Legal, Regulations, Compliance and Investigations

CISSP®

Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

Computer Crime

- Crimes that target computer networks or devices directly
  - Malware (malicious code).
  - Denial-of-service attacks.
  - Computer viruses.
- Crimes facilitated by computer networks or devices, the primary target of which is independent of the computer network or device.
  - Cyber stalking.
  - Fraud and identity theft.
  - Phishing scams.
  - Information warfare.

Specific Computer Crimes

- Spam.
- Fraud.
- Obscene or offensive content.
- Harassment.
- Drug trafficking.

Initiatives to fight Cybercrime

- UK
  - Computer Misuse Act 1990
    - Provision for securing computer material against unauthorised access or modification.
      - Unauthorised access to computer materials.
      - Unauthorised access with intent to commit or facilitate the commission of further offences.
      - Unauthorised modification of computer material.
- United States
  - Computer Fraud and Abuse Act (CFAA).
  - Electronic Signatures in Global and National Commerce Act.
  - Uniform Electronic Transactions Act - adopted by 46 states.
  - Digital Signature And Electronic Authentication Law.
  - Government Paperwork Elimination Act (GPEA).
  - The Uniform Commercial Code (UCC).
- Europe
  - eSignatures
    - Directive 1999/93/EC of the European Parliament and of the Council
    - Community framework for electronic signatures implemented in all member states by 19 Jul 01
    - Repealed 1/6/2016, replaced by EU regulation for electronic ID & e-signatures (eIDAS)
  - Attacks against Information Systems
    - Council Decision 2005/222/JHA was designed to improve cooperation between judicial and other competent authorities (police, etc..).
    - Replaced by Directive 2013/40/EU on attacks against information systems in August 2013.

Initiatives to fight Cybercrime

- **Convention on Cybercrime**
  - The Council of Europe (CoE) ETS No. 185 Convention on Cybercrime is the only binding international instrument on this issue.
  - Guideline for any country developing comprehensive national legislation against Cybercrime and coop between signatories.
  - 1 March 2006 the Additional Protocol to the Convention on Cybercrime came into force. (USA did not sign).
  - Additional protocol criminalises the dissemination of racist and xenophobic material through computer systems, as well as of racist and xenophobic-motivated threats and insults.
  - Forty-three nations have signed the treaty. The Convention entered into force in the United States in 2007.
    - Non Europe - Australia, Canada, Dominican Republic, Japan, Mauritius, Panama, Sri Lanka, and the United States.

Intellectual Property (IP)

- **Patent**
  - This term refers to a right granted to anyone by the state (Government patent office) who invents or discovers any new and useful process, machine, article of manufacture, or composition of matter, or any new and useful improvement thereof.
- **Trademark**

  - A trademark is a distinctive sign or indicator used to identify that the products or services originate from a unique source.
  - A trademark is designated by the following symbols:
    - ™ Unregistered trade mark.
    - SM Unregistered service mark.
    - ® Registered trademark.

Intellectual Property (IP)

- **Copyright**
  - Copyright is a form of intellectual property that gives the author of an original work exclusive right for a certain time period.
    - Original literary, dramatic, musical or artistic works.
    - Sound recordings and films.
    - Broadcasts and TV programmes.
    - The typographical arrangement of published editions.
    - Computer programmes.
    - Original databases.
  - It typically applies for 50 – 70 years depending on the form of work.

Copyleft

- Copyleft is a play on the word copyright to describe the practice of using copyright law to remove restrictions on distributing copies and modified versions of a work for others and requiring that the same freedoms be preserved in modified versions.
- Common practice for using copyleft is to codify the copying terms for a work with a license.
  - the freedom to use the work.
  - the freedom to study the work.
  - the freedom to copy and share the work with others.
  - the freedom to modify the work, and the freedom to distribute modified and therefore derivative works.
- The GNU General Public License, originally written by Richard Stallman, was the first copyleft license to see extensive use, and continues to dominate the licensing of copylefted software.

