Cyberlaw

Vidyalankar Institute of Technology

Electronics & Telecommunication Department

Academic Year 2020 – 2021

Subject: ILO1016 - Cyber Security and Laws

Semester: I

Subject Teacher

Prof. Harshada Rajale

VIT Vidyalankar Institute of Technology

Accredited A+ by NAAC

University of Mumbai

Cyberlaw

- Cyber Law is the term which deals with the issues related to the internet, communication technology, technological & electronic elements including hardware, software, computer & information systems.

Top Colleges/ Universities of India offers Cyber law courses:

- All National Law Universities (NLUs)
- National Law School of India University, Bangalore
- NALSAR University of Law, Hyderabad
- ILS Law College, Pune
- Indian Institute of Information and Technology, Allahabad

Some of the career prospects are:

- Become a lawyer working in IT companies
- Specialist in Cyber/IT Based Arbitration
- Security Computer Auditors
- Techno-legal Professional in Computer Security

Candidates holding degree in cyber law may be designated as:

- Cyber Lawyer
- Legal Advisor
- Cyber Assistant

Candidates holding degree in cyber law may be designated as:

- Become a cyber consultant in IT firms or police department.
- Research assistant in law firm
- Research assistant in technology firm
- Security Auditors and Network Administrators in Technology firms.

Several challenges:

- Regular updating of knowledge, news & devices
- Keep up with changing & upgraded laws
- Lack of role-models
- Know-how of different technologies
- Performance based work environment

Salary

- In India, professional cyber lawyers earns an average pay of **6 lacs per year**.

- If you are working with reputed law firms, the you will get the demanding remuneration.

Cyber Security and Laws

Cyberspace

- Cyberspace refers to the virtual computer world, and more specifically, is an electronic medium used to form a global computer network to facilitate online communication.
- Cyberspace's core feature is an interactive and virtual environment for a broad range of participants.

E- Commerce

- Can be defined as buying and selling of goods, products, or services over the Internet
- Online transaction of money, funds transfer and data are also part of the e-commerce

Benefits of e- commerce

- Sellers can expand their markets
- Better and faster transactions
- Anytime service
- Reduces paper work
- Encourages digital payment
- Reduce physical efforts

Types of e-commerce

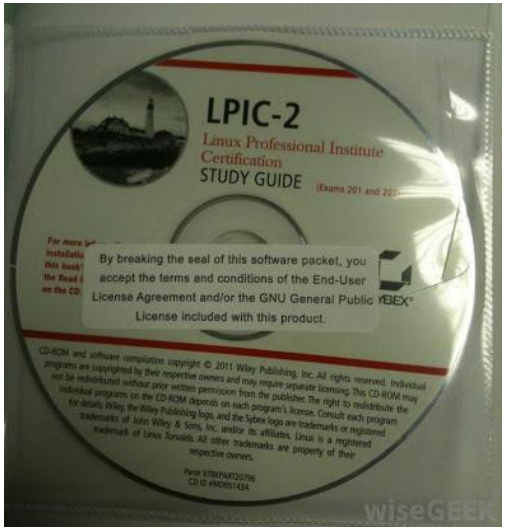
- B2C
- B2B
- C2C
- C2B
- G2C

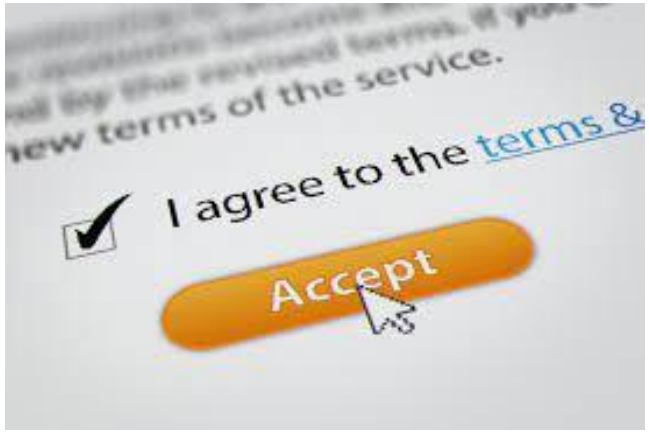
E-contract

- E-contract is any kind of contract formed in the course of e-commerce by the interaction of two or more individuals using electronic means that are programmed to recognize the existence of a contract.
- The Uniform Computer Information Transactions Act provides rules regarding the formation, governance, and basic terms of an e-contract.

Types of e- contract

- Shrink Wrap Contracts
- Click Wrap Contracts
- Browse Wrap Contracts





Indian Contract Act, 1872

- Defines the term “Contract” under section 2(h) as “An agreement enforceable by law”

Key terms defined in Indian Contract Act, 1872

Section	Key term
2(a)	Offer
2(b)	Acceptance
2(b)	Promise
2(c)	Promisor and Promisee
2(d)	Consideration
2(e)	Agreement
2(f)	Reciprocal Promises

Section	Key term
2(g)	Void agreement
2(h)	Contract
2(i)	Voidable contract
2(j)	Void contract

