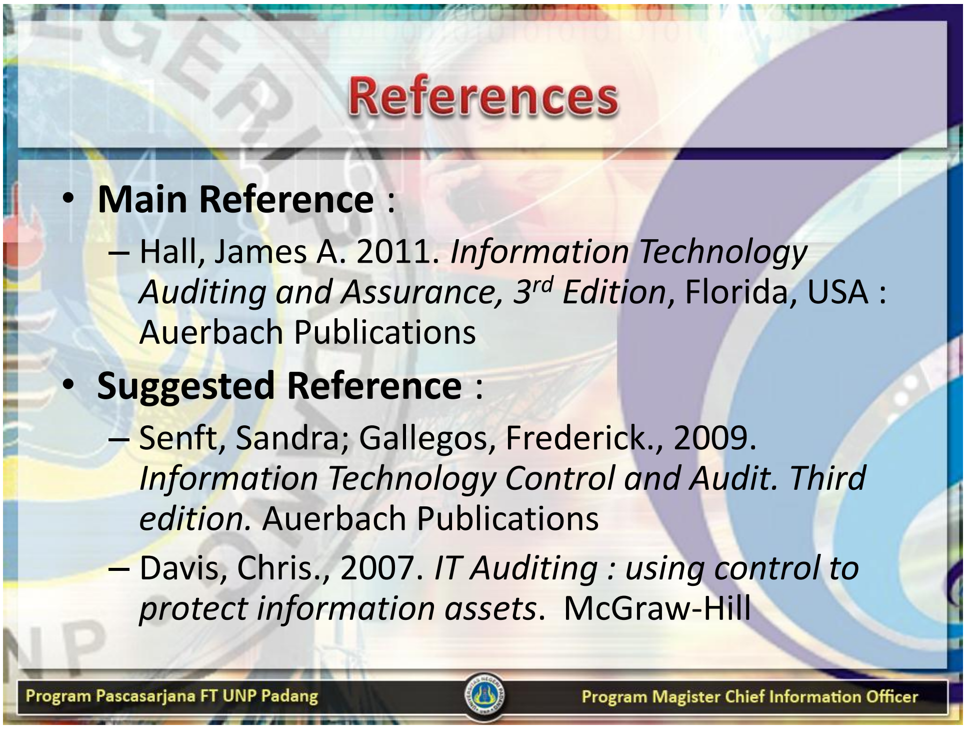


# Information Technology Audit

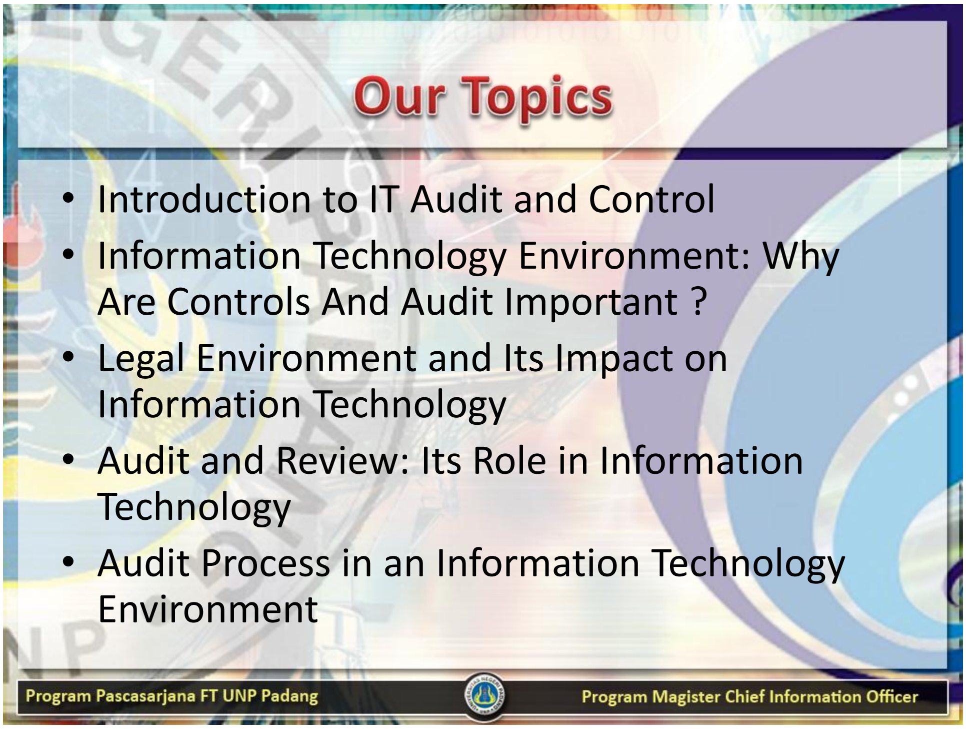
## Lecture 1

## A Foundation for IT Audit and Control



## References

- **Main Reference** :
  - – Hall, James A. 2011. *Information Technology Auditing and Assurance, 3$^{rd}$ Edition*, Florida, USA : Auerbach Publications
- **Suggested Reference** :
  - – Senft, Sandra; Gallegos, Frederick., 2009. *Information Technology Control and Audit. Third edition.* Auerbach Publications
  - – Davis, Chris., 2007. *IT Auditing : using control to protect information assets*. McGraw-Hill