Trade Secret

- A trade secret is information that:
  - Is not generally known to the public
  - Confers some sort of economic benefit on its holder
  - Is the subject of reasonable efforts to maintain its secret?
- A company can protect its confidential information through non-competitive and non-disclosure agreements (NDA) with its employees.

International Trade

- International trade is exchange of capital, goods, and services across international borders or territories. It refers to exports of goods and services by a firm to a foreign-based buyer or importer.
  - World Trade Organisation (**WTO**) at the global level.
  - European Union between member states.
  - MERcado COmún del SUR (Spanish) Southern Common Market (**MERCOSUR**) in South America.
  - North American Free Trade Agreement (**NAFTA**) between the United States, Canada and Mexico.

Encryption Export Control

- Origin of the issue
  - Encryption export controls became a matter of public concern with the introduction of the PC.
  - Phil Zimmermann's PGP cryptosystem and its distribution on the Internet in 1991.
  - Electronic commerce in the 1990s created additional pressure for reduced restrictions.
  - Netscape's SSL technology was widely adopted as a method for protecting credit card transactions using public key cryptography.
  - SSL-encrypted messages used the RC4 cipher, and used 128-bit keys.
  - US government export regulations would not permit crypto systems using 128-bit keys to be exported.
  - Netscape SSL:
    - US Edition (128 bit).
    - International edition (40 bit).

Encryption Export Control

- Change
  - 1996 US President Bill Clinton signing the Executive order 13026 transferring the commercial encryption from the Munition List to the Commerce Control List.
  - Non-military cryptography exports from the USA are controlled by the Department of Commerce's Bureau of Industry and Security. Some restrictions still exist, even for mass market products, particularly with regard to export to "rogue states" and terrorist organisations.
  - Militarised encryption equipment, TEMPEST-approved electronics, custom cryptographic software, and even cryptographic consulting services still require an export license.

Encryption Export Control

- **Wassenaar Arrangement**
  - Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies is a Multilateral Export Control Regime (**MECR**) with 40 participating states.
  - It is the successor to the Cold war-era Coordinating Committee for Multilateral Export Controls (**COCOM**), and was established on May 12, 1996, in the Dutch town of Wassenaar, near The Hague.
  - It is considerably less strict than COCOM, focusing primarily on the transparency of national export control regimes and not granting veto power to individual members over organisational decisions.
  - A Secretariat for administrating the agreement is located in Vienna, Austria.

Liability and Negligence

- **Legal liability**
  - Legal bound obligation to pay debts.
  - A person is said to be legally liable when they are financially and legally responsible for something.
  - Bankruptcy.

- **Negligence**
  - A type of delectation or civil wrong.
  - The difference between Actions where due diligence is expected and due care as defined in a policy.
  - The gap between the policy and best practice or regulation.
  - Civil litigation.

Privacy

- **Privacy**
  - The ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively.
- **Data privacy**
  - The evolving relationship between technology and the legal right to, or public expectation of privacy in the collection and sharing of data about one's self.
- Personal information often come under privacy concerns:
  - Financial privacy.
  - Internet privacy.
  - Medical privacy.
  - Sexual privacy.
  - Political privacy.

Privacy

- **US Health Insurance Portability & Accountability Act (HIPPA)**
  - HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs it requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.
- **Canadian Personal Information Protection & Electronic Documents Act (PIPEDA)**
  - PIPEDA requires private-sector organisations to collect, use or disclose your personal information by fair and lawful means, with your consent, and only for purposes that are stated and reasonable.
  - Also obliged to protect your personal information through appropriate security measures, and to destroy it when it's no longer needed for the original purpose.

Privacy

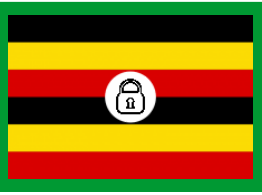
- **EU Directive 95/46/EC** (Data Protection)
  - Protection of individuals with regard to the processing of personal data and on the free movement of such data.
  - Regulates the processing of personal data within the Union member states.
  - Component of EU privacy and human rights law and was implemented in 1995 by the European Commission.

