2006

Creating a High Level Incident Response/Forensics Policy by Complying with State and Federal Regulations

Jennie DeLucia

Creating a High Level Incident Response/Forensics Policy by Complying with State and Federal Regulations

By

Jennie DeLucia

Thesis submitted in partial fulfillment of the requirements for the degree of Master of Science in Information Technology

Rochester Institute of Technology

B. Thomas Golisano College

Of

Computing and Information Sciences

2/7/2006

Rochester Institute of Technology

B. Thomas Golisano College of Computing and Information Sciences

Master of Science in Information Technology

Thesis Approval Form

Student Name: Jennie Delucia

Thesis Title: Creating a High Level Incident Response/Forensics Policy by Complying with State and Federal Regulations

Thesis Committee

Name	Signature	Date
Prof. Bill Stackpole Chair	Bill Stackpole	
Luther Troell, Ph.D. Committee Member	Luther Troell	
Yin Pan, Ph.D. Committee Member	Yin Pan	

Thesis Reproduction Permission Form

Rochester Institute of Technology

B. Thomas Golisano College of Computing and Information Sciences

Master of Science in Information Technology

Title

I, Jennie DeLucia, do not hereby grant permission to the Wallace Library of the Rochester Institute of Technology to reproduce my thesis in whole or in part. Any reproduction must not be for commercial use or profit.

Date: _ _____Signature of Author: ____Jennie DeLucia_____

Table of Contents

With the increasing number of threats involving organization's today, i.e., identity theft, fraud, and embezzlement, it's imperative that companies have an incident response/forensic policy in place in order to successfully retain and preserve potential evidence. Organizations need to not only combat current problems, but to prevent them from reoccurring. Organizations should not feel alone in this battle. The federal government along with state governments have passed legislation that mandates an incident response/forensic policy be implemented in order to comply with the newly passed regulations, such has Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA), and Gramm-Leach Bliley (GLBA). Also taken into account are guidances, frameworks, and standards that are the building blocks that many organizations have used to create their incident response/forensic policies and procedures. But how do organizations know what to document in these policies? How do they know if their policies comply with the ever growing number of regulations? How do they know that the information they are retrieving is not considered personally identifiable information that may have not been obtained legally? They do so by complying with the redundant, common criterion that is found in these regulations, standards, frameworks, and guidances.

Before creating an incident response/forensic policy, organizations need to identify privacy provisions as well as pertinent regulations, standards, frameworks, and guidances. After the latter have been identified, the incident response/forensics requirements need to be identified as well. Many organizations are now realizing the commonality/redundancies when reviewing these regulations, standards, frameworks, and guidances. By identifying these requirements and eliminating the redundancy, organizations can create and maintain a doctrine of documents that ensure that they are in compliance. When new regulations, standards, frameworks, and/or guidances are drafted and released, organizations are inconsistent when trying to comply with the

specified timelines instead of integrating them or identifying how they already fit with the current environment.

Understanding the current computer incident state and federal laws is equally important, but this expertise is expected of the legal department and law enforcement. Such laws include The Compute Fraud and Abuse Act, The Computer Security Act of 1987, The US Privacy Act of 1974, The Electronic Communication Privacy Act of 1986, the Economic Espionage Act of 1996, The National Information Infrastructure Protection Act of 1996, USA PATRIOT Act of 2001, and the Homeland Security Act of 2002. Only law enforcement, legal departments, and state and federal district attorneys can determine whether or not the incident has the acceptable amount of evidence to prosecute at the state or federal level. For the purposes of this paper, the proceeding laws will not be analyzed.

This paper will give a high level overview of the regulations, standards, frameworks, and guidances chosen for an incident response/forensics cross-mapping matrix. In addition, once the appropriate requirements have been identified, new common language requirements will be created, and the identified regulations, standards, frameworks, and guidances will be mapped to them. Once the mapping is complete, the requirements will be written as policy statements, which will create a high level policy that is in compliance with the noted regulations, standards, frameworks, and guidances.

Although redundant requirements will have been eliminated, there is still not a standardize computer forensics/incidents handling policy, procedure or process for commercial organizations. When trying to establish a standardized process, circumstances that need to be taken into account are the size of the organization: people, resources, and budget. The latter are the three biggest restraints for organizations to move forward with an incident management

program, so creating a standard will only force companies to either not have a process or have to expend above and beyond the resources they have to offer.

Although there are many regulations, standards, frameworks, guidances, and requirements mandated and implemented by organizations today, the following standards (ISO 17799:2005, FFIEC Information Security Handbook, Basel II), regulations (HIPAA, Privacy and Security Rule, GLBA Privacy and Safeguard Rule, California Information Practice Act (CA SB 1386), NY State Security Breach and Notification Act (NY AB 4254), and Sarbanes-Oxley (SOX) Section 301, 302, 404, 409, and 806), frameworks and guidances (Control Objectives for Information and related Technology (COBIT), The Committee of Sponsoring Organizations of the Treadway Commission (COSO), The Information Security Forum (ISF March 2005), and VISA/MC Payment Card Industry (PCI) requirements will be the focus for this research. All requirements associated with the latter will be listed and then common language will be extracted to and mapped within a matrix.