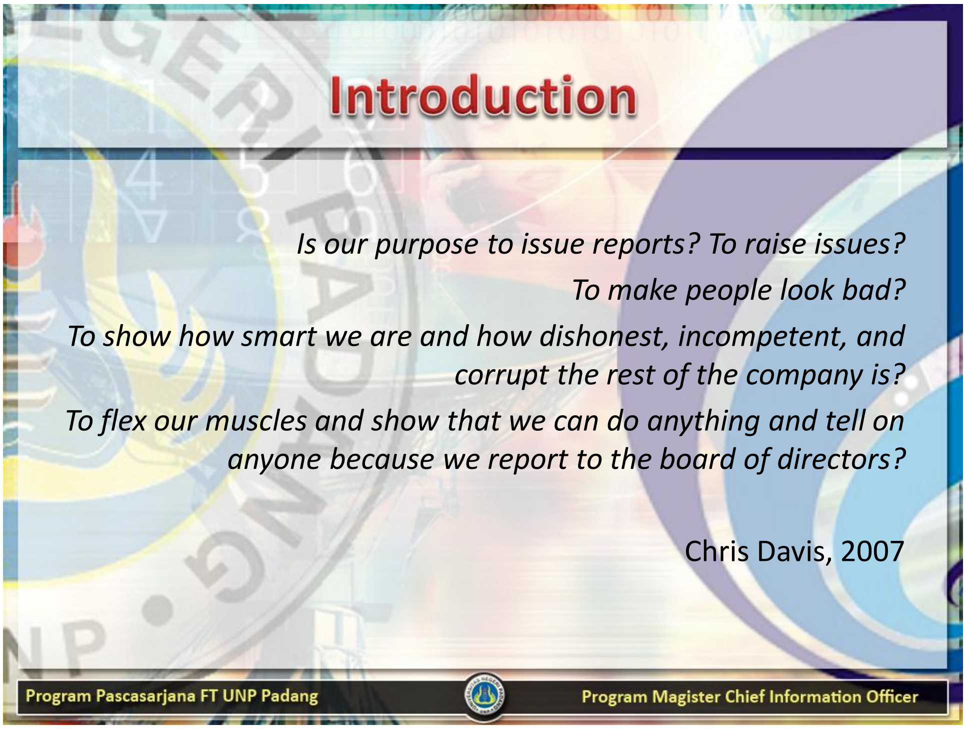


## Our Topics

- Introduction to IT Audit and Control
- Information Technology Environment: Why Are Controls And Audit Important ?
- Legal Environment and Its Impact on Information Technology
- Audit and Review: Its Role in Information Technology
- Audit Process in an Information Technology Environment

Program Pascasarjana FT UNP Padang

Program Magister Chief Information Officer



## Introduction

*Is our purpose to issue reports? To raise issues?*

*To make people look bad?*

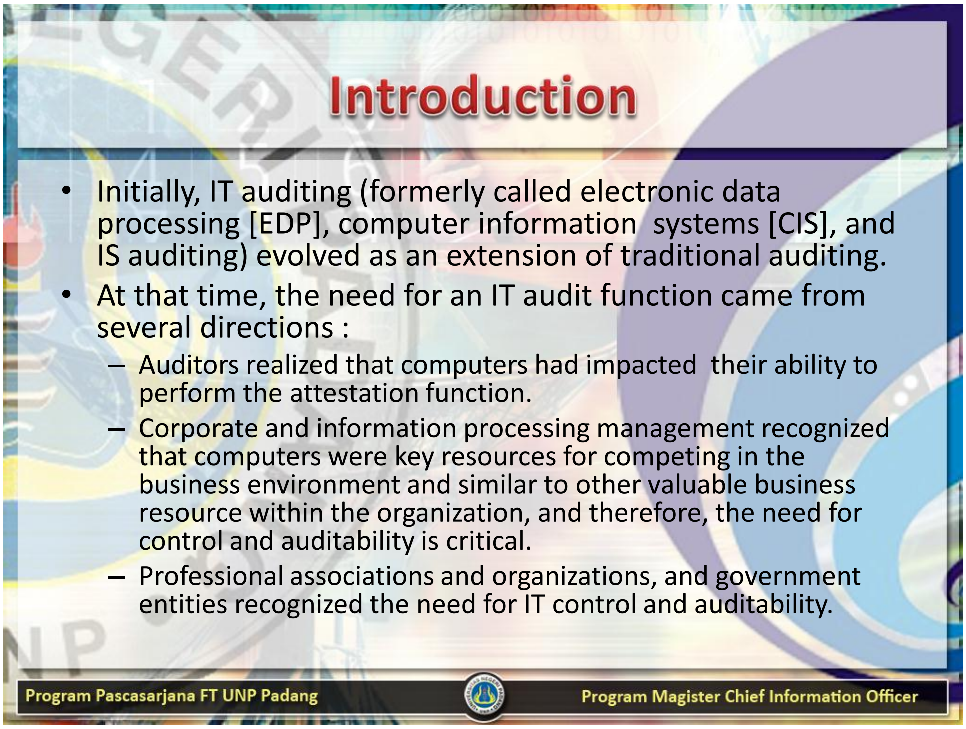
*To show how smart we are and how dishonest, incompetent, and corrupt the rest of the company is?*