Data Protection

- General Data Protection Regulation (GDPR)
  - Replaces Data Protection Directive 95/46/EC on 25/5/2018.
  - Control to citizens of their personal data
  - Simplify the regulatory environment for business
  - Data breach notification obligation within 72 hours
    - Sanctions
      - €20,000,000 (84,000,000,000 UGx)
      - 4% of the annual worldwide turnover.
  - Right to erasure (“Right to be forgotten”)
  - Data portability
  - Data protection by ‘Design’ and by ‘Default’.

Ref: *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016*

Data Protection



- Data Protection and Privacy Bill, 2016
  - Principles of Data Protection
  - Data Collection and Processing
    - Consent, protection of privacy
  - Security of Data - breach notification to NITA-U
  - Rights of subjects
    - Access, prevent processing, etc..
  - Sanctions
    - Individuals: 4,800,000 Ugx and/or 10 years prison.
    - Corporations: All individuals involved.

Ref: *Uganda Data Protection and Privacy bill 2016, First Reading, 20 Apr, 2016*

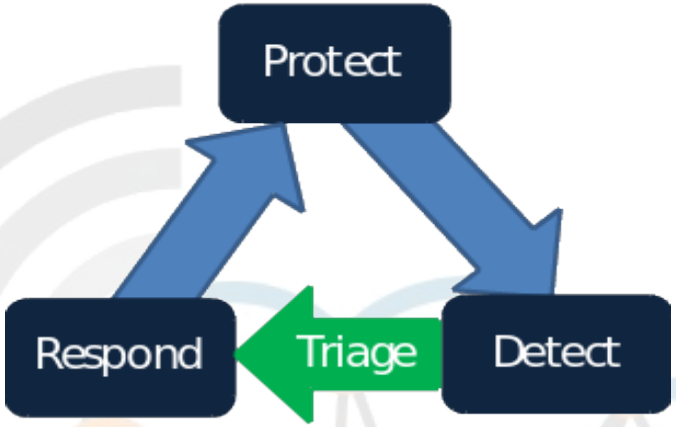
Data protection, recommendations

- Robust **Data Breach Incident Management Policy**
- **Pseudonymisation** of personal data
  - Separation of data from direct identifiers so that linkage to an identity is not possible without additional information that is held separately
- **Encryption** of data
- **Assess** applications and critical infrastructure for security vulnerabilities and the effectiveness of security controls
  - Vulnerability Testing
  - Penetration Testing
  - Control Testing.

Privacy at work

- Increasing pressure to monitor employees electronically, and workers should assume they are being watched.
- Companies generally conduct some form of active monitoring of their employees, particularly E-mail monitoring.
- Employees generally have a right to privacy based on a '*reasonable expectation of privacy*' but a written policy notifying employees of monitoring lifts somewhat the expectation of privacy.
- If an employee is led to expect something is private, such as e-mail communications, then that privacy cannot be violated.
- If the company informs its employees of monitoring, then the employee can no longer claim an expectation of privacy.
- Managing the balancing act between privacy and security is for firms to make clear to their employees that their privacy at work is limited.
- E-mail is quite often used as a tool of harassment and employers have a duty to be sure harassment isn't being propagated.
- For the company to exercise its responsibility it needs to monitor or at least record the e-mail traffic.

Incident Management



- **Proactive preparation**
  - The preparation of policies to deal with possible events and the implementation of a continuous cycle of auditing and improvement of these policies.
- **Reaction**
  - Measures carried out on the detection of an incident. How the incident was detected, what triage classification and prioritisation was carried out and how the response was conducted.