The following paragraphs will give an overview of each regulation, standard, guidance, framework, and requirements chosen for this paper. After the overview, each incident response/forensic requirement will be documented and noted. After all the appropriate requirements have been identified, the matrix and cross-mapping with be created along with policy statements and an over all high-level incident response/forensic policy.

Since ISO 17799:2005 and ISO 27001:2005 are not free documents, one will not find much detail in regards to its content on the Internet, but its origin and background are easier to come by. By definition, ISO 17799 is an internationally recognized Information Security Management Standard that was published originally by ISO (International Organization for

Standardization; www.iso.ch) in Switzerland in 2000 (Hoffman, 2003). The origin of the document though goes back further.

'In the mid-1990s, a group of companies in the U.K. combined to develop BS 7799 Part 1: Code of Practice for Information Security Management. The Specification for Information Security Management Systems (ISMS), which is BS 7799 Part 2, was published in February of 1998. When certification was established for BS 7799, The British Standards Institute pushed for worldwide acceptance. In October 2005, BS 7799 Part 2 was renamed to ISO 27001:2005.

The International Standards Organization (ISO) agreed, along with the International Electro-technical Commission (IEC) to 'fast track' it into an internationally accepted standard. In December 2000, BS 7799 Part 1 was adopted as an international standard. Its official document name is ISO / IEC 17799:2000. For the purposes of this document, the updated ISO 17799:2005 and ISO 27001:2005 versions were used.' (Hoffman, 2003).

ISO 17799 is very broad in scope and does not conform to any specific technology, application, software, hardware, etc. Its broad scope allows the standard to be utilized across many types of organizations and enterprises. 'The goal of ISO 17799 is to protect the assets of a corporation to ensure business continuity, minimize impact or damage to a business, and maximize an organization's return on investment.' (Hoffman, 2003).

ISO/IEC 17799:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 17799:2005 contains best practices of control objectives and controls in the following areas of information security management:

- Security policy;

- Organization of information security;
- Asset management;
- Human resources security;
- Physical and environmental security;
- Communications and operations management;
- Access control;
- Information systems acquisition, development and maintenance;
- Information security incident management;
- Business continuity management;
- Compliance

The original ISO 17799:2000 did not include Human resources security or Information systems acquisition, development, and maintenance.

The specific incident management and forensics requirements stated in ISO 17799:2005 are the following:

5.1.1 Information security policy document

Control

An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties.

Implementation guidance

The information security policy document should state management commitment and set out the organization's approach to managing information security. The policy document should contain statements concerning:

e) A definition of general and specific responsibilities for information security management, including reporting information security incidents; (BS ISO/IEC 17799:2005, 7, (2005))

5.1.2 Review of the information security policy

Control

The information security policy should be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

Implementation guidance

The information security policy should have an owner who has approved management responsibility for the development, review, and evaluation of the security policy. The review should include assessing opportunities for improvement of the organization's information security policy and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions, or technical environment. (BS ISO/IEC 17799:2005, 8, (2005))

6.1 Internal organization

Objective: To manage information security within the organization.

A management framework should be established to initiate and control the implementation of information security within the organization. Management should approve the information security policy, assign security roles and co-ordinate and review the implementation of security across the organization. If necessary, a source of specialist information security advice should be established and made available within the organization. Contacts with external security specialists or groups, including relevant authorities, should be developed to keep up with industrial trends, monitor standards and assessment methods and provide suitable liaison points

when handling information security incidents. A multi-disciplinary approach to information security should be encouraged. (BS ISO/IEC 17799:2005, 9, (2005)).

6.1.2 Information security co-ordination

Control

Information security activities should be coordinated by representatives from different parts of the organization with relevant roles and job functions.

Implementation guidance

Typically, information security co-ordination should involve the co-operation and collaboration of managers, users, administrators, application designers, auditors and security personnel, and specialist skills in areas such as insurance, legal issues, human resources, IT or risk management. This activity should: evaluate information received from the monitoring and reviewing of information security incidents, and recommend appropriate actions in response to identified information security incidents. (BS ISO/IEC 17799:2005, 10, (2005)).

6.1.6 Contact with authorities

Control

Appropriate contacts with relevant authorities should be maintained.

Implementation guidance

Organizations should have procedures in place that specify when and by whom authorities (e.g. law enforcement, fire department, supervisory authorities) should be contacted, and how identified information security incidents should be reported in a timely manner if it is suspected that laws may have been broken.

Other information

Maintaining such contacts may be a requirement to support information security incident management (Section 13.2) or the business continuity and contingency planning process (Section 14). Contacts with regulatory bodies are also useful to anticipate and prepare for upcoming changes in law or regulations, which have to be followed by the organization. Contacts with other authorities include utilities, emergency services, and health and safety, e.g. fire departments (in connection with business continuity), telecommunication providers (in connection with line routing and availability), water suppliers (in connection with cooling facilities for equipment). (BS ISO/IEC 17799:2005, 12, (2005)).