*To flex our muscles and show that we can do anything and tell on anyone because we report to the board of directors?*

Chris Davis, 2007

Program Pascasarjana FT UNP Padang

Program Magister Chief Information Officer



# Introduction

- Initially, IT auditing (formerly called electronic data processing [EDP], computer information systems [CIS], and IS auditing) evolved as an extension of traditional auditing.
- At that time, the need for an IT audit function came from several directions :
  - Auditors realized that computers had impacted their ability to perform the attestation function.
  - Corporate and information processing management recognized that computers were key resources for competing in the business environment and similar to other valuable business resource within the organization, and therefore, the need for control and auditability is critical.
  - Professional associations and organizations, and government entities recognized the need for IT control and auditability.

Program Pascasarjana FT UNP Padang

Program Magister Chief Information Officer

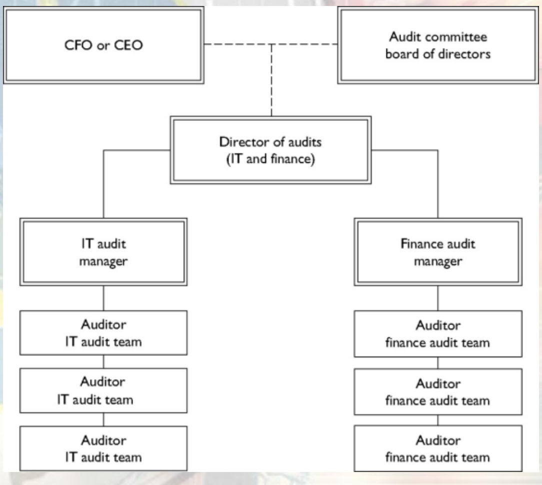
# Introduction

- IT auditing is an integral part of the audit function because it supports the auditor’s judgment on the quality of the information processed by computer systems
- there are many types of audit needs within IT auditing, such as :
  - Organizational IT audits (management control over IT),
  - Technical IT audits (infrastructure, data centers, data communication),
  - Application IT audit (business/financial/operational),
  - Development/implementation IT audits (specification/ requirements, design, development, and postimplementation phases),
  - Compliance IT audits involving national or international standards

