Table of Contents

Contents

Appendix A – Laws and Regulations review 2
Potential threats and their impact on the business 2
Adhering to Compliance Laws and Regulations 3
Gramm – Leach - Bliley 4
Dodd-Frank 5
HIPAA – Health Information Protection and Accounting Act 6
History of HIPAA and the Patient Protection and Affordability Act (Obamacare) 7
HIPAA Audience and Compliance Requirements 8
Who is affected by the new HIPAA Laws 9
HIPAA Contingency Planning and Security Guidelines (newly updated) 10
Penalties for non-compliance to new HIPAA rules 11
HIPAA Five Step Circle of Compliance 12
Healthcare Industry Workflow Management System Goals 13
Sarbanes-Oxley Act (SOX) 14
EPA and Superfund 15
Patriot Act 16
Basel II overview 17
ISO 27000 Information Security Management System guidelines 18
Strategies for Eliminating Gaps and Exceptions 19
Compliance Reporting Technique 20
Creating Compliance Reports and a Letter of Attestation 21

Appendix A – Laws and Regulations review

Potential threats and their impact on the business

Malicious Activity:
- Fraud, Theft, and Blackmail;
- Sabotage, Workplace Violence; and
- Terrorism.

Natural Disasters:
- Fire;
- Floods and other Water Damage;
- Avian, Swine, or other Epidemic / Pandemic occurrence;
- Severe Weather;
- Air Contaminants; and
- Hazardous Chemical Spills.

Technical Disasters:
- Communications;
- Power Failures;
- Data Failure;
- Backup and Storage System Failure;
- Equipment and Software Failure; and
- Transportation System Failure.

External Threats:
- Suppliers Down;
- Business Partner Down; and
- Neighboring Business Down.

Facilities:
- HVAC – Heating, Ventilation, and Air Conditioning;
- Emergency Power / Uninterrupted Power; and
- Recovery Site unavailable.

Recovery Management plans for loss of a location, service, vendor, or personnel due to a disaster event, while safeguarding the company reputation.

Disasters can render unusable / un-accessible specific resources (like a building) due to: flooding; water damage; inclement weather; transportation outage; power outage; or many other situations. Rather than write specific recovery plans for each event that could render a building un-accessible, a single plan for loss of a building can be written and incorporated into the crisis management plan associated with the specific disaster event causing the need to evacuate a building.

Disasters result from problems and problems are the result of a deviation from standards. By making sure your standards and procedures are correct and maintained you will reduce disaster events. These procedures should be included in the SDLC, Maintenance, Support, and Change Control process.

Working with the community will allow recovery managers to become good neighbors, build relationships with other recovery managers, and keep aware of situations outside of their control.

Working with governmental agencies like OSHA, FEMA , OEM, and Homeland Security will help recovery managers to stay current with compliance needs and recovery planning trends, thereby better safeguarding the workplace and employees.

Adhering to Compliance Laws and Regulations

Adhering to Compliance Laws

- **Gramm Leach Bliley** – Safeguard Act (was Bank Holding Act);
- **Dodd – Frank** – Wall Street Reform and Consumer Protection Act;
- **HIPAA** – Healthcare regulations (including ePHI, HITECH, and Final Ombudsman Rule);
- **Sarbanes – Oxley Act** (sections 302, 404, and 409) on financial assessment and reporting by authorized "Signing Officer";
- **EPA and Superfund** (how it applies to Dumping and Asset Management Disposal);
- **Supply Chain Management "**Laws and Guidelines" included in ***ISO 24762*** (SSAE 16 for Domestic compliance and SSAE 3402 for International Compliance, and NIST 800-34);
- **Supply Chain Management "**Technical Guidelines" described in ***ISO 27031***;
- **Patriots Act** (Know Your Customer, Money Laundering, etc.);
- **Workplace Safety and Violence Prevention** via OSHA, OEM, DHS, and governmental regulations (State Workplace Guidelines and Building Requirements);
- **Income Tax and Financial Information protection** via ***Office of the Comptroller of the Currency*** (OCC) regulations (***Foreign Corrupt Practices Act***, **OCC-177** Contingency Recovery Plan, **OCC-187** Identifying Financial Records, **OCC-229** Access Controls, and **OCC-226** End User Computing).