INTELLECTUAL PROPERTY IN CYBERSPACE

➢ Intellectual Property

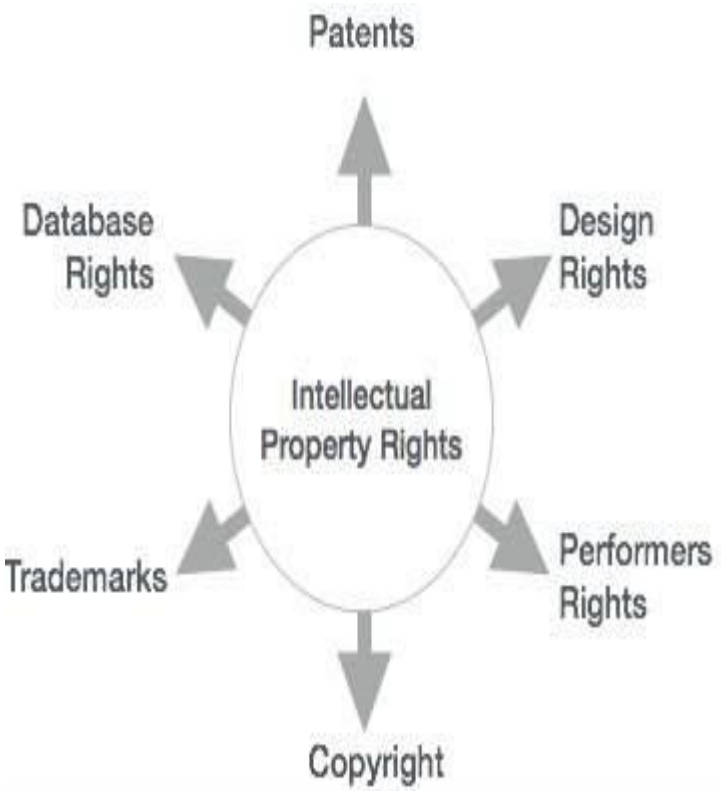
- Intellectual property rights are the legal rights that cover the privileges given to individuals who are the owners and inventors of a work, and have created something with their intellectual creativity.
- Individuals related to areas such as literature, music, invention, etc., can be granted such rights, which can then be used in the business practices by them.

➢ Why do we need intellectual property?

- The protection of Intellectual Property Rights (IPR) is important for the economy and for its further growth in areas such as research, innovation and employment.
- Effective IPR enforcement is also essential to health and safety.

➢ Intellectual Property Rights

•There are various kinds of tools of protection that come under the term ‘Intellectual Property’.
•Important among these are the following:



➢ Copyright

- Copyright is a kind of protection against unauthorized use or misuse of a work,but for a limited duration.
- Generally the rights includes the rights of authorship,reproduction,distribution,communication to the public,broadcasting,adaptation & translation.
- In India,copyright is governed by the Copyright Act,1957,the Copyright Rules ,1958 & the International Copyright Order,1999.

➢ Purpose of copyright:

The **purpose of copyright** law is to promote the progress of useful arts and science by protecting the exclusive right of authors and inventors to benefit from their works of authorship.

Trademarks

❖ **What is a Trademark?**

- A trademark is a unique symbol or word(s) used to represent a business or its products. Once registered, that same symbol or series of words cannot be used by any other organization, forever, as long as it remains in use and proper paperwork and fees are paid.
- Trademark are granted for a period of 20 years, trademarks never end. Companies do need to apply for them and receive ownership confirmation with the U.S. Patent and Trademark Office in order to claim protection from copycats, however.

❖ **Signs of a Trademark**

- To indicate that a trademark has been claimed companies use one of three symbols:

1. TM
2. ®
3. SM

➢ Patent

- Patent, is a legal document granted by the government giving an inventor the exclusive right to make,use,& sell an invention for a specified number of years.Patents are also available for significant improvements on previously invented items.

❖ Advantages of patents

- A **patent** gives you the right to stop others from copying, manufacturing, selling or importing your invention without your permission. See protecting intellectual property. You get protection for a pre-determined period, allowing you to keep competitors at bay.

- **Trade secret**

- The IP in the form of formula, practice, process, design, instrument, pattern, commercial method or compilation of information which is generally not known to the public and using which a business can obtain economic advantage over competitors or customers

- **Geographical Indication**
- Name or sign used on products which corresponds to specific geographical location or origin indicating the source of product.

- **Industrial design**
- constitutes the ornamental or aesthetic aspect of an article.

IP Laws and Cyberspace in India

- Indian Copyright Act, 1957
- Patent Act, 1970

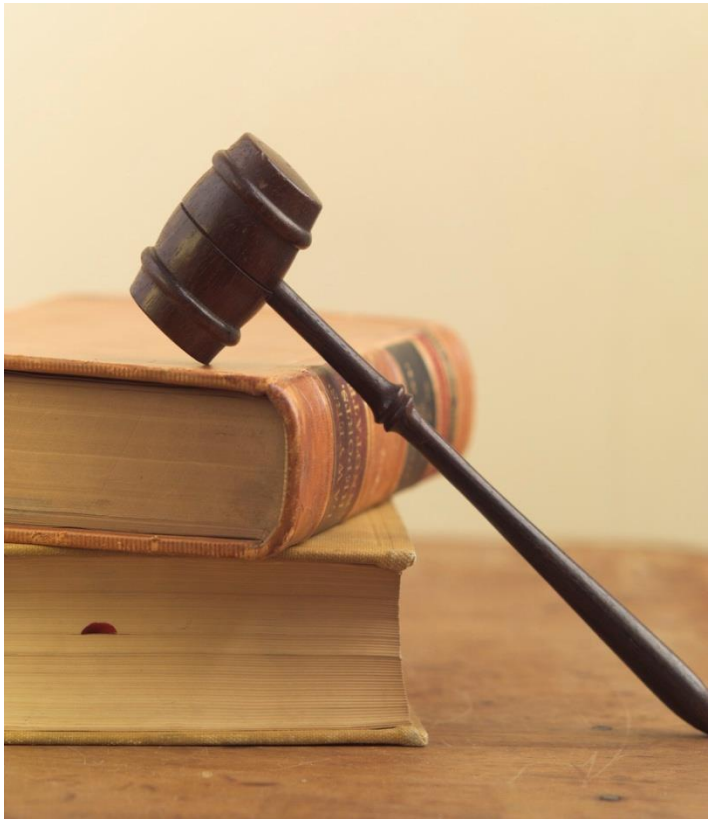
Information Technology Act 2000- An overview

Contents

- Need of cyberlaw
- IT Act 2000
- Objective of ITA 2000
- Cybercrime provisions under IT Act,2000
- IT Amendment Bill 2008
- Positive aspects of ITA 2000
- Weak areas of ITA 2000

Need of cyberlaw

- provide legal infrastructure for E-commerce.
- Framework created to give legal recognition
- To have some legal recognition to the Internet
- To protect against **cyberterrorism**



IT Act, 2000

- India has adopt cyber laws on 17th May 2000

- It consist of 94 sections segregated into 13 chapters.