Program Pascasarjana FT UNP Padang

Program Magister Chief Information Officer

# Who are IT Auditor?

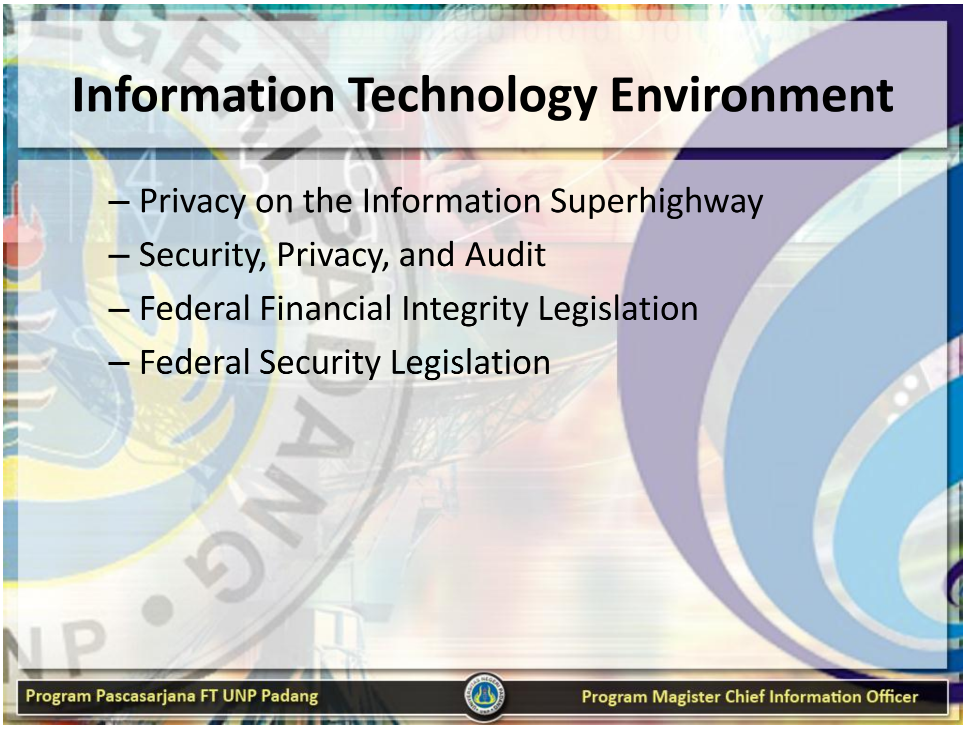

CFO or CEO
Audit committee board of directors
Director of audits (IT and finance)
IT audit manager
Finance audit manager
Auditor IT audit team
Auditor IT audit team
Auditor IT audit team
Auditor finance audit team
Auditor finance audit team
Auditor finance audit team

- an IT auditor plans to move into the IT organization
- it's probably best if the *chief information officer* (CIO)

- *Chris Davis, 2007*

# Information Technology Environment

- Information Technology Environment: Why Are Controls and Audit Important?
  - IT Today and Tomorrow
    - Information Integrity, Reliability, and Validity: Importance in Today’s Global Business Environment
  - E-Commerce and Electronic Funds Transfer
  - Future of Electronic Payment Systems
  - Legal Issues Impacting IT



# Information Technology Environment

- – Privacy on the Information Superhighway
- – Security, Privacy, and Audit
- – Federal Financial Integrity Legislation
- – Federal Security Legislation

Program Pascasarjana FT UNP Padang

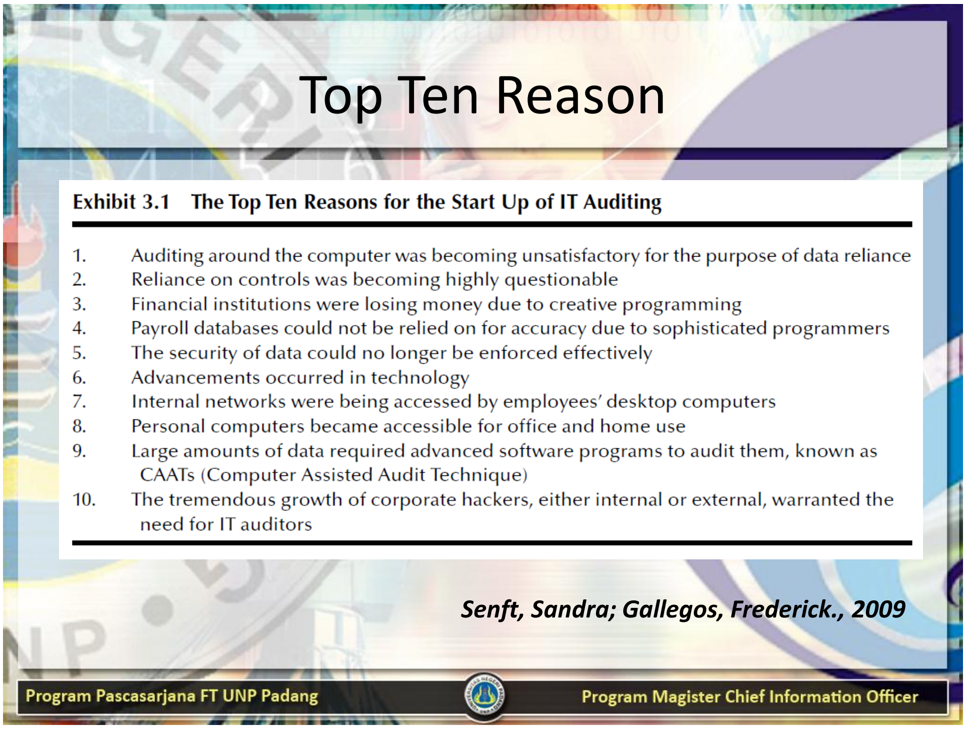
Program Magister Chief Information Officer

# Technology Impact on Bussiness

- Essentially, technology has impacted three significant areas of the business environment:
  - – It has impacted what can be done in business in terms of information and as a business enabler
  - – Technology has significantly impacted the control process
  - – Technology has impacted the auditing profession in terms of how audits are performed (information capture and analysis, control concerns) and the knowledge required to draw conclusions regarding operational or system effectiveness, efficiency and integrity, and reporting integrity