6.1.7 Contact with special interest groups

Control

Appropriate contacts with special interest groups or other specialist security forums and associations should be maintained.

Implementation guidance

Membership in special interest groups or forums should be considered as a means to: provide suitable liaison points when dealing with information security incidents (see also 13.2.1). (BS ISO/IEC 17799:2005, 13, (2005)).

6.2.1 Identification of risks related to external parties

Control

The risks to the organization's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access.

Implementation guidance

Where there is a need to allow an external party access to the information processing facilities or information of an organization, a risk assessment (see also Section 4) should be carried out to identify any requirements for specific controls. The identification of risks related to external party access should take into account the following issues: practices and procedures to deal with information security incidents and potential damages, and the terms and conditions for the continuation of external party access in the case of an information security incident; (BS ISO/IEC 17799:2005, 14, (2005).

6.2.2 Addressing security when dealing with customers

Control

All identified security requirements should be addressed before giving customers access to the organization's information or assets.

Implementation guidance

The following terms should be considered to address security prior to giving customers access to any of the organization's assets (depending on the type and extent of access given, not all of them might apply): arrangements for reporting, notification, and investigation of information inaccuracies (e.g. of personal details), information security incidents and security breaches; (BS ISO/IEC 17799:2005, 16, (2005)).

6.2.3 Addressing security in third party agreements

Control

Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements.

Implementation guidance

The agreement should ensure that there is no misunderstanding between the organization and the third party. Organizations should satisfy themselves as to the indemnity of the third party. The following terms should be considered for inclusion in the agreement in order to satisfy the identified security requirements (see 6.2.1): arrangements for reporting, notification, and investigation of information security incidents and security breaches, as well as violations of the requirements stated in the agreement; (BS ISO/IEC 17799:2005, 17, (2005)).

Other information

Some of the differences between outsourcing and the other forms of third party service provision include the question of liability, planning the transition period and potential disruption of operations during this period, contingency planning arrangements and due diligence reviews, and collection and management of information on security incidents. Therefore, it is important that the organization plans and manages the transition to an outsourced arrangement and has suitable processes in place to manage changes and the renegotiation/termination of agreements. (BS ISO/IEC 17799:2005, 18, (2005)).

8.2.1 Management responsibilities

Control

Management should require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.

Implementation guidance

Management responsibilities should include ensuring that employees, contractors and third party users:

Other Information

If employees, contractors and third party users are not made aware of their security responsibilities, they can cause considerable damage to an organization. Motivated personnel are likely to be more reliable and cause less information security incidents. Training to enhance awareness is intended to allow individuals to recognize information security problems and incidents, and respond according to the needs of their work role. (BS ISO/IEC 17799:2005, 26, (2005)).

10.2.2 Monitoring and review of third party services

Control

The services, reports and records provided by the third party should be regularly monitored and reviewed, and audits should be carried out regularly.

Implementation guidance

Monitoring and review of third party services should ensure that the information security terms and conditions of the agreements are being adhered to, and that information security incidents and problems are managed properly. This should involve a service management relationship and process between the organization and the third party to: provide information about information security incidents and review of this information by the third party and the organization as required by the agreements and any supporting guidelines and procedures;

The organization should maintain sufficient overall control and visibility into all security aspects for sensitive or critical information or information processing facilities accessed, processed or managed by a third party. The organization should ensure they retain visibility into security activities such as change management, identification of vulnerabilities, and information security incident reporting/response through a clearly defined reporting process, format and structure. (BS ISO/IEC 17799:2005, 40, (2005)).

10.2.3 Managing changes to third party services

Control

Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.

Implementation guidance

The process of managing changes to a third party service needs to take account of: new controls to resolve information security incidents and to improve security; (BS ISO/IEC 17799:2005, 41, (2005)).

10.8.2 Exchange agreements

Control

Agreements should be established for the exchange of information and software between the organization and external parties.

Implementation guidance

Exchange agreements should consider the following security conditions: responsibilities and liabilities in the event of information security incidents, such as loss of data; (BS ISO/IEC 17799:2005, 40, (2005)).

10.10.2 Monitoring system use

Control

Procedures for monitoring use of information processing facilities should be established and the results of the monitoring activities reviewed regularly.

Implementation guidance

The level of monitoring required for individual facilities should be determined by a risk assessment. An organization should comply with all relevant legal requirements applicable to its monitoring activities. Areas that should be considered include:

Other information

Usage monitoring procedures are necessary to ensure that users are only performing activities that have been explicitly authorized. A log review involves understanding the threats faced by the system and the manner in which these may arise. Examples of events that might require further investigation in case of information security incidents are given in 13.1.1. (BS ISO/IEC 17799:2005, 40, (2005)).