Objectives of the IT Act

To provide legal recognition for transactions:-

- Carried out by means of electronic data interchange
- To facilitate electronic filing of documents
- To amend (alter) the Indian Penal Code, Indian Evidence Act,1872, the Banker's Books Evidence Act 1891, Reserve Bank of India Act ,1934

Cybercrime provisions under IT Act,2000

Section	Offence
65	Tampering with Computer source documents
66	Hacking with Computer systems, Data alteration
67	Publishing obscene information
71	Misrepresentation
72	Breach (break) of Confidentiality and Privacy
73	Publishing false digital signature certificates
74	Publication for fraudulent purpose

Section 65: Source Code

Offence	Penalty
• Knowingly or intentionally concealing, destroying or altering any computer source code • Computer Source Code means the listing of programmes, computer commands, design and layout Ingredients	• Custody of 3 years • Fine 2 lakhs

Section 66 : Hacking

Offence	Penalty
• Intention or knowledge to cause wrongful loss or damage to the public or any person • Destruction, deletion, alteration, diminishing value or utility or injuriously affecting information residing in a computer resource	• Custody of 3 years • Fine 2 lakhs

Sec. 67: Pornography

Offence	Penalty
Publishing or transmitting or causing to be published in the electronic form, Obscene material	On first conviction • Imprisonment 5 years • Fine 1 lakh
	On subsequent conviction • Imprisonment 10 years • Fine 2 lakhs

Section 71: Misrepresentation to the Controller or the Certifying Authority

Offence	Penalty
Making any misrepresentation to, or suppression of any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate, as the case may be.	• Imprisonment 2 years • Fine 1 lakhs

Section 72: Penalty for breach (break) of confidentiality and privacy

Offence	Penalty
Any person who, in pursuance of any of the powers conferred under IT Act, has secured access to any electronic record, book, register, correspondence, information or document without the consent of the person concerned discloses such electronic record, book., register, correspondence, information, document to any other person.	• Imprisonment 2 years • Fine 1 lakhs

Section 73: Publishing Digital Signature Certificate false in certain particulars

Offence	Penalty
Publishing a Digital Signature Certificate or otherwise making it available to any other person with the knowledge tha*t* 1) The Certifying Authority listed in the certificate has not issued it or 2) The subscriber listed in the certificate has not accepted it or 3) The certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.	• Imprisonment 2 years • Fine 1 lakhs

Section 74: Publication for fraudulent purpose

Offence	Penalty
Creation, publication or otherwise making available a Digital signature Certificate for any fraudulent or unlawful purpose	• Imprisonment 2 years • Fine 1 lakhs

IT Amendment Bill 2008

- ITAA 2008 is new version of ITA 2000 which provides additional focus on Information Security.

- In the 2008 version of the Act, there are 124 sections (excluding 5 sections that have been omitted from the earlier version) and 14 chapters.

IT Amendment Bill 2000

- Schedules of ITA 2000 are amended
  - Second schedule –

    The Indian Evidence Act 1872
  - Third schedule –

    The Banker's Books Evidence Act 1891
  - Fourth schedule –

    The Reserve bank of India Act 1934

Amendment to the Indian Evidence Act.

- In section 3,words "all documents produce for inspection of the court." replace with

  "**all electronics documents produce for inspection of the court**."
- In section 17 , words " oral or documents are replace with "oral or documents or contain in **electronics form**"
- in Section 35 the word " records" is replace with " **electronics records**"
- In section 39, the electronics evidences such as documents, statements , conversation , series of letter or paper are consider by courts.

Amendment to the Indian Evidence Act.

- Sector 47 is modified as 47A where **digital certificate signature** is consider as a relevant fact.

- In section 59 , the words “ the contents of documents” replace with” **contents of documents or electronics records**”.

Admissibility of Electronics records

- Information contain in electronics record Presumption (agree) as to
- Gazette in electronics form.
- electronics agreements.
- electronics records and digital signature.
- digital certificate .
- electronics message.
- electronics records of five year old.

The Third schedule of the Indian IT act. 2000 : Amendment to the Banker Book Evidence ACT

- printed form or in floppy disk.

- After section 2 , New section 2A is introduce which deals with condition in printout.

Positive aspects of ITA 2000

- Prior to ITA 2000 even an Email was not accepted as an legal form of communication and as evidence in court of law
- Corporate will now able to carry out their transactions online
- ITA 2000 has given validity to digital transaction.

Weak areas of ITA 2000

- It is likely to cause a conflict of jurisdiction (auth. or control power)
- Not even touched the issues like
  - Domain names
  - Protection of intellectual property
  - Online copyrights, trademarks and patents
  - Antitrust issues
- Does not cover various cybercrimes like
  - Theft of internet hours
  - Cybertheft
  - Cyberstalking
  - Misuse of credit card numbers

- Challenges to Indian Law and Cyber crime scenario in India

  - Law does not provide legal definition of cyber crime.
  - IPC does not use term *cybercrime* after amendment of ITA 2000.
  - In ITA 2000 cybercrime declare as a penal offences punishable with custody and fine.