Incident Management

- Good source of information are the:
  - NIST SP 800-61 Computer Security Incident Handling Guide
- Software Engineering Institute (SEI)
  - Handbook for Computer Security Incident Response Teams (CSIRTs)

NIST

Software Engineering Institute

Collection of Digital Evidence

- Evidence is subject to strict rules regarding its admissibility in courts. To be presented, recorded in the court record and considered in the verdict, evidence must be:
- **Relevant**
  - It must pertain to the actual case.
- **Material**
  - It must prove or disprove facts that impact the question before the court.
- **Competent**
  - It must be proven to actually be what it purports to be.

Collection of Digital Evidence

- "**DO NOT HARM**"
  - Do not start open the log files, shutting down the system, etc. Do as little as possible beyond disconnecting the system from the network and protecting it until it can be handed over to the police or other law enforcement.
- **Don't turn off** the system as data in volatile memory (RAM) will be lost
- **Disconnect from the network** as this prevents a hacker from covering their tracks by deleting evidence like log files
- **Don't use the system** for any reason, like running programs as you may unwittingly overwrite data in memory
- **Don't open files** to examine them as you will modify the access and modify time record on the file.
- **Document everything** you do.

Preservation of Digital Evidence

- **Preserve digital evidence in its original state**
  - Copy it from one machine to another via a private network connection.
  - The source computers memory should be transferred to the target computer first.
  - The contents of the source computer's hard disk should be copied to the target computer as a bit level image not file by file to create an exact copy of the source disk data including empty space (which may include deleted residual data).
  - A number of specialist software programs exist for this purpose.

Preservation of Digital Evidence

- A **forensic duplicate** consists of every bit of the raw bitstream stored in an identical format (e.g. using an identical disk).
- On the other hand, a qualified forensic duplicate is a copy where every bit of information is still stored, but perhaps in a different form, such as an ISO image.
- Both are permissible as evidence, but the "best evidence" should be used, e.g. the original disk.

Evidence Chain of Custody

- Chain of Custody is the chronological documentation, showing the seizure, custody, control, transfer, analysis, and disposition of evidence, physical or electronic.
  - Who.
  - What.
  - When.
  - Where.
  - How.

Process of Investigation

- Identify:
  - Suspects.
  - Systems.
  - Witnesses.
  - Investigative team.
  - Search warrants
- For filesystems, analyse the ownership and the modification records.
- What were the Means, Opportunity and Motives (**MOM**) of personnel can assist in narrowing down suspects to a crime.
- Are there any Modus Operandi (**MO**), methods, choice of software or applications that may point to a particular set of habits, traits, or practices that can be used to identify a suspect.

Interviewing Suspects

- **Plan** the interview.
- Interview or interrogation techniques.
- **Interview**
  - Conducted in a cordial atmosphere where a suspect or witness is more comfortable physically and psychologically.
- **Interrogation**
  - Questioning in an uncomfortable atmosphere under psychological pressure.

Hearsay

- Information gathered by one person from another concerning some event, condition, or thing of which the first person had no direct experience.
- "**hearsay evidence**" in court is generally not allowed.
- **Business entry rule** (US) which is an exception to the hearsay rule.
  - Writings or records of acts, events, conditions, opinions, or diagnosis, made at or near the time by, or from information transmitted by, a person with knowledge are admissible if kept in the regular course of business.
  - Employees are under a duty to be accurate in observing, reporting, and recording business facts.
  - The exception allows the record to substitute for the in-court testimony of the employees, but it can only substitute for what the employee could testify about.