12.6.1 Control of technical vulnerabilities

Control

Timely information about technical vulnerabilities of information systems being used should be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

Implementation guidance

A current and complete inventory of assets (see 7.1) is a prerequisite for effective technical vulnerability management. Specific information needed to support technical vulnerability management includes the software vendor, version numbers, current state of deployment (e.g. what software is installed on what systems), and the person(s) within the organization responsible for the software. Appropriate, timely action should be taken in response to the identification of potential technical vulnerabilities. The following guidance should be followed to establish an effective management process for technical vulnerabilities:

e) Depending on how urgently a technical vulnerability needs to be addressed, the action

taken should be carried out according to the controls related to change management (see 12.5.1) or by following information security incident response procedures (see 13.2); (BS ISO/IEC 17799:2005, 88, (2005)).

13.1.1 Reporting information security events

Control

Information security events should be reported through appropriate management channels as quickly as possible.

Implementation guidance

A formal information security event reporting procedure should be established, together with an incident response and escalation procedure, setting out the action to be taken on receipt of a report of an information security event. A point of contact should be established for the reporting of information security events. It should be ensured that this point of contact is known throughout the organization, is always available and is able to provide adequate and timely response. All employees, contractors and third party users should be made aware of their responsibility to report any information security events as quickly as possible. They should also be aware of the procedure for reporting information security events and the point of contact. The reporting procedures should include:

a) Suitable feedback processes to ensure that those reporting information security events are notified of results after the issue has been dealt with and closed;

b) Information security event reporting forms to support the reporting action, and to help the person reporting to remember all necessary actions in case of an information security event;

c) The correct behavior to be undertaken in case of an information security event, i.e.

1) Noting all important details (e.g. type of non-compliance or breach, occurring malfunction, messages on the screen, strange behavior) immediately;

2) Not carrying out any own action, but immediately reporting to the point of contact;

d) Reference to an established formal disciplinary process for dealing with employees, contractors or third party users who commit security breaches.

In high-risk environments, a duress alarm4 may be provided whereby a person under duress can indicate such problems. The procedures for responding to duress alarms should reflect the high risk situation such alarms are indicating." (BS ISO/IEC 17799:2005, 88, 90, (2005)).

13.1.2 Reporting security weaknesses

Control

All employees, contractors and third party users of information systems and services should be required to note and report any observed or suspected security weaknesses in systems or services.

Implementation guidance

All employees, contractors and third party users should report these matters either to their management or directly to their service provider as quickly as possible in order to prevent information security incidents. The reporting mechanism should be as easy, accessible, and available as possible. They should be informed that they should not, in any circumstances, attempt to prove a suspected weakness. (BS ISO/IEC 17799:2005, 91, (2005)).

13.2.1 Responsibilities and procedures

Control

Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents.

Implementation guidance

In addition to reporting of information security events and weaknesses (see also 13.1), the monitoring of systems, alerts, and vulnerabilities (10.10.2) should be used to detect information security incidents. The following guidelines for information security incident management procedures should be considered: a) procedures should be established to handle different types of information security incident,

including:

1) Information system failures and loss of service;

2) Malicious code (see 10.4.1);

3) Denial of service;

4) Errors resulting from incomplete or inaccurate business data;

5) Breaches of confidentiality and integrity;

6) misuse of information systems;

In addition to normal contingency plans (see 14.1.3), the procedures should also cover (see also 13.2.2):

1) Analysis and identification of the cause of the incident; 4) communication with those affected by or involved with recovery from the incident;

The objectives for information security incident management should be agreed with management, and it should be ensured that those responsible for information security incident management understand the organization's priorities for handling information security incidents. (BS ISO/IEC 17799:2005, 92, (2005)).

Other information

Information security incidents might transcend organizational and national boundaries. To respond to such incidents there is an increasing need to coordinate response and share information about these incidents with external organizations as appropriate. (BS ISO/IEC 17799:2005, 93, (2005)).

13.2.2 Learning from information security incidents

Control

There should be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.

Implementation guidance

The information gained from the evaluation of information security incidents should be used to identify recurring or high impact incidents.

Other Information

The evaluation of information security incidents may indicate the need for enhanced or additional controls to limit the frequency, damage, and cost of future occurrences, or to be taken into account in the security policy review process (see 5.1.2). (BS ISO/IEC 17799:2005, 94, (2005)).

13.2.3 Collection of evidence

Control

"Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence should be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

Implementation guidance

Internal procedures should be developed and followed when collecting and presenting evidence for the purposes of disciplinary action handled within an organization.

Any forensics work should only be performed on copies of the evidential material. The integrity of all evidential material should be protected. Copying of evidential material should be supervised by trustworthy personnel and information on when and where the copying process was executed, who performed the copying activities and which tools and programs have been utilized should be logged." (BS ISO/IEC 17799:2005, 94, (2005)).

14.1.1 Including information security in the business continuity management process

Control

A managed process should be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.

Implementation guidance

The process should bring together the following key elements of business continuity management: understanding the impact which interruptions caused by information security incidents are likely to have on the business (it is important that solutions are found that will handle incidents causing smaller impact, as well as serious incidents that could threaten the viability of the organization), and establishing the business objectives of information processing facilities; (BS ISO/IEC 17799:2005, 95, (2005)).

14.1.4 Business continuity planning framework

Control

A single framework of business continuity plans should be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.