Program Pascasarjana FT UNP Padang

Program Magister Chief Information Officer

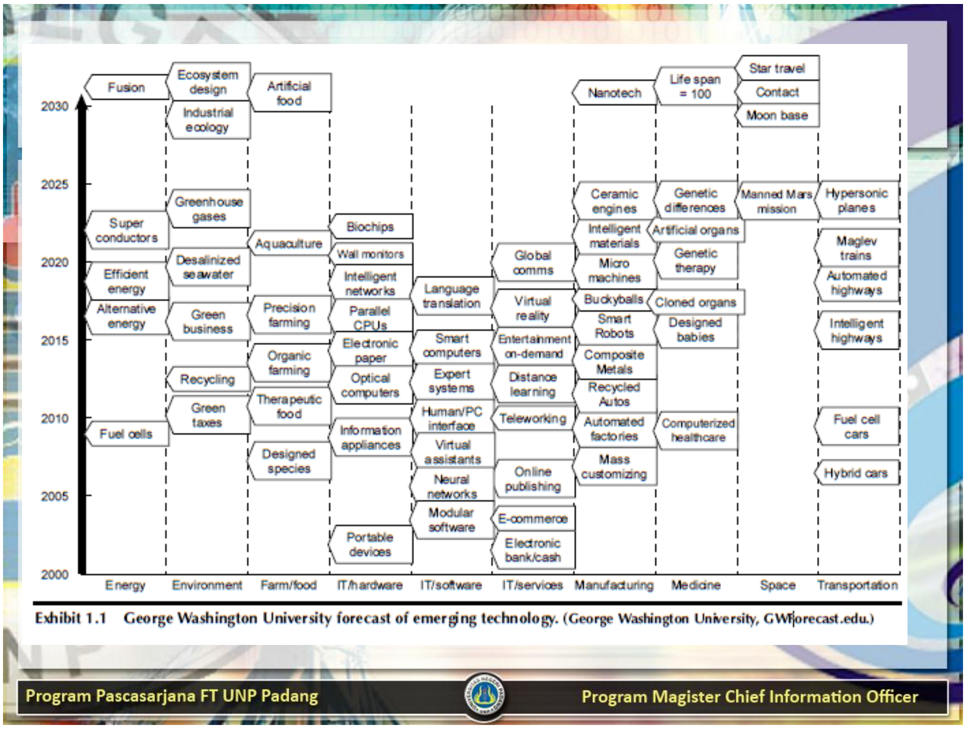


# Top Ten Reason

**Exhibit 3.1 The Top Ten Reasons for the Start Up of IT Auditing**

1. Auditing around the computer was becoming unsatisfactory for the purpose of data reliance
2. Reliance on controls was becoming highly questionable
3. Financial institutions were losing money due to creative programming
4. Payroll databases could not be relied on for accuracy due to sophisticated programmers
5. The security of data could no longer be enforced effectively
6. Advancements occurred in technology
7. Internal networks were being accessed by employees' desktop computers
8. Personal computers became accessible for office and home use
9. Large amounts of data required advanced software programs to audit them, known as CAATs (Computer Assisted Audit Technique)
10. The tremendous growth of corporate hackers, either internal or external, warranted the need for IT auditors