Offenses Covered under ITA 2000

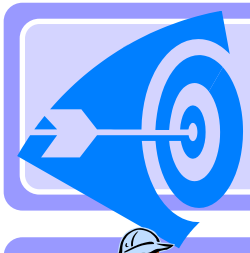
- Tampering with computer source code
- Unauthorized access to computer
- Publishing, transmitting any information in electronic form.
- Failure to decrypt information in interest of integrity of India ,security of state.
- Accessing to protected systems.
- Publication of Digital Signature certificates which are false.
- Publication of Digital Signature certificates for fraudulent.

Legal drawbacks / Limitations

Most Indians do not report the cybercrime

Awareness on cybercrime is relatively low

•



Law enforcement agencies are neither well equipped nor knowledgeable enough

Dedicated and continuous training is required

Need for Today

- Distinct law
- Uniform guidelines
- Expedite
- Encourage people
- Can follow the example set by FBI
- Complete secrecy

Need for Today

- India cyber low does not prescribe punishment but made an ground for claiming compensation in terms of fine.

Consequences

- Indian cyber law is not strong
- India's outsourcing sector
- News about overseas customer worrying about data breaches and data leakages
- Quick and intelligent

Module 5: Indian IT Act. Cyber Crime and Criminal Justice

Outline

- Penalties, Adjudication and Appeals Under the IT Act, 2000,
- IT Act. 2008 and its Amendments

India Information Technology Act, 2000

Information Technology Act, 2000

- An Act of Indian Parliament (No 21 of 2000) notified on 17th October 2000 and became the primary law in India to deal with cybercrime and electronic commerce.

- It is based on the Model Law on e-commerce and with its adoption, India became the twelfth country to enable cyberlaw.

Features of the IT Act, 2000

- Provides legal recognition to records in electronic form
- Provides legal recognition to e-commerce and electronic transactions in India
- Provides legal recognition to digital signatures issued and authenticated by the Certifying authorities
- Applicable to cybercrimes and contraventions committed in India and outside India
- Has appointment adjudicating officers
- Elaborates on offences, penalties ad breaches
- Established the Cyber Appellate Tribunal to hear appeals

India Information Technology Amendment Act, 2008

Information Technology (Amendment) Act, 2008

- The Information Technology (Amendment) Act, 2008 makes amendments to the Information Technology Act, 2000

- It was passed by the Indian Parliament in October 2008 and came into force in 2009.

Information Technology (Amendment) Act, 2008

- The amendments include:
  - Redefining terms
  - Validating electronic signatures and contracts
  - Making the owner of a given IP address responsible for content accessed or distributed through it
  - Implementing effective data security practices

Information Technology (Amendment) Act, 2008

- The amendments were made to following sections of IT Act, 2000:
  - Section 43
  - Section 66
  - Section 67
  - Section 69
  - Section 72

Features of the IT Amendment Act, 2008

- Defines a “communication device”
- Defines “Cyber Cafe”
- Makes any contract concluded electronically
- Makes amendments to the penalties and punishments of the ITA 2000
- Provides power to the law enforcement agencies
- Section 66A to 66F has been added to Section 66
- Exempts intermediaries from being liable for any third-party information data or communication link

Penalties and offences under IT Act, 2000

Penalties, Compensation and Adjudication under the IT Act, 2000

- Section 43: Penalty for damage to computer, computer system, etc
- Section 43A: Compensation for failure to protect data
- Section 44: Penalty for failure to furnish information, return, etc
- Section 45: Residuary Penalty

Offences under the IT Act, 2000

- Section 65: Tampering with computer source documents
- Section 66: Computer related offences
- Section 66B: Punishment for dishonestly receiving stolen computer resource or communication device
- Section 66C: Punishment for identity theft
- Section 66D: Punishment for cheating by personation by using computer resource
- Section 66E: Punishment for violation of policy
- Section 66F: Punishment for cyberterrorism

Offences under the IT Act, 2000

- Section 67: Punishment for publishing or transmitting obscene material in electronic form.
- Section 67A: Punishment for publishing or transmitting of material containing sexually explicit act, etc in electronic form.
- Section 67B: Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc in electronic form.
- Section 67C: Preservation and retention of information by intermediaries
- Section 68: Power of controller to give directions

Offences under the IT Act, 2000

- Section 69: Power to issue directions for interception and monitoring or decryption of any information through any computer resource
- Section 70: Protected System
- Section 71: Penalty for misrepresentation
- Section 72: Breach of confidentiality and privacy
- Section 72A: Punishment for disclosure of information in breach of lawful contract

Cyber Appellate Tribunal

- Section 48: Establishment of Cyber Appellate Tribunal
- Section 57: Appeal to Cyber Regulations Appellate Tribunal
- Section 58: Procedures and powers of Cyber Appellate Tribunal
- Section 62: Appeal to High Court

THANK YOU ...

Module 6: Information Security Standard compliances

Outline

- SOX
- GLBA
- HIPAA
- ISO
- FISMA
- NERC
- PCI.