Implementation guidance

Each business continuity plan should describe the approach for continuity, for example the approach to ensure information or information system availability and security. Each plan should also specify the escalation plan and the conditions for its activation, as well as the individuals responsible for executing each component of the plan. When new requirements are identified, any existing emergency procedures, e.g. evacuation plans or fallback arrangements, should be amended as appropriate. Procedures should be included within the organization's change management program to ensure that business continuity matters are always addressed appropriately. A business continuity planning framework should address the identified information security requirements and consider the following: emergency procedures, which describe the actions to be taken following an incident, which jeopardizes business operations; (BS ISO/IEC 17799:2005, 97, (2005)).

14.1.5 Testing, maintaining and re-assessing business continuity plans

Control

Business continuity plans should be tested and updated regularly to ensure that they are up to date and effective.

Implementation guidance

Business continuity plan tests should ensure that all members of the recovery team and other relevant staff are aware of the plans and their responsibility for business continuity and information security and know their role when a plan is invoked. The test schedule for business

continuity plan(s) should indicate how and when each element of the plan should be tested. Each element of the plan(s) should be tested frequently. A variety of techniques should be used in order to provide assurance that the plan(s) will operate in real life. These should include: simulations (particularly for training people in their post-incident/crisis management roles); (BS ISO/IEC 17799:2005, 98, (2005)).

As noted above, the ISO 17799:2005 requirements for incident management and response and forensics transcend the organization's information security policy and posture, which include training, business continuity, third party agreements, contacts, management's involvement and support, and reporting. Requirements do not simply fall under and incident response and forensic categories, furthering the need for a policy that maps directly to regulations, standards, and frameworks.

The next standard used for research is The Federal Financial Institutions Examination Council (FFIEC). 'The FFIEC is an organization established by Congress in 1987 to coordinate and unify regulations, standards, and report forms among the five member federal agencies that regulate savings institutions, commercial banks, and credit unions: Office of Thrift Supervision (OTS), Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System (FRB), Federal Deposit Insurance Corporation (FDIC), and National Credit Union Administration (NCUA). The work of the council is carried out by five task forces, made up of representatives of each agency, dealing with: education and training, supervision, reports, consumer compliance, and surveillance. For the purposes of this paper, the focus will be on the FFIEC Information Security (IS) Examination Handbook. Overall, there are twelve handbooks. The Information Security Examination Handbook contains 80% of the material found in the other handbooks.' (http://www.ffiec.gov/).

The FFIEC IS Handbook is divided into seven sections; Introduction, Security Process, Information Security Risk Assessment, Information Security Strategy, Security Controls, Implementation, Security Testing, and Monitoring and Updating, accompanied by three appendices; Appendix A: Examination Procedures, Appendix B: Glossary, and Appendix C: Laws, Regulations, and Guidance. The specific incident management and forensics requirements stated in the FFIEC Information Security Examination Handbook are the following sections:

"Security Controls Implementation (Logical and Administrative Control):

Security personnel and network administrators have related but distinct responsibilities for ensuring secure network access across a diverse deployment of interconnecting network servers, file servers, routers, gateways, and local and remote client workstations. Security personnel typically lead or assist in the development of policies, standards, and procedures, and monitor compliance. They also lead or assist in incident-response efforts. Network administrators implement the policies, standards, and procedures in their day-to-day operational role." ((FFIEC), 28, (2002)).

"Physical Security (Data Center Security):

Detection devices, where applicable, should be utilized to prevent theft and safeguard the equipment. They should provide continuous coverage. Detection devices have two purposes—to alarm when a response is necessary and to support subsequent forensics. The alarm capability is only useful when a response will occur." ((FFIEC), 45, (2002)).

"Logging and Data Protection:

Financial institutions should take reasonable steps to ensure that sufficient data is collected from secure log files to identify and respond to security incidents and to monitor and enforce policy compliance." ((FFIEC), 64, (2002)). "Many products such as firewall and intrusion detection

software can simplify the security monitoring by automating the analysis of the logs and alerting the appropriate personnel of suspicious activity. Log files are critical to the successful investigation and prosecution of security incidents and can potentially contain sensitive information." ((FFIEC), 65, (2002)).

"The financial institution should have an effective means of tracing a security event through their system. Synchronized time stamps on network devices may be necessary to gather consistent logs and a consistent audit trail. Additionally, logs should be available, when needed, for incident detection, analysis and response." ((FFIEC), 66, (2002)).

"Service Provider Oversight:

Financial institutions should exercise their security responsibilities for outsourced operations through Coordination of incident response policies and contractual notification requirements." ((FFIEC), 66, (2002)).

"Financial institutions should determine the following security considerations when selecting or monitoring a service provider: Clear understanding of the provider's security incidence response policy and assurance that the provider will communicate security incidents promptly to the institution when its systems or data were potentially compromised." ((FFIEC), 67, (2002)).