***Senft, Sandra; Gallegos, Frederick., 2009***

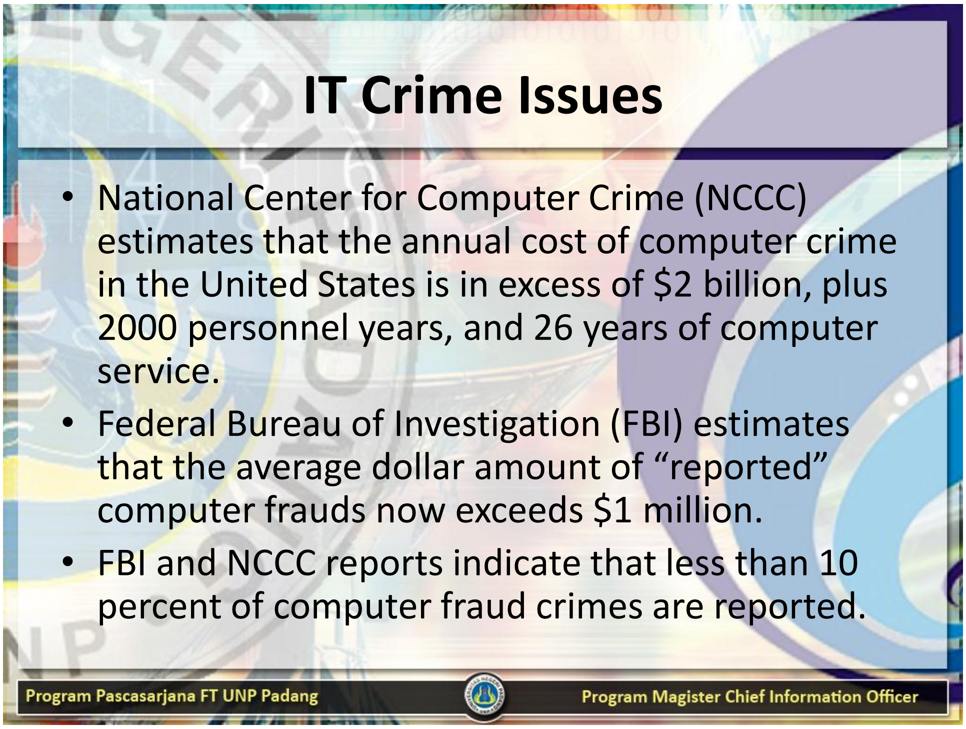


| Energy | Environment | Farm/food | IT/hardware | IT/software | IT/services | Manufacturing | Medicine | Space | Transportation |
|---|---|---|---|---|---|---|---|---|---|
| Fusion<br>Super conductors<br>Efficient energy<br>Alternative energy<br>Fuel cells | Ecosystem design<br>Industrial ecology<br>Greenhouse gases<br>Desalinized seawater<br>Green business<br>Recycling<br>Green taxes | Artificial food<br>Aquaculture<br>Precision farming<br>Organic farming<br>Therapeutic food<br>Designed species | Biochips<br>Wall monitors<br>Intelligent networks<br>Parallel CPUs<br>Electronic paper<br>Optical computers<br>Information appliances<br>Portable devices | Language translation<br>Smart computers<br>Expert systems<br>Human/PC interface<br>Virtual assistants<br>Neural networks<br>Modular software | Global comms<br>Virtual reality<br>Entertainment on-demand<br>Distance learning<br>Teleworking<br>Online publishing<br>E-commerce<br>Electronic bank/cash | Nanotech<br>Ceramic engines<br>Intelligent materials<br>Micro machines<br>Buckyballs<br>Smart Robots<br>Composite Metals<br>Recycled Autos<br>Automated factories<br>Mass customizing | Life span = 100<br>Genetic differences<br>Artificial organs<br>Genetic therapy<br>Cloned organs<br>Designed babies<br>Computerized healthcare | Star travel<br>Contact<br>Moon base<br>Manned Mars mission | Hypersonic planes<br>Maglev trains<br>Automated highways<br>Intelligent highways<br>Fuel cell cars<br>Hybrid cars |

**Exhibit 1.1** George Washington University forecast of emerging technology. (George Washington University, GWforecast.edu.)

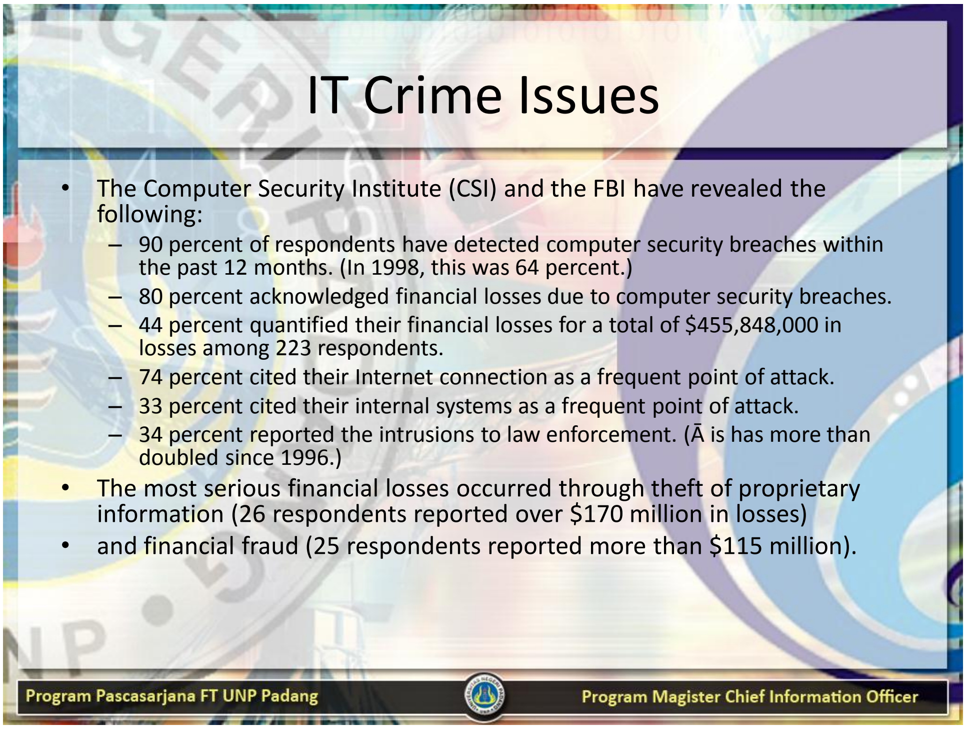
# A Legal Environment

- A Legal Environment and Its Impact on Information Technology
  - IT Crime Issues
  - Protection against Computer Fraud
  - Remedies and Effectiveness
  - The National Strategy for Securing Cyberspace