Gramm – Leach - Bliley

Gramm-Leach-Bliley

- **Covers Financial Organizations (as defined in the Bank Holding Act) that possess, process, or transmit private customer information.**
- **Its purpose is to protect Customer Information from unauthorized disclosure or use.**
- **An Information Security Program must be in place to comply and the following operating mechanisms must be established:**
  - **Responsible employee as Security Officer.**
  - **Risk Assessment to uncover and correct exposures.**
  - **Information Safeguards and Controls must be established.**
  - **Oversight of "Service Providers and Vendors" to guaranty compliance.**
  - **Testing and Monitoring in an on-going fashion.**
  - **Evaluation and Reporting to management.**
- **Compliance date of May, 2003. Law provides for fines and imprisonment of up to 5 years for intentional violations.**

Dodd-Frank

Dodd–Frank Wall Street Reform and Consumer Protection Act (Overview)

1, The consolidation of regulatory agencies, elimination of the national thrift charter, and new oversight council to evaluate systemic risk;

2. Comprehensive regulation of financial markets, including increased transparency of derivatives (bringing them onto exchanges);

3. Consumer protection reforms including a new consumer protection agency and uniform standards for "plain vanilla" products as well as strengthened investor protection;

4. Tools for financial crises, including a "resolution regime" complementing the existing Federal Deposit Insurance Corporation (FDIC) authority to allow for orderly winding down of bankrupt firms, and including a proposal that the Federal Reserve (the "Fed") receive authorization from the Treasury for extensions of credit in "unusual or exigent circumstances";

5. Various measures aimed at increasing international standards and cooperation including proposals related to improved accounting and tightened regulation of credit rating agencies.

Provisions:

1. Title I - Financial Stability
2. Title II – Orderly Liquidation Authority
3. Title III – Transfer of Powers to the Comptroller, the FDIC, and the Fed
4. Title IV – Regulation of Advisers to Hedge Funds and Others
5. Title V – Insurance
6. Title VI – Improvements to Regulation
7. Title VII – Wall Street Transparency and Accountability
8. Title VIII – Payment, Clearing and Settlement Supervision
9. Title IX – Investor Protections and Improvements to the Regulation of Securities
10. Title X – Bureau of Consumer Financial Protection
11. Title XI – Federal Reserve System Provisions
    a. Governance and oversight
    b. Standards, Plans & reports, and off-balance-sheet activities
12. Title XII – Improving Access to Mainstream Financial Institutions
13. Title XIII – Pay It Back Act
14. Title XIV – Mortgage Reform and Anti-Predatory Lending Act
    a. Property Appraisal Requirements
15. Title XV – Miscellaneous Provisions.
    a. Restriction on U.S. Approval of Loans issued by International Monetary Fund
    b. Disclosures on Conflict Materials in or Near the Democratic Republic of the Congo
    c. Reporting on Mine Safety
    d. Reporting on Payments by Oil, Gas and Minerals in Acquisition of Licenses
    e. Study on Effectiveness of Inspectors General
    f. Study on Core Deposits and Brokered Deposits
16. Title XVI – Section 1256 Contracts

HIPAA – Health Information Protection and Accounting Act

HIPAA

- **Covers organizations that possess, transmit, or process electronic protected health information (EPHI).**
- **Responsible for protecting EPHI data from unauthorized disclosure or use.**
- **Required Security Safeguards include:**
  - **Risk Assessment to uncover and resolve exposures.**
  - **Policies and Procedures to control access and track usage.**
  - **Physical and IT Security Measures.**
  - **Contingency Plan and Disaster Recovery Plan.**
  - **Appointment of Security Officer and Business Continuity Officer.**
  - **Training and communications to improve awareness.**
  - **Periodic Audits and maintenance of Audit Trail.**
  - **Agreement with "Business Associates" to comply to requirements.**
  - **On-going Testing and Evaluation of plan and deliverables.**
- **Comply by April 2005, with fines to $250,000 and imprisonment for up to 10 years.**

History of HIPAA and the Patient Protection and Affordability Act (Obamacare)

History and purpose of HIPAA rules and regulations, from original to current updates.

- **1996** - Initially **HIPAA** was introduced to improve efficiency and effectiveness of the U.S. Healthcare System through guidelines and regulatory requirements.
- **2/2009** – (**HITECH**) Health Information Technology for Economic and Clinical Health Act was introduced as part of the **American Recovery and Reinvestment Act** covering health records from paper based through all types of current and future electronic health records.
- **1/25/2013** – The **Final Omnibus Rule** was published by the **Federal Register** to include **more stringent privacy and security protection for patients** **(to be en-acted 9/23/13)**.
  - Rule also increased **sanctions and penalties** for failure to comply, including the right of States Attorneys General to bring lawsuits on behalf of private individuals for breach of the Privacy Rule.
  - The Security Rule expands data protection to include electronic media and electronic Personal Health Information (**ePHI**) - **covering paper, video, OCR, Social Media, and electronic media**.
  - Although HITECH has been enforceable since **2/2010** many organizations have failed to take action to fully comply, thereby risking **penalties, financial loss, patient services, and reputational loss** that could damage the ability to continue serving the public's medical needs.
  - Included in **Patient Protection and Affordable Care Act** (Obama Care) to reduce costs and improve service.
- **HIPAA** was developed to improve the education of hospital and medical record keepers on the rules and regulations that must be followed to safeguard patients. The **Final Omnibus Rule** and **Patient Protection and Affordable Care Act** provide a more detailed explanation of these safeguards and how best to protect the rights and privacy of patients.