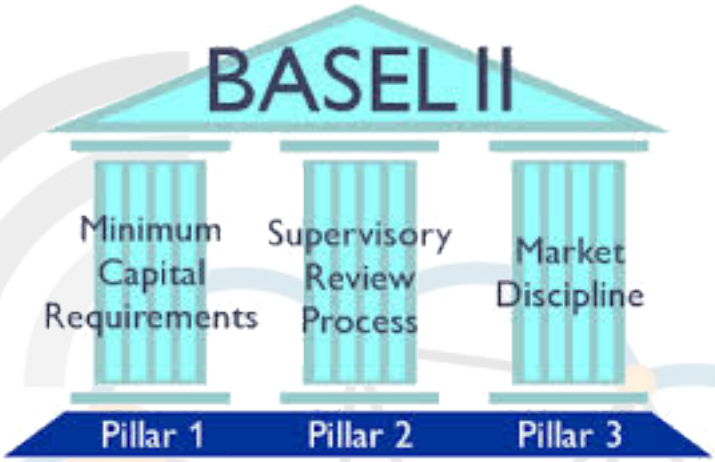
Compliance and ethics

- Regulatory Compliance
  - All countries there have been periods of business and government excesses and subsequent legal, public and political reaction.
  - All countries have imposed regulation of compliance to prevent and punish companies who participate in corporate malpractice.
- EU DIRECTIVE **2006/43/EC**
  - Statutory audits of annual accounts and consolidated accounts.
  - USA equivalent is the US Sarbanes–Oxley Act.

Compliance and ethics

- **US Foreign Corrupt Practices Act (FCPA)**
  - Anti-bribery provision makes it unlawful for a United States citizen, and certain foreign issuers of securities, to make a corrupt payment to a foreign official.
  - Companies to have an adequate systems of internal accounting controls.
- **US Sarbanes–Oxley Act (SOX)**
  - The act is the US Public Company Accounting Reform and Investor Protection Act.
  - Major corporate and accounting scandals
    - Enron
- **US Gramm-Leach-Bliley Act (GLBA)**
  - US Financial Services Modernisation Act to allow commercial banks, investment banks, securities firms and insurance companies to consolidate.
  - Protection of the privacy of consumer information held by these organisations.