Information Security Standard

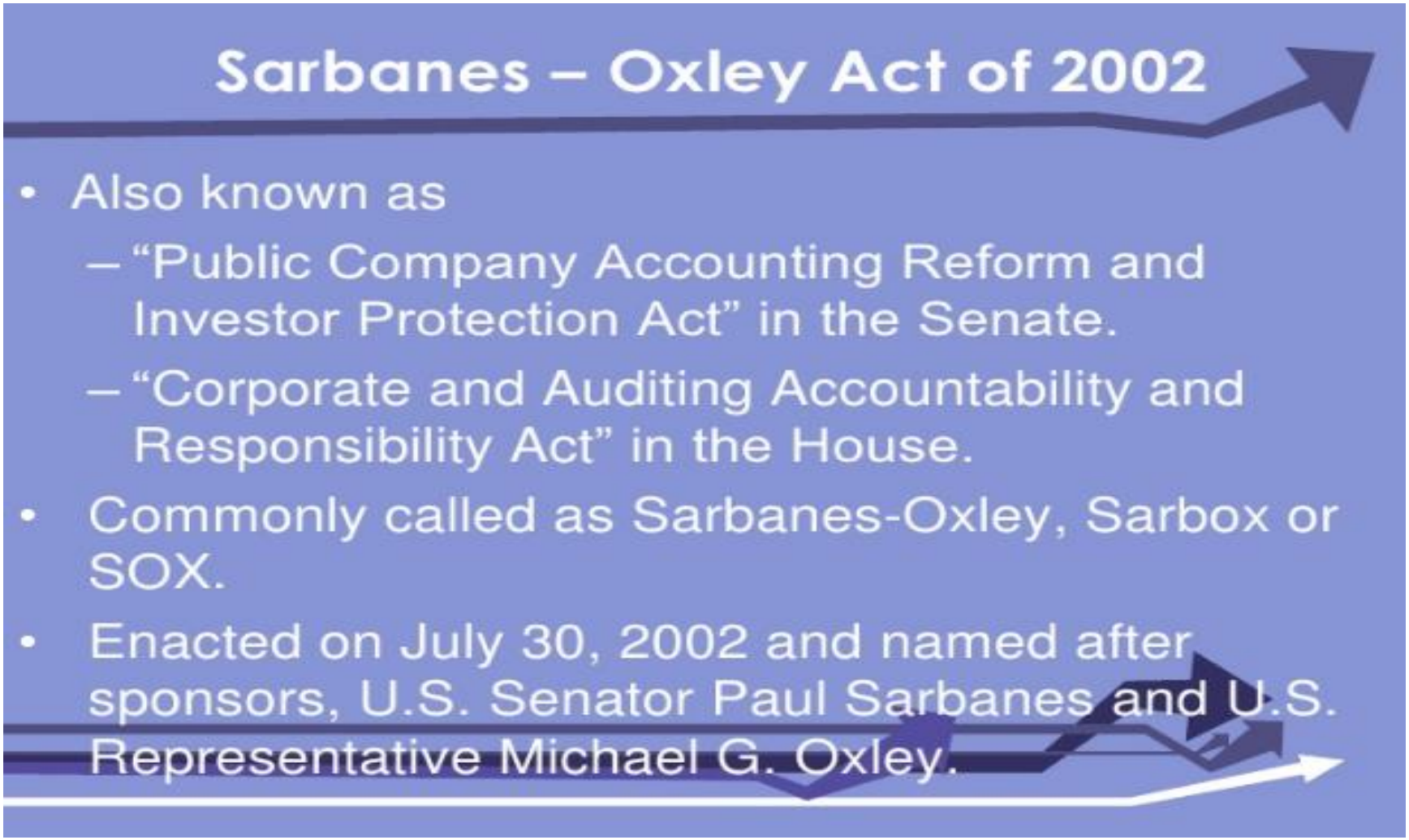
Information Security Standard

- Helps organization to manage their information security requirements

- Recommend adoption of best practices to achieve performance and cost benefits

SOX / SARBOX

SOX / SARBOX / Sarbanes – Oxley Act



SOX/ SARBOX


Paul Sarbanes
Michael Oxley
Then Pres. George W. Bush signing the Sarbanes-Oxley Act of 2002
CORPORATE RESPONSIBILITY

SOX / SARBOX / Sarbanes – Oxley Act

- SOX Section 302
- SOX Section 401
- SOX Section 404
- SOX Section 409
- SOX Section 802
- SOX Section 806
- SOX Section 902
- SOX Section 906

SOX – Key IT requirements

- Written security policy
- Company should baseline its current compliance state
- Timely monitoring and response
- Access to financial data and critical files

GLBA / GLB

GLBA / GLB / Gramm- Leach – Bliley Act

- Financial Services Modernisation Act of 1999

- Section 501 (b) of the Act specifies the objectives of these standards:

  - The Financial Privacy Rule
  - The Safegaurds Rule
  - The pretexting provisions