HIPAA Audience and Compliance Requirements

Audience and Compliance Requirements

Healthcare Industry	• Hospitals; Clinics; Doctors Offices; and, • Business Associates and Sub-Contractors.
Patient Security & Safety	• HIPAA; HITECH; ePHI; and Final Omnibus Rule. • "Meaningful Use" reimbursement for electronic data ($40-60K)
New Patient Freedoms	• Ability to have records transferred by request of patient or their authorized representative (Record Sharing).
Workplace Protection	• Responsible for protecting employees, patients, and visitors; • OSHA, DHS, OEM, and NFPA 1600; • Workplace Violence Prevention; • Workplace Physical Security and Evidence Capturing; and, • Ability to evacuate patients in Emergency Mode.
Penalties and Financial Losses	• Criminal and Civil penalties; fines up to $1.5 million per occurrence taking effect 9/23/2013.
Training and Awareness	• Staff must be aware of requirements and trained on how to respond to a wide-range of disaster events.
Risk Management	• Identification of Risks and potential Disaster Event obstacles.
Response Identification and Planning	• Mitigate Gaps and Exceptions; Mediate obstacles blocking the ability to respond to Disaster events; insure the ability to respond to encountered incidents; have the ability to provide a safeguarded environment capable of providing enhanced protections and efficiency while achieving compliance. Integrate within the everyday functions and environment.

Who is affected by the new HIPAA Laws

Who is effected by these changes?

Business Associates and Contractors including:

- **Physical (Guards, CCTV, Card Keys, etc.) and Data Security Service Providers;**
- **IT Equipment, Software, Consulting, and Support Vendors;**
- **Lawyers, Accountants, and Auditors;**
- **Leasing firms and other financial providers;**
- **Telephone and Communications Vendors;**
- **Shredding Vendors, Waste Disposal, and Transportation;**
- **Primary and Secondary Data Centers;**
- **Cloud Computing and Virtualization Service Providers;**
- **Answering Services for Medical Offices;**
- **Medical Billing Services;**
- **Medical Transcriptions Services;**
- **Medical Collection Agencies; and,**
- **Cleaning, Disposal, and internal Service staff.**

The best protection is to perform a Risk Analysis to determine regulatory gaps and exceptions that must be mitigated, along with impeding obstacles that must be mediated. Then implement controls and procedures to create a safeguarded and compliant environment.

HIPAA Contingency Planning and Security Guidelines (newly updated)

HIPAA Contingency Planning and Security Guidelines (newly updated)

Administrative Safeguards include:

- **Security Management Process** (for People, Physical Environments and Data);
- **Assigned Security Responsibility** (Management through all levels of Personnel);
- **Workforce Security** (Procedures governing personnel Screening through Termination);
- **Information Access Management** (Data Sensitivity, Access Controls, Backup / Recovery, etc.)
- **Security Awareness and Training;**
- **Security Incident Procedures** (from identification through "Root Cause" analysis, resolution; Logging, Tracking, Reporting, and Repository Maintenance);
- **Contingency Plan** (Disaster, Business, Emergency, and Crisis Management Responses);
- **Evaluation** (Risk Analysis and Periodic Reviews, with Attestation by Executive Management); and,
- **Business Associate Contact and Other Arrangements** (from definition to accreditation).

Physical Safeguards include:

- **Facility Access Controls (Physical Security to produce a safe workplace);**
- **Workstation Use;**
- **Workstation Security; and,**
- **Device and Media Controls.**

Technical Safeguards include:

- **Access Controls (Data Security and elimination of Data Corruption);**
- **Audit Controls;**
- **Integrity;**
- **Person and Entity Authentications (User Entitlements); and,**
- **Transmission Security (Local and Remote / Encryption).**