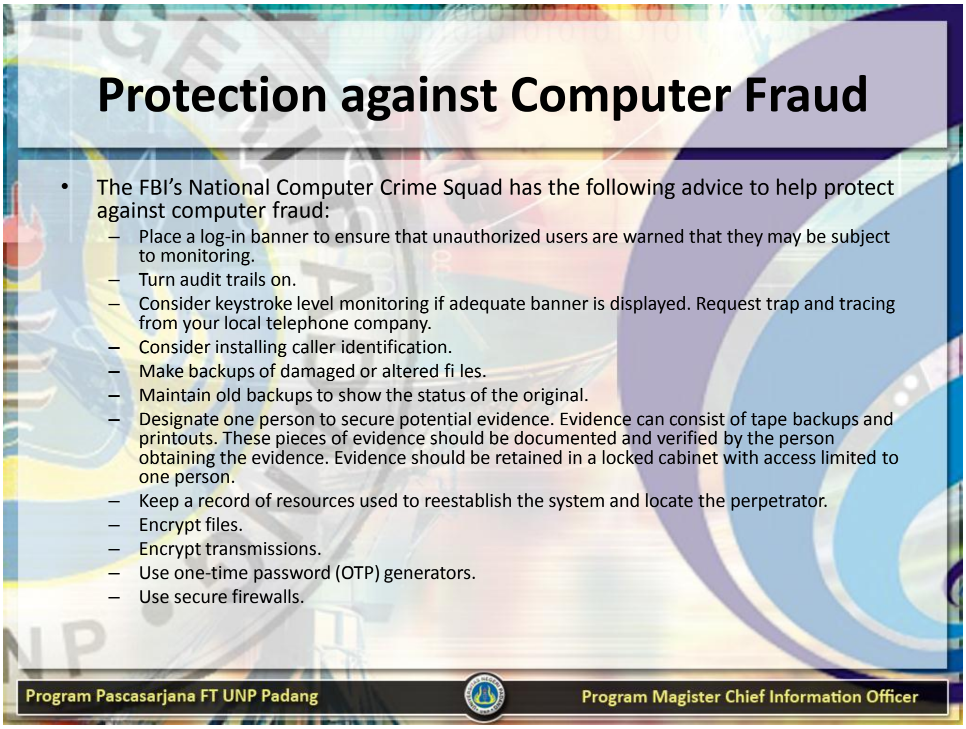
# IT Crime Issues

- National Center for Computer Crime (NCCC) estimates that the annual cost of computer crime in the United States is in excess of $2 billion, plus 2000 personnel years, and 26 years of computer service.
- Federal Bureau of Investigation (FBI) estimates that the average dollar amount of “reported” computer frauds now exceeds $1 million.
- FBI and NCCC reports indicate that less than 10 percent of computer fraud crimes are reported.