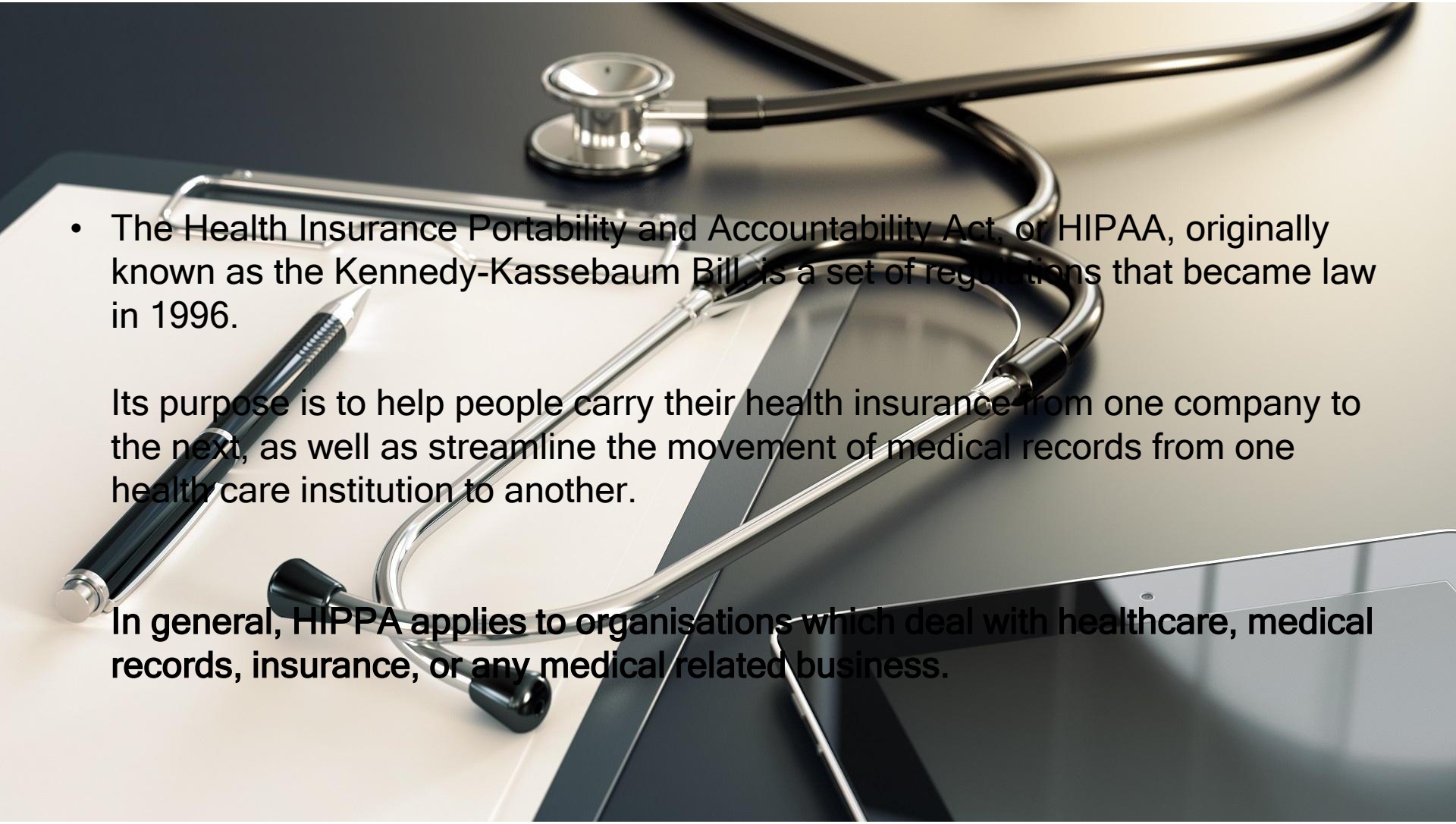
GLBA – Key IT requirements

- Written security policy
- Establish baseline, risk assessment and vulnerability scan
- Monitor and report any access to files, etc
- Notify customer if required
- Designate security program coordinator
- Security awareness and training programs
- Policies for information processing
- Appropriate measures to detect, prevent and respond to attacks
- Procedure for FTC reviews and audits

HIPAA

HIPAA

Health Insurance Portability and Accountability Act of 1996



- The Health Insurance Portability and Accountability Act, or HIPAA, originally known as the Kennedy-Kassebaum Bill, is a set of regulations that became law in 1996.

  Its purpose is to help people carry their health insurance from one company to the next, as well as streamline the movement of medical records from one health care institution to another.

  In general, HIPPA applies to organisations which deal with healthcare, medical records, insurance, or any medical related business.

- The security standards as per HIPAA are divided into 3 broad categories:
  - 1. Administrative Safeguard
  - 2. Physical Safeguard
  - 3. Technical Safeguard

ADMINSTRATIVE SAFEGUARDS

1) **Security Management Process**

a. Risk analysis:.

b. Risk management:

c. Sanction (Penalty) policy:

d. Information system activity review:

2) **Assigned Security Responsibility**

Organizations need to identify the security official who is responsible for the development and implementation of policies and procedures.

3) **Workforce Security**

Organizations need to implement and supervise policies and procedures to ensure that all members of their workforce have access to electronic protected health information strictly based on their roles and authorization levels.

4) **Information Access Management**

Organizations need to implement policies and procedures for authorizing access to electronic protected health information that is consistent with the applicable requirements.

5) **Security Awareness and Training**

- Periodic security updates.
- Guarding against, detecting and reporting malicious software.
- Monitoring log-in attempts and reporting discrepancies.
- Creating, changing, and safeguarding passwords.

6) **Security Incident Procedures**

Organizations need to implement policies and procedures to address security incidents.

7) **Contingency Planning**

- A data backup plan
- A disaster recovery plan
- An emergency mode operation plan
- Periodic testing and revision of contingency plans
- Periodic analysis of applications and data criticality

8) **Evaluation**

Organizations need to perform technical and non-technical evaluations, periodically,

9) **Business Associate Contracts and Other Arrangements**

An organization may permit a business associate to create, receive, maintain, or transmit electronic protected health information on its behalf only if it obtains satisfactory assurances that the business associate will appropriately safeguard the information.

PHYSICAL SAFEGUARDS

1) **FACILITY ACCESS CONTROL:**

- Contingency operations
- Facility security plan
- Access control and validation procedures
- Maintenance records

2) **WORKSTATION USE:**

Organization need to implement policies that specify functions to be performed ,manner in which they are performed ,physical attributes of the surroundings of a workstation that can access electronic health information.

3) **WORKSTATION SECURITY:**

Organisation need to implement physical safeguard for all workstations that access electronic protected health information to restrict access to authorized users.