Penalties for non-compliance to new HIPAA rules

Penalties for non-Compliance

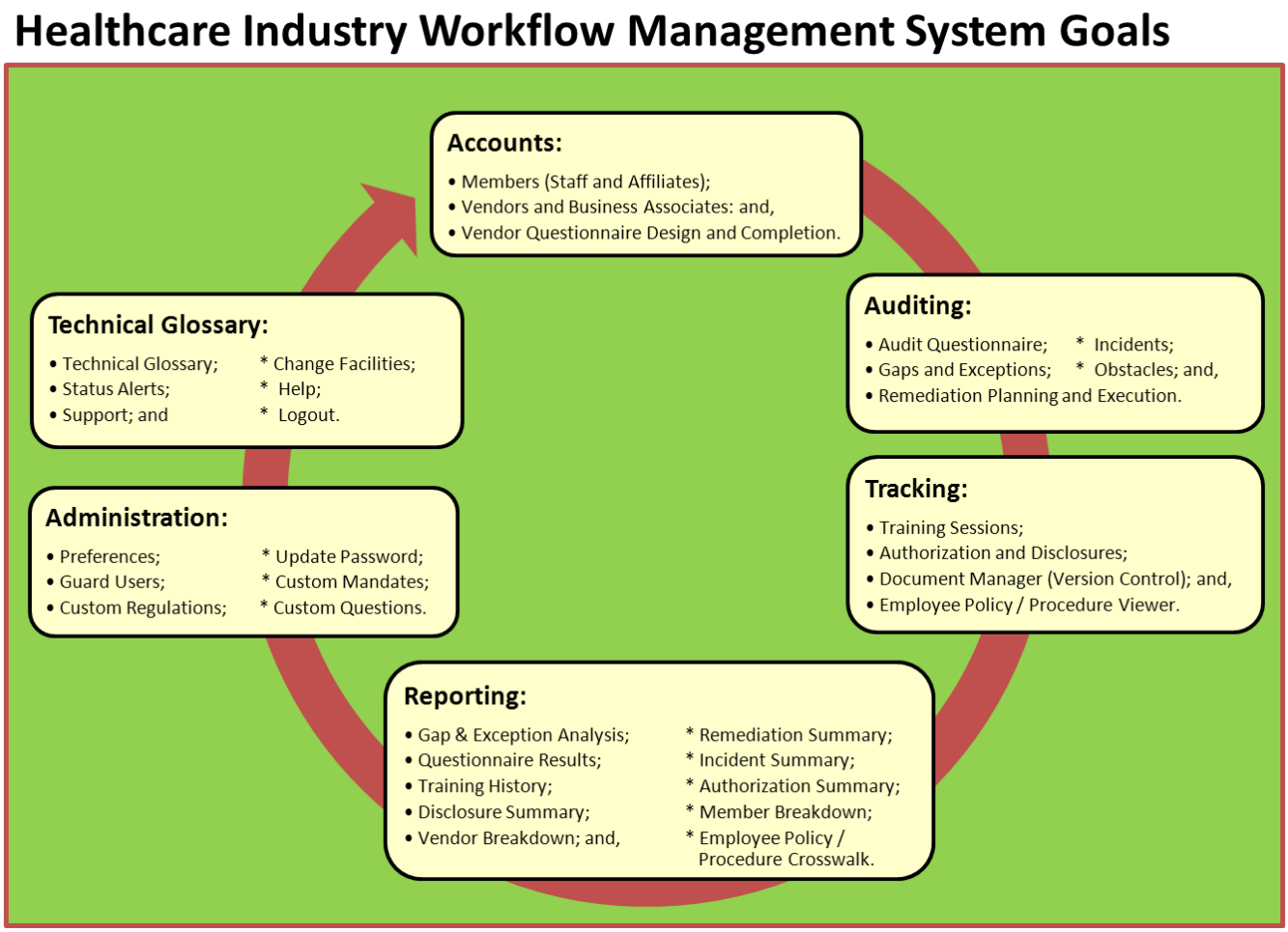
CATEGORIES OF VIOLATIONS AND RESPECTIVE PENALTY AMOUNTS AVAILABLE

Violation Category Section 1176 (a) (1):	Each Violation:	All such Violations of an identical provision in a calendar year:
A. Did Not Know	$100 to Max of $5,000	$1,500,000
B. Reasonable Cause	$1,000 to Max of $50,000	$1,500,000
C. 1. – Willful Neglect – Corrected	$10,000 to Max of $50,000	$1,500,000
C. 2. – Willful Neglect – Not Corrected	$50,000	$1,500,000

As you can see, penalties and loss of reputation can grow rapidly through repeated violations

HIPAA Five Step Circle of Compliance

Healthcare Industry Workflow Management System Goals



Sarbanes-Oxley Act (SOX)

Sarbanes-Oxley Act

- **Requires companies to perform quarterly self-assessments of risks to business processes that affect financial reporting and to attest to findings on an annual basis (CFO and CEO, possibly CIO too). Section 302 requires "Signing Officer" to design reports for compliance submission.**

- **Section 404 requires that technology personnel develop and implement means for protecting critical financial data (data security, back-up and recovery, business continuity planning, and disaster recovery), because loss of data is not acceptable.**

- **Section 409 will require "Real-Time Reporting" of financial data, thus creating the need for new Standards and Procedures and perhaps re-engineering of functions to better comply with the Law.**