"Intrusion Detection and Response (Intrusion Response):

Successful implementation of any response policy and procedure requires the assignment of responsibilities and training. Some organizations formalize the response organization with the creation of a computer security incident response team (CSIRT). The CSIRT is typically tasked with performing, coordinating, and supporting responses to security incidents. Due to the wide range of non-technical issues that are posed by an intrusion, typical CSIRT membership includes individuals with a wide range of backgrounds and expertise, from many

different areas within the institution. Those areas include management, legal, public relations, as well as information technology. Other organizations may outsource some of the CSIRT functions, such as forensic examinations." ((FFIEC), 74, (2002)).

"Insurance:

Insurance coverage is increasingly available to cover risks from security breaches or denial of service attacks. For example, several insurance companies offer e-commerce insurance packages that can reimburse financial institutions for losses from fraud, privacy breaches, system downtime, or incident response. Insurance coverage is rapidly evolving to meet the growing number of security-related threats. Coverage varies by insurance company, but currently available insurance products may include coverage for the following risks: Incident response costs related to the use of negotiators, public relations consultants, security and computer forensic consultants, programmers, replacement systems, etc.' ((FFIEC), 76, (2002)). 'For example, financial institutions should understand the extent of coverage available in the event of security breaches at a third-party service provider. In such a case, the institution may want to consider contractual requirements that require service providers to maintain adequate insurance to cover security incidents." ((FFIEC), 77, (2002)).

"Appendix A (Quality Risk Management Objective 5: Evaluate the security-related controls embedded in vendor management):

Evaluate the adequacy of incident response policies and contractual notification requirements in light of the risk of the outsourced activity." ((FFIEC), A-5, (2002)).

"Appendix A (Objective 7: Evaluate the effectiveness of enterprise-wide security administration):

Evaluate coordination of incident response policies and contractual notification

requirements." ((FFIEC), A-7, (2002)).

"Appendix A (Examination Procedures- Network Security):

Determine whether logs of security-related events are sufficient to affix accountability for network activities, as well as support intrusion forensics and IDS. Additionally, determine that adequate clock synchronization takes place." ((FFIEC), A-13, (2002)).

"Appendix A (Examination Procedures-Host Security):

Determine whether logs are sufficient to affix accountability for host activities and to support intrusion forensics and IDS and are appropriately secured for a sufficient time period." ((FFIEC), A-15, (2002)).

"Appendix A (Personnel Security):

Determine if employees have an available and reliable mechanism to promptly report security incidents, weaknesses, and software malfunctions." ((FFIEC), A-16, (2002)).

"Appendix A (Examination Procedures- Application Security):

Determine whether appropriate logs are maintained and available to support incident detection and response efforts." ((FFIEC), A-17, (2002)).

"Appendix A (Examination Procedures- Intrusion Detection and Response):

Determine whether logs of security-related events are sufficient to assign accountability for intrusion detection system activities, as well as support intrusion forensics and IDS. ((FFIEC), A-18, (2002)). Determine whether an incident response team: contains appropriate membership, is available at all times, has appropriate training to investigate and report findings, has access to back-up data and systems, an inventory of all approved hardware and software, and monitored access to systems (as appropriate), and has appropriate authority and timely access to decision makers for actions that require higher approvals. ((FFIEC), A-19, (2002)).

"Appendix A (Service Provider Oversight Security):

Determine whether appropriate reporting of security incidents is required under the contract." ((FFIEC), A-21, (2002)).

Again, as with the ISO 17799:2005 standard, the FFIEC's incident management and response and forensics requirements transcend into security controls, physical security, third-party access and contractors, personnel security, and logical access. In addition, the FFIEC also contains an insurance section, which was not noted in the ISO 17799:2005 standard.

The last standard is Basel II, which in some eyes, is considered a framework. 'The leading international financial standards-setting institution, the Basel Committee on Banking Supervision has created important new standards for electronic banking. In a report entitled 'Risk Management for Electronic Banking,' the Basel Committee set fourth risk management principles to help banking institutions expand their existing risk oversight policies and processes to cover electronic banking. These Risk Management Principles call for banks to establish effective incident response capabilities, including essential computer forensic tools.' (Patzakis, J. 2003).

'In order to implement the Risk Management Principle (Principle 14), the Basel Committee highlighted eight actions that should be undertaken by banks, including four specific incident response and forensic functions or capabilities that banks should develop:

- Incident response plans to address recovery of e-banking systems and services under various scenarios, business and geographic locations
- Mechanisms to identify a crisis as soon as it occurs, access its materiality, and controls the reputation risk associated with any services

- Incident response teams with the authority to act in an emergency and sufficiently trained to analyzing incident detection/response systems and interpreting the significance of related output.
- A process for collecting and preserving forensic evidence to facilitate appropriate post-mortem reviews of any e-banking incidents as well to assist in the prosecuting of attackers'. (Patzakis, J. 2003).