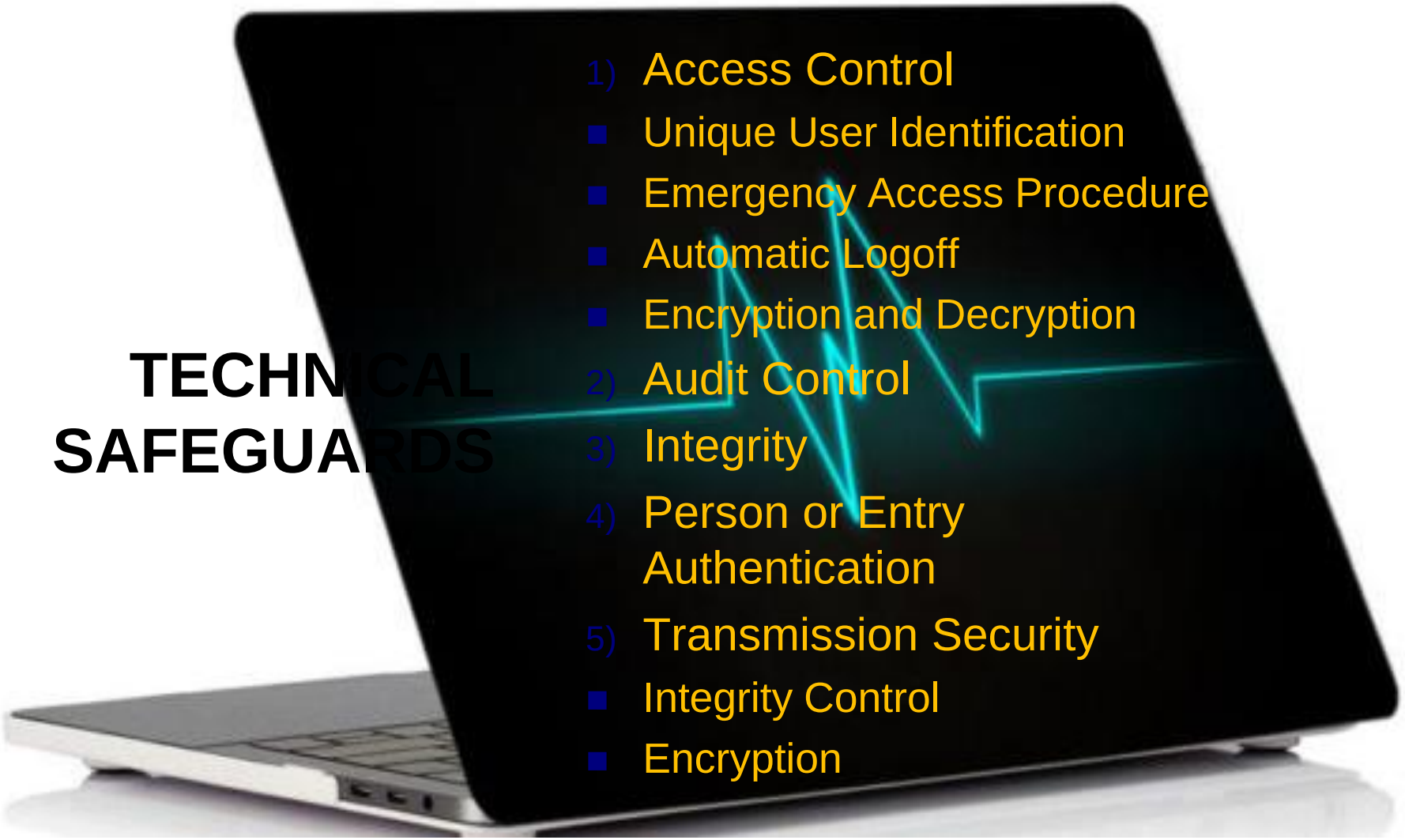
4) **DEVICE AND MEDIA CONTROL:**

Implementation specifications:

- Disposal
- Media reuse
- Accountability
- Data backup and storage.

TECHNICAL SAFEGUARI

TECHNICAL SAFEGUARDS



1) Access Control
   - Unique User Identification
   - Emergency Access Procedure
   - Automatic Logoff
   - Encryption and Decryption
2) Audit Control
3) Integrity
4) Person or Entry Authentication
5) Transmission Security
   - Integrity Control
   - Encryption

KEY IT REQUIREMENTS

THE KEY REQUIREMENTS OF THE HIPAA ACT IS LISTED BELOW

Organisations need to:

1. Conduct an initial risk assessment, periodic review and reassessments.
2. Designate security person.
3. Implement termination policy and procedures3 Have a written security and incident handling policy.
4. Have a backup emergency operations, and disaster recovery plan.
5. Have policies for the use of the Internet, various systems (laptops, servers) and reusable.
6. Storage media (USB drives, CDs/DVDs) along with their reuse and disposal plan.
7. Have audit controls, including unique user identifiers, for authenticating users, recording and auditing user sessions and logout/disconnect inactive sessions.
8. Have a policy to encrypt sensitive data, monitor and audit access and alterations to sensitive data, protect data in transmission with backup.

FISMA

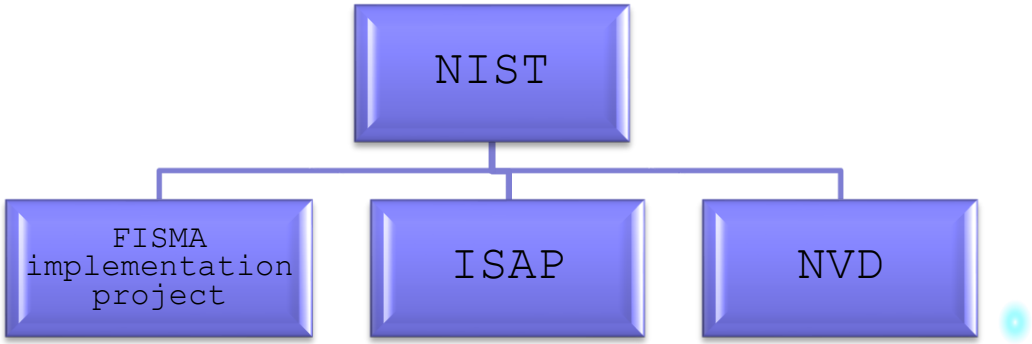
What is FISMA?