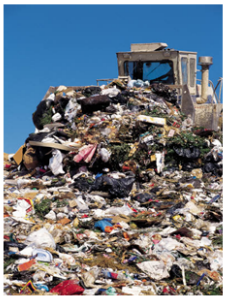
- **Companies must devise "Checks and Balances" to guaranty that those people creating functions (like programmers) are not the person responsible for validating the functions operation (rather a separate checker must validate function).**

- **Checks and Balances prohibit big 4 accounting firms from performing Risk Assessment because they are the ones performing audit (Conflict of Interest).**

- **Penalties can include fines as high as $5 million and imprisonment can be for as long as 20 years for deliberate violation.**

EPA and Superfund

EPA and Superfund



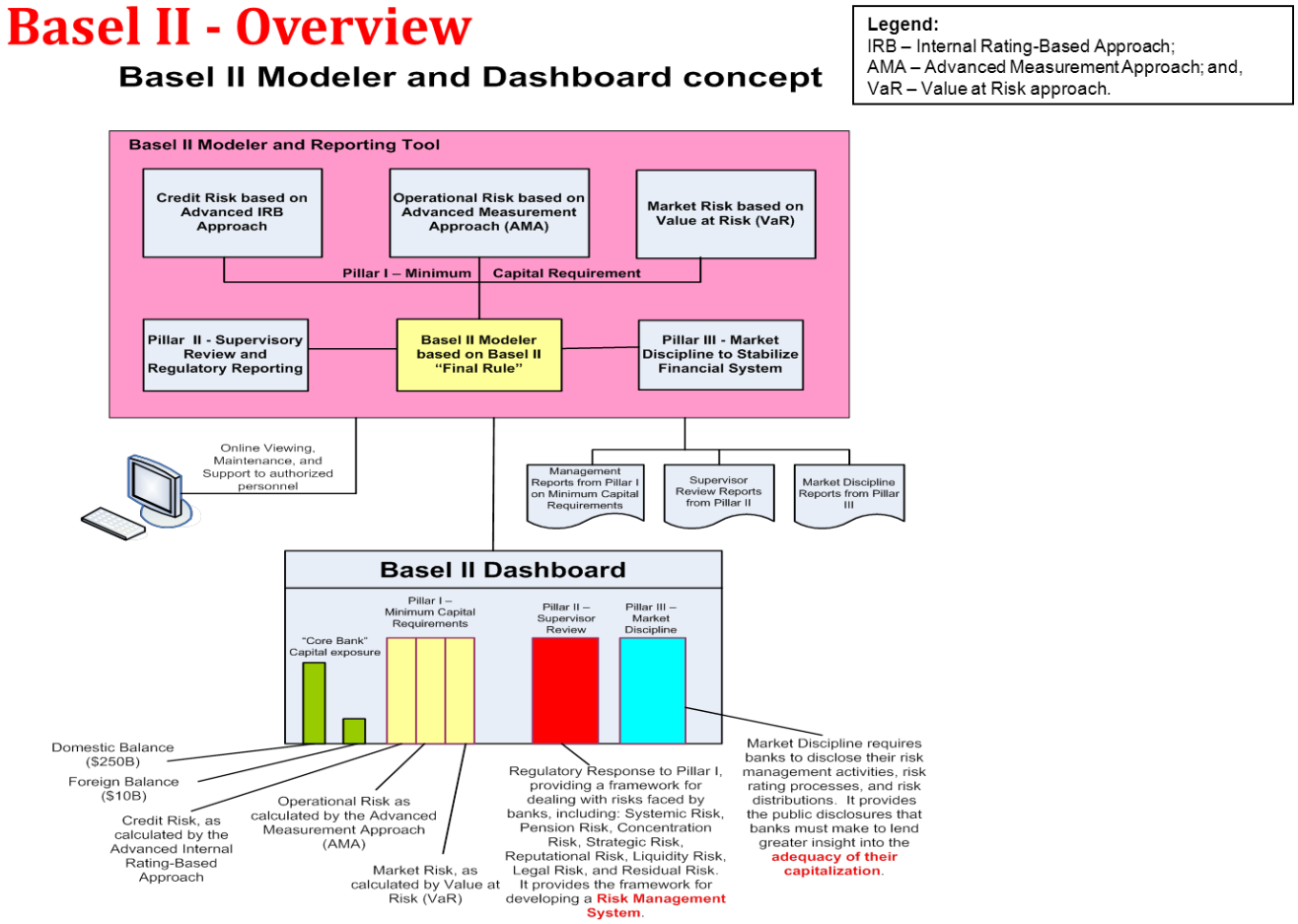
- **Designed to protect the environment from Toxic Materials that could lead to death or illness.**
- **Regulated by the Environmental Protection Agency.**
- **Fines and imprisonment can be imposed when violation is intentional, or through a third party acting in your behalf.**
- **Safeguards should be imposed to:**
  - **Identify toxic materials,**
  - **Take appropriate steps to protect employees and community personnel,**
  - **Insure that proper and authorized Waste Removal procedures are implemented,**
  - **Provide personnel awareness programs and Standards and Procedures,**
  - **Support and maintain program going forward.**