Now that the above standards have been parsed, and incident and forensic requirements have been identified, the following paragraphs will cover federal regulations. These regulations include The Health Insurance Portability and Accountability Act (HIPAA) of 1996, Gramm-Leach-Bliley Act of 1999 (GLBA), California State Bill 1386 (CA SB 1386), New York State Information Security Breach and Notification Act (NY AB 4254), and Sarbanes-Oxley Act of 2002 (SOX). These regulatory acts have specific requirements to ensure the protection and privacy of individual's personal data as well as mandate incident response and forensics policies and procedures.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was passed to ensure that individual personal health care information was not being disclosed to unauthorized individuals. HIPAA includes two rules, the Privacy and Security Rule. The Security Rule is broken down into Administrative, Physical, and Technical Safeguards that include and require incident management and response and forensics. Each requirement within each safeguard is either required or addressable. If the requirement is required, then it is mandatory that their implementation be carried out. If the requirement is addressable, it does not mean that it is not required, only that it needs to be implemented when necessary and reasonable. Administrative safeguards make up fifty percent of the Security Rule's standard. In general, they require

documented policies and procedures for day to day operations; managing the conduct of employees with protected health information (PHI); and managing the selection, development, and use of security controls. The specific administrative standards that pertain to incident management and response and forensics:

'Section 164.308 (1) (i) Security management process: Implementing policies and procedures to prevent, detect, contain, and correct security violations

Section 164.308(5) (ii) Security incident procedures: Implementing policies and procedures to handle security incidents.' (SANS 2003, page 7).

'Under the Security Management process there are four required requirements, one of which involves Incident Management; Information System Activity Review. This requirement states that security incident reports are used to assess if security controls are appropriate or need to be improved for organizational effectiveness. Under the Security Incident Procedures there is one requirement that is also required; Response and Reporting. This requirement states that organization's policies and procedures must identify the actions to take when a security incident is discovered, the outcome of your actions, and the impact on the information you are protecting. This means if you, an unauthorized person, gained access to electronic protected health information (ePHI), what actions did you take to revoke the access, access that the information is still valid and controls you put in place so the event could not occur again.' (SANS 2003, page 22).

Gramm-Leach-Bliley Act (GLBA), also known as The Financial Modernization Act of 1999, includes provision to protect consumers' personal financial information by financial institutions. Like with HIPAA, GLBA not only contains a Privacy Rule, but a Safeguards Rule as well. (http://www.ftc.gov/privacy/privacyinitiatives/glbact.html).

The Safeguards Rule requires financial institutions to have a security plan established and in place to protect the confidentiality and integrity of individual's personal consumer information. (http://www.ftc.gov/privacy/privacyinitiatives/safeguards.html).

Similar to HIPAA, GLBA breaks down its requirements into three distinct categories/safeguards for securing personal or personally identifiable information: Employee Management and Training, Information Systems, and Managing System Failures.

The main incident response/forensic procedure requirement within GLBA falls under the Employee Management and Training safeguard:

1. Recognizing any fraudulent attempt to obtain customer information and reporting it to the appropriate law enforcement agencies. (http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm).

Additional requirement do fall under the Information Systems Safeguard as well:

1. Store paper records in a room, cabinet, or other container that is locked when unattended;

2. Ensure that storage areas are protected against destruction or potential damage from physical hazards, like fire or floods;

3. Store electronic customer information on a secure server that is accessible only with a password - or has other security protections - and is kept in a physically-secure area;

4. Don't store sensitive customer data on a machine with an Internet connection; and

5. Maintain secure backup media and keep archived data secure, for example, by storing off-line or in a physically-secure area.

6. Dispose of customer information in a secure manner. For example:

a. Hire or designate a records retention manager to supervise the disposal of records containing nonpublic personal information;

b. Shred customer information recorded on paper;

c. Erase all data when disposing of computers, diskettes, magnetic tapes, hard drives or any other electronic media that contain customer information;

d. Effectively destroy the hardware; and

e. Promptly dispose of outdated customer information.

(http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm).

Last, are the Managing System Failures safeguards, which include the following relevant requirements:

1. Maintain up-to-date and appropriate programs and controls by:

a. Following a written contingency plan to address any breaches of your physical, administrative or technical safeguards;

b. Checking with software vendors regularly to obtain and install patches that resolve software vulnerabilities;

c. Using anti-virus software that updates automatically;

d. Maintaining up-to-date firewalls, particularly if you use broadband Internet access or allow employees to connect to your network from home or other off-site locations; and

e. Providing central management of security tools for your employees and passing along updates about any security risks or breaches.

(http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm).

The next piece of legislation relevant to an incident response/forensic policy is California's State Bill number 1386 (CA SB 1386). 'CA SB 1386 obligates companies to electronically store any encrypted personal information of any California resident and to notify such persons of a security breach to the database storing their data. The statute was created to address one of the fastest growing crimes committed in California-identity theft, but it has far broader legal implications. Specifically, SB 1386, codified as Civil Code Â§ 1798.82, *et seq.*, requires 'any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, [to] disclose any breach of the security system to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person'. The statute imposes specific notification requirements on companies in such circumstances. The statute applies regardless of whether the computerized consumer records are maintained in or *outside* California. As long as a company conducts business in California and owns or licenses computerized data that includes "personal information" (defined below) about residents, it has a legal obligation to notify its California consumers of security breaches to their personal information. The statute thus has broad implications for companies across the United States, and worldwide, if they maintain, own, or license unencrypted computer data containing personal