Compliance and ethics

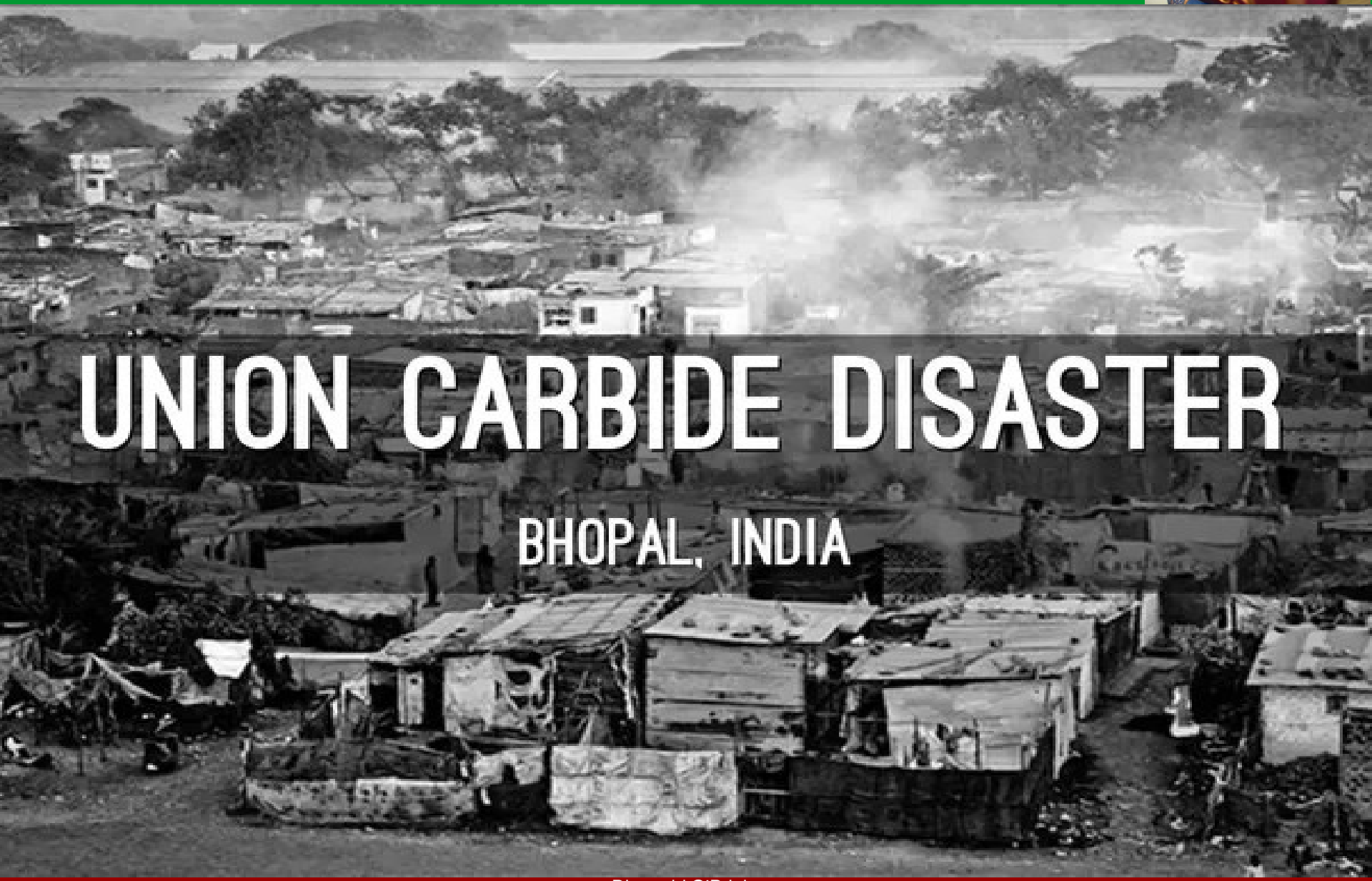


- **Basel II**
  - Series of recommendations on banking laws and regulations issued by the Basel Committee on Banking Supervision.
  - International standard that banking regulators can use when creating regulations about how much capital banks need to guard against financial and operational risk.
  - The greater risk to which the bank is exposed, the greater capital the bank needs to hold to safeguard its solvency and stability.

Compliance auditing

- Evaluation of an organisation, its systems and process to ascertain the validity and reliability of information and assessment of internal controls against compliance to the rules of business.
- The audit is carried out by an approved third party auditor who will compare the stated policies with the actual controls in place.
- Continuous auditing is an automated method of auditing by use of software to perform the audit on a continuous basis.

Business Ethics - Bhopal disaster



Business Ethics - Bhopal disaster

- 2 December 1984 – 3 December 1984
- Bhopal, Madhya Pradesh, India
- Methyl Isocyanate leak from Union Carbide India Limited storage tank
- Deaths: Officially 3,787; over 16,000 claimed
- Non-fatal injuries: 558,125

- "***Hold paramount the safety, health and welfare of the public.***"
  - Poor quality and lack of many instruments, safety equipment and reduced operation of critical systems.
    - Flare Tower, VGS, Water Sprays, MIC refrigerator, Tank 610.
  - The local community was never given any information about MIC and other chemicals.

Business Ethics – Enron Scandal

- October 2001 – Enron financial scandal
  - Hid billions of dollars in debt from failed deals and projects
    - accounting loopholes
    - special purpose entities
    - poor financial reporting.
  - Pressured Arthur Andersen to ignore the issues.
- Eventually led to the bankruptcy of the Enron Corporation, an American energy company
- Arthur Andersen was charged with and found guilty of obstruction of justice for shredding documents and files
- Although only a small number of their employees were involved with the scandal, the firm was effectively put out of business

Business Ethics

- Applied ethics that examines ethical principles and moral or ethical problems that arise in a business environment.
- The range and quantity of business ethical issues reflects the degree to which business is perceived to be at odds with non-economic social values.
- Companies
  - Internal policies on the ethical conduct of employees.
  - Company's expectations of workers.
  - Offer guidance on handling some of the more common ethical problems.
  - Greater ethical awareness, consistency in application, and the avoidance of ethical disasters.

Thank you