Patriot Act

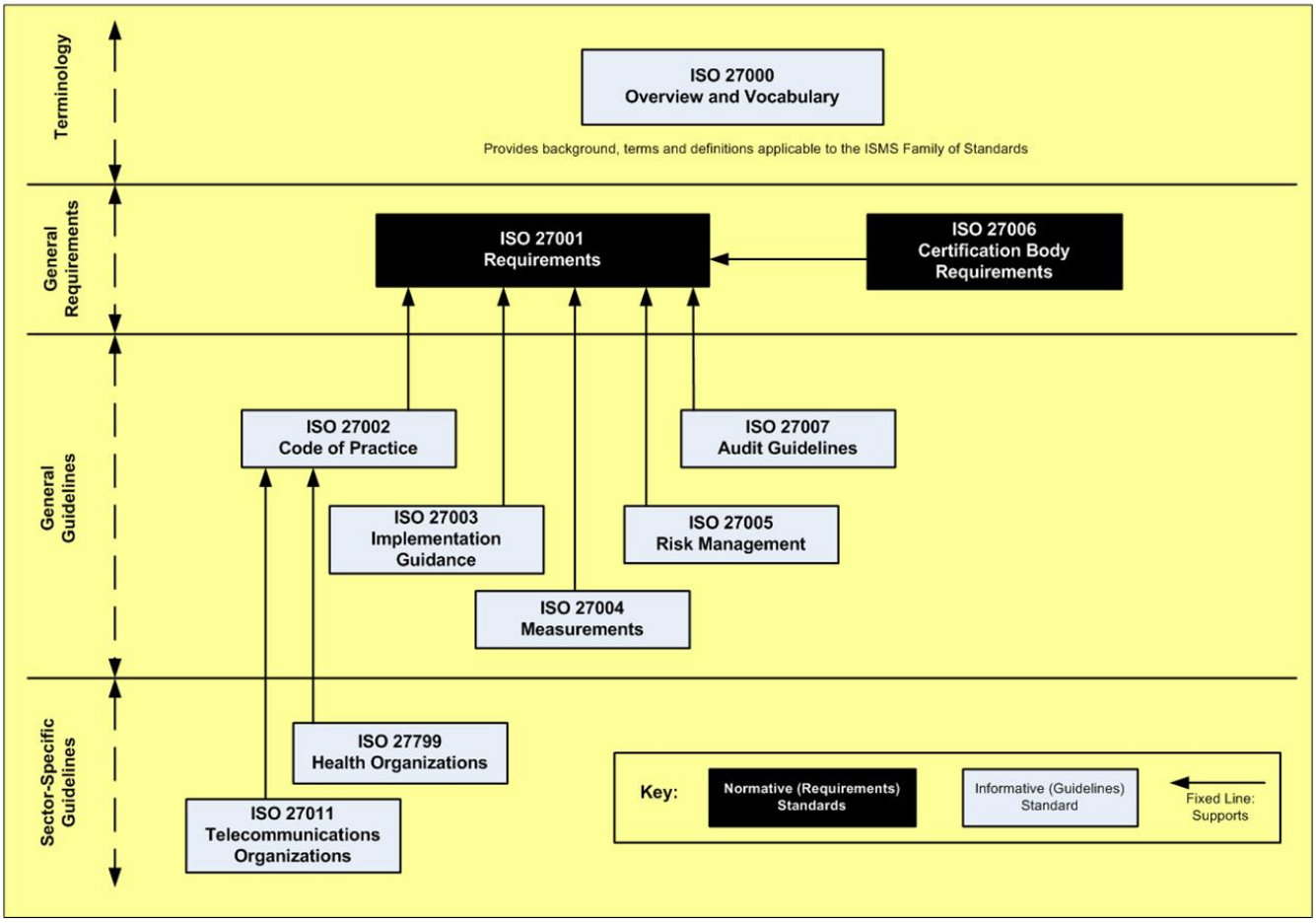
Patriots Act

- **New Requirements — Severe Penalties** (Official Title is "**Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism**").
- **USA PATRIOT Act Section 326** imposes new requirements on how organizations screen existing customers and process new customer information.
- **By October 1, 2003**, all financial services organizations must have in place procedures for:
  - **1. Customer Screening** — On a regular basis, customers and transactions must be matched against government-provided lists of suspected terrorists, drug traffickers, money launderers and other criminals.
  - **2. Customer Information Program (CIP)** — On all new customers, basic identification information must be obtained to verify the customer's identity. Failure to comply can result in penalties of up to $1 million, and/or imprisonment.
- Used to **protect the confidentiality** of telephone, face-to-face, and computer communications, **while enabling authorities to identify and intercept during criminal investigations** with warrant.
- Improves ability to obtain data during **Foreign Intelligence Investigations** and increases a companies need to safeguard voice, face-to-face, and computer based data.
- Enhances financial organizations ability to track suspected **Money Laundering** activities and requires reporting of activity when uncovered, thus fostering the need to obtain, store, and safeguard data used to report on suspected Money Laundering activities.