- FISMA – Federal Information Security Management Act
- United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats.
- FISMA was signed into law part of the Electronic Government Act of 2002.
- Again rewritten and signed into law by the President Obama in 2014.

What was the purpose of FISMA?

- To ensure the security of data in the federal government.
- According to FISMA, the term information *security* means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality and availability.

- NIST (National Institute of Standards and Technology) has authority to create programs that bolster IT security and risk management practices.
- DHS (Department of Homeland Security) responsible for administering the implementation of programs created by NIST in order to secure federal information system security.



FISMA – KEY IT REQUIREMENTS

1. Identify information and information systems
2. Risk assessment and categorization
3. Meet minimum security requirements
4. Refine controls using Risk assessment
5. Document controls
6. Implement Security controls
7. Authorise the Information
8. Continuous monitoring

NERC

NERC – North American Electric Reliability Corporation

- March 28, 2006
- Oversee and regulate the reliability of North American bulk power systems

- Key terms :
  - Bulk Electric System (BES)
  - Critical Assets
  - Critical Cyber Assets

NERC – North American Electric Reliability Corporation

- Standards are organized on topics as follows :
  - CIP-001
  - CIP-002
  - CIP-003
  - CIP-004
  - CIP-005
  - CIP-006
  - CIP-007
  - CIP-008
  - CIP-009

NERC – North American Electric Reliability Corporation

- NERC applies to companies that generate or provide or transmit energy:
  - FERC
  - SCADA

NERC – Key IT requirements

- Electronic security
- Personal security, training and awareness
- Physical security
- Recovery plans
- Audits and documentation

ISO

INTRODUCTION TO “ISO”

- The **International Organization for Standardization** (**ISO)** is an international standard-setting body composed of representatives from various national standard organizations.
- Founded on 23 February 1947, the organization promotes worldwide proprietary, industrial and commercial standards.
- It is headquartered in **Switzerland** and works in 164 countries.
- It was one of the first organizations granted general consultative status with the United Nations Economic and Social Council.

ISO/IEC 27001:2013

- The ISO/IEC 27000 family of standards helps organizations **keep information assets secure**.
- Using this family of standards will help organizations manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties.
- ISO/IEC 27001 is the best-known standard in the family **providing requirements for an information security management system** (ISMS).
- ISO/IEC 27001:2013 Provides requirements for Establishing, Implementing, Maintaining and Continually Improving an Information Security Management System.

ISO/IEC 27001:2013 Annex A

- 14 control areas comprising 35 Control Objectives and 114 Controls

A.5 Information security policies – controls on how the policies are written and reviewed

A.6 Organization of information security – controls on how the responsibilities are assigned; also includes the controls for mobile devices and tele-networkworking.

A.7 Human resources security – controls prior to employment, during, and after the employment

A.8 Asset management – controls related to inventory of assets and acceptable use, also for information classification and media handling

A.9 Access control – controls for Access control policy, user access management, system and application access control, and user Responsibilities

A.10 Cryptography – controls related to encryption and key management

A.11 Physical and environmental security – controls defining secure areas, entry controls, protection against threats,

ISO/IEC 27001:2013 Annex A

A.12 Operational security – lots of controls related to management of IT production: change management, capacity management, malware, backup, logging, monitoring, installation, vulnerabilities, etc.

A.13 Communications security – controls related to network security, segregation, Network services, transfer of information, messaging, etc.

A.14 System acquisition, development and maintenance – controls defining security requirements and security in development and support processes

A.15 Supplier relationships – controls on what to include in agreements, and how to monitor the suppliers

A.16 Information security incident management – controls for reporting events and weaknesses, defining responsibilities, response procedures, and collection of evidence

A.17 Information security aspects of business continuity management – controls requiring the planning of business continuity, procedures, verification and reviewing, and IT redundancy

A.18 Compliance – controls requiring the identification of

PCI

What is PCI?

The Payment Card Industry (PCI) standard is a set of requirements designed to ensure that **ALL** organizations that store, process, or transmit cardholder data do so in a secure environment.

The PCI Security Standards Council

Evolution of PCI

PCI Security Standards Council was founded in 2006 by the major card brands:

- Visa
- MasterCard
- Amex
- Discover
- JCB

Each card brand has input into the guidance provided by the Council.

Evolution of PCI (cont.)

PCI Security Standard Council is responsible for the oversight of the PCI Standards, which include guidance relative to the following:

PCI DSS

- PA-DSS

What is PCI DSS?

- Payment card industry data security standard
- Set of 12 requirements broken down into 6 categories, as follows:
    1. Build and maintain a secure network
    2. Protect cardholder data
    3. Maintain a vulnerability management program
    4. Implement strong access control measures
    5. Monitor and test networks
    6. Maintain an information security policy

What is PA DSS?

- PAYMENT APPLICATION DATA SECURITY STANDARD
- requirements as follows:

1. do not retain full data
2. Protect stored cardholder data
3. Secure authentication feature
4. Payment activity
5. Secure payment app
6. Protect wireless transmission
7. Test payment app

What is PA DSS?

8. Secure network implementation
9. Data on server
10. Secure remote access
11. Encrypt secure information
12. Secure all administrative process
13. Implementation guide
14. Assign responsibilities

THANK YOU ...