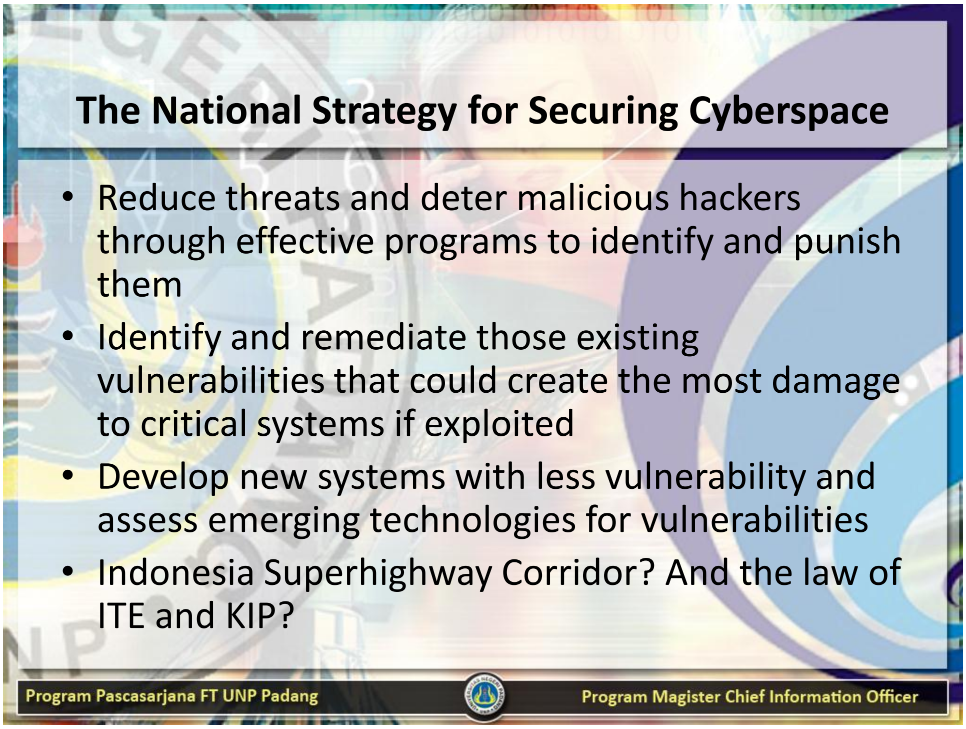
# IT Crime Issues

- The Computer Security Institute (CSI) and the FBI have revealed the following:
  - 90 percent of respondents have detected computer security breaches within the past 12 months. (In 1998, this was 64 percent.)
  - 80 percent acknowledged financial losses due to computer security breaches.
  - 44 percent quantified their financial losses for a total of $455,848,000 in losses among 223 respondents.
  - 74 percent cited their Internet connection as a frequent point of attack.
  - 33 percent cited their internal systems as a frequent point of attack.
  - 34 percent reported the intrusions to law enforcement. (Ā is has more than doubled since 1996.)
- The most serious financial losses occurred through theft of proprietary information (26 respondents reported over $170 million in losses)
- and financial fraud (25 respondents reported more than $115 million).



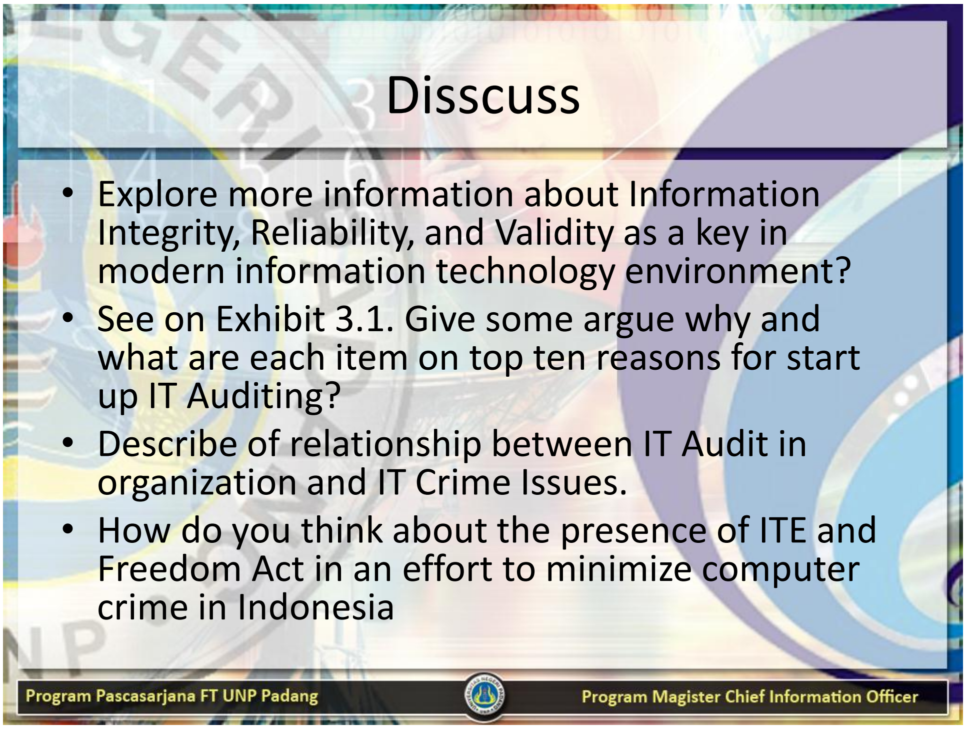
# Protection against Computer Fraud

- The FBI’s National Computer Crime Squad has the following advice to help protect against computer fraud:
  - Place a log-in banner to ensure that unauthorized users are warned that they may be subject to monitoring.
  - Turn audit trails on.
  - Consider keystroke level monitoring if adequate banner is displayed. Request trap and tracing from your local telephone company.
  - Consider installing caller identification.
  - Make backups of damaged or altered files.
  - Maintain old backups to show the status of the original.
  - Designate one person to secure potential evidence. Evidence can consist of tape backups and printouts. These pieces of evidence should be documented and verified by the person obtaining the evidence. Evidence should be retained in a locked cabinet with access limited to one person.
  - Keep a record of resources used to reestablish the system and locate the perpetrator.
  - Encrypt files.
  - Encrypt transmissions.
  - Use one-time password (OTP) generators.
  - Use secure firewalls.



## The National Strategy for Securing Cyberspace

- Reduce threats and deter malicious hackers through effective programs to identify and punish them
- Identify and remediate those existing vulnerabilities that could create the most damage to critical systems if exploited
- Develop new systems with less vulnerability and assess emerging technologies for vulnerabilities
- Indonesia Superhighway Corridor? And the law of ITE and KIP?



## Disscuss

- Explore more information about Information Integrity, Reliability, and Validity as a key in modern information technology environment?
- See on Exhibit 3.1. Give some argue why and what are each item on top ten reasons for start up IT Auditing?
- Describe of relationship between IT Audit in organization and IT Crime Issues.
- How do you think about the presence of ITE and Freedom Act in an effort to minimize computer crime in Indonesia