Basel II overview



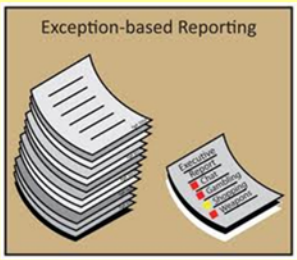
ISO 27000 Information Security Management System guidelines



Strategies for Eliminating Gaps and Exceptions

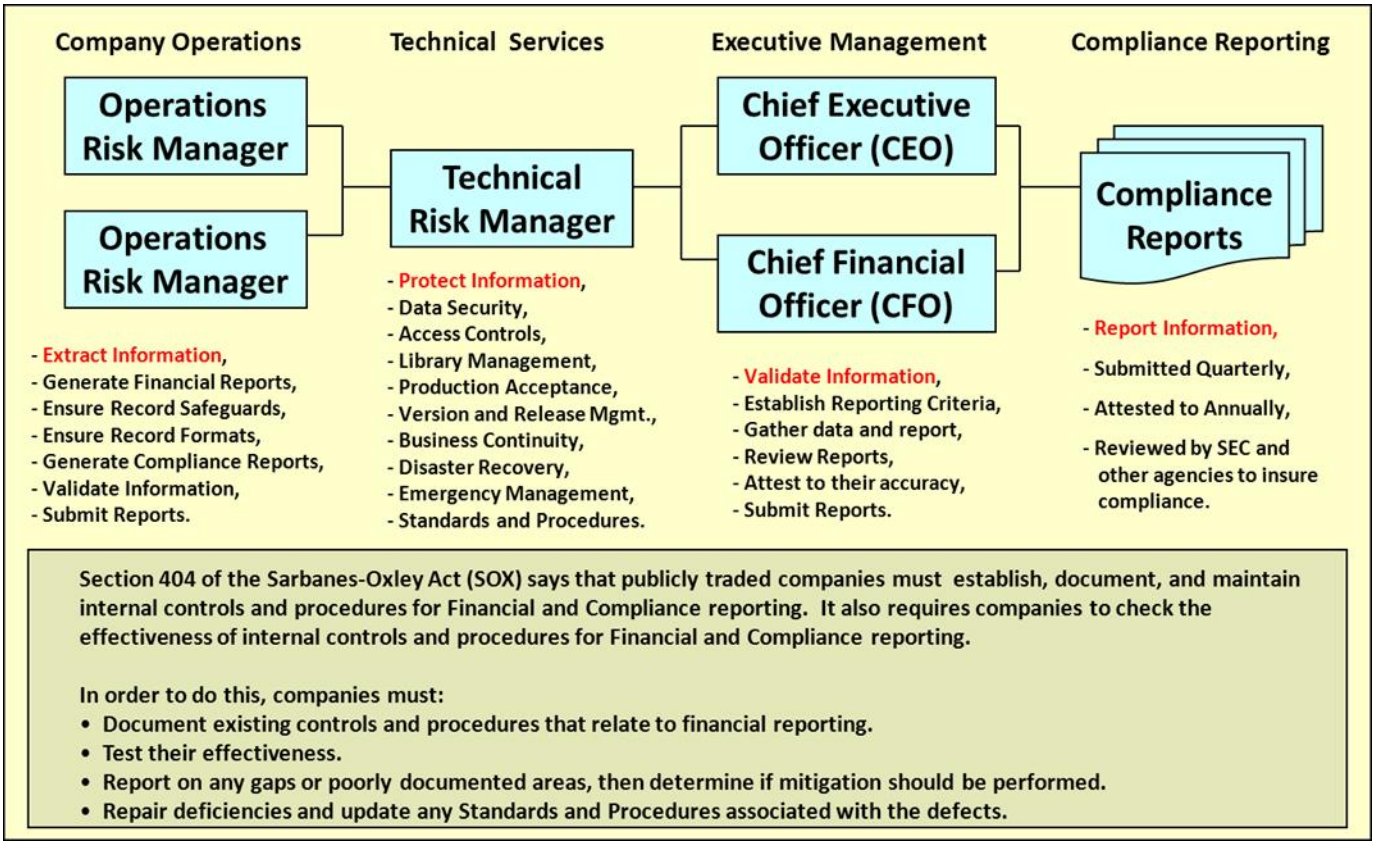
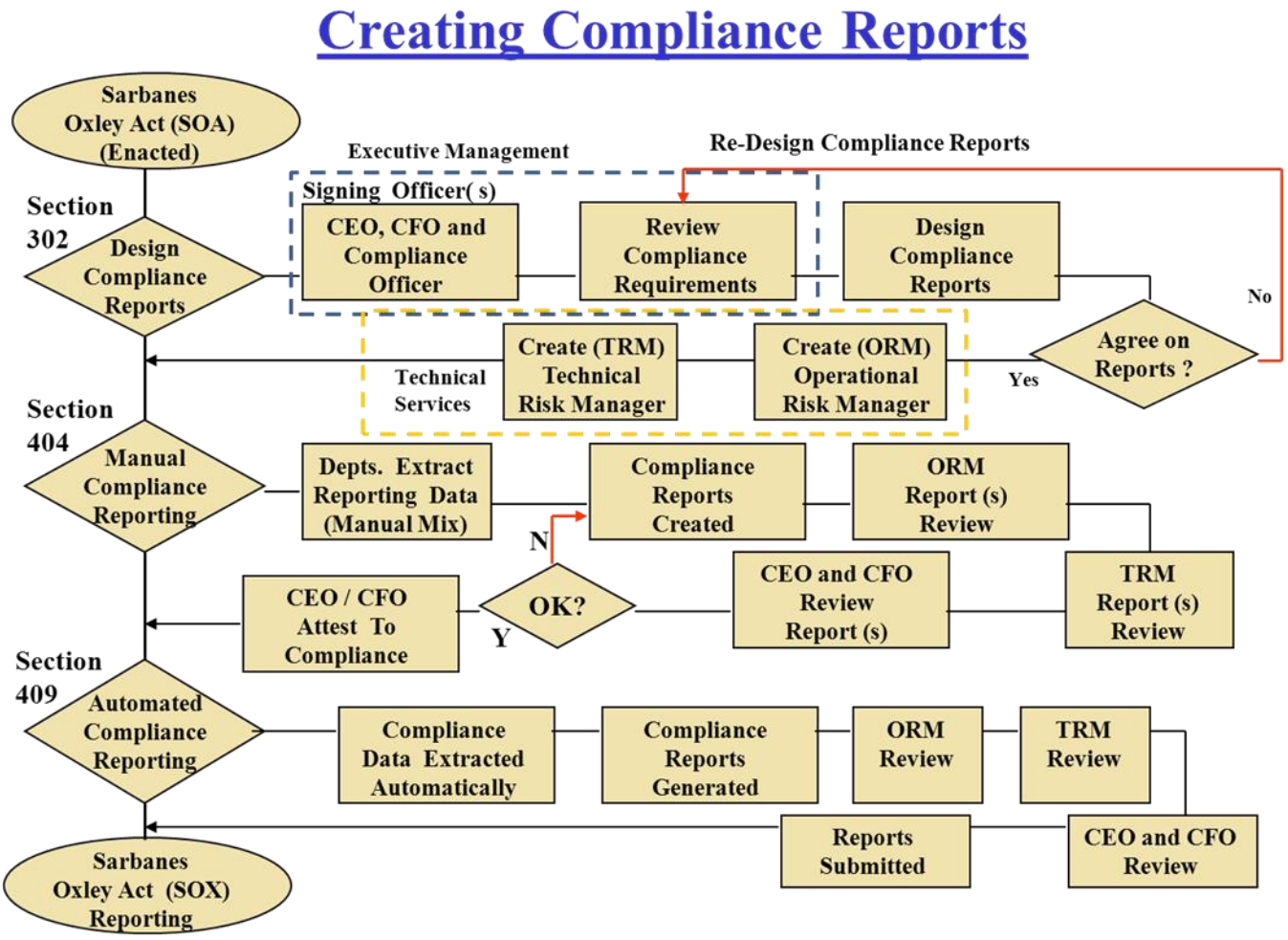
Strategies for Eliminating Audit Exceptions

- Review of Compliance Requirements (Business and Industry)
- Ensure Data Sensitivity, IT Security and Vital Records Management,
- Eliminate Data Corruption and Certify HA / CA Application recovery,
- Adhere to Systems Development Life Cycle (SDLC),
- Utilize Automated Tools whenever practical,
- Elimination of Single-Point-Of-Failure concerns,



- Create Inventory / Configuration / Asset Management guidelines,
- Develop Incident / Problem and Crisis Management procedures,
- Integrate Work-Flow automation through Re-Engineering processes,
- Implement and conduct Training and Awareness programs.

Compliance Reporting Technique



Creating Compliance Reports and a Letter of Attestation