information about California residents. The statute defines "personal information" as an individual's first name or first initial and last name in combination with any one or more of the following, when either the name or data elements are not encrypted: (a) Social Security number; (b) driver's license number or California ID card number; (c) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.' ('Technology', 2003). Again, a majority of the provisions included in CA SB 1386 are also addressed in the VISA CISP (PCI requirements), which will be defined later in the paper. For the purposes of an incident response/forensics policy, it will be crucial to identify such personal information and determine, what, if any, was compromised during the breach. In addition, the policy must define and determine what the procedures are to recover any compromised encrypted data as well. The statute broadly defines a security breach as an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. The statute does not define the term unauthorized or specify what evidence of a breach is necessary to trigger notification obligations. The statute also leaves unresolved whether companies have an affirmative duty to actively monitor and detect security breaches. In order to gain compliance under this bill, organizations need to implement the following:

1. 'Develop and implement measures for detecting and reporting incidents of unauthorized access to personal information. Make sure you retain relevant records and test, maintain and audit the effectiveness of access controls and security measures'. ('Technology', 2003).

2. 'Develop and implement procedures for rapid assessment of suspected security breaches, referral of suspected criminal acts to law enforcement agencies, notification of affected California residents and for appropriate public announcements to stakeholders and other interested parties to minimize the negative impact of the security breach.' ('Technology', 2003).

California is not the only state that has passed such legislation. New York State has its own version of the CA SB 1386 as well. Its name is The Information Security Breach and Notification Act (NY AB 4254).

'The Information Security Breach and Notification Act (NY AB 4254) requires entities that conduct business in New York State and own or license 'private' data to notify state residents affected by any security breach that results in unauthorized acquisition of that data. 'Private' data is defined as unencrypted computerized information that can identify the individual, combined with one of the following data elements: 1) social security number, 2) driver's license or non-driver identification card number, or 3) financial account information such as credit or debit card numbers in combination with access codes or PIN numbers. Private data is considered to be unencrypted when either the identifying information or the data element is not encrypted or is encrypted with a key that has also been acquired. Notification must be provided directly to the affected persons by a) written notice, b) electronic form, c) telephone notice, or d) under certain conditions, e-mail notice, conspicuous posting of the notice on the website of the affected business, and notification to major statewide media. In addition, persons or businesses that maintain, but do not own private data, are obligated to notify the entity that owns or licenses the data when a security breach results in unauthorized access. Under the Act,

the data owner or licensee most likely remains responsible for notifying the individuals affected by the security breach. In light of these legislative developments, entities that conduct business in New York State must be particularly vigilant to ensure that privacy date is secure. At a minimum, a person or business that possesses private should: 1) implement procedures to monitor the review database and other computerized information storage devices to identify where private data is stored; and 2) establish clear and effective notification procedures to responds to actual breaches of security. The specific requirement that needs to be added to an organization's incident response/forensic policy is that notification procedures are defined and that personal information is defined as well.' ('New York', 2005)

The last regulation analyzed is the Sarbanes-Oxley (SOX) Act of 2002. This act, or certain sections of this act, has cost publicly traded organizations time, resources, and their sanity. Sarbanes-Oxley was created and passed due to the lack of internal controls that caused inflated profits and the loss of employees' retirements. The following sections contain incident response and forensic requirements:

Section 404 requires companies to institute effective 'internal controls that provide assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the company's assets that could have a material effect on financial documentation.' (Limongelli and Patzakis, 2004).

Section 302 requires CEOs and CFOs to evaluate the company's 'internal controls and their effectiveness, noting, when assessing a company's internal control structure, management must analyze those controls related to the prevention, identification, and detection of fraud. (68 FR 36636, 36643) (Limongelli and Patzakis, 2004).

Section 301 states that 'The Audit Committee must 'establish procedures for (a) the receipt, retention, and treatment of complaints regarding accounting, internal accounting controls, anonymous submission by employees of concerns regarding questionable accounting auditing matters. Failure to investigate whistleblower complaints, quickly and competently would suggest a lack of internal controls under Section 404 and 302. Companies must provide basis for any assessment and rejection of claims. Failure to follow Section 301 of Sarbanes-Oxley subjects a company to being de-listed.' (68 FR 64154). (Limongelli and Patzakis, 2004).

Section 806 of SOX provides a 'civil cause of action for any employee who is retaliated against for whistle blowing if employee 'reasonably believes' fraud is occurring. Section 1107 of SOX creates federal crime for retaliating against whistleblowers that provide assistance to law enforcement.' (Limongelli and Patzakis, 2004).

'Section 409 of Sarbanes-Oxley; each reporting company must communicate timely information to the public. Delayed investigation may prevent timely response, and delays may result in lost evidence or opportunities. Section 802 of Sarbanes-Oxley institutes severe criminal penalties for destruction of evidence.' (Limongelli and Patzakis, 2004).

The following table summarized the overall requirements/per section for the Sarbanes-Oxley Act:

Sarbanes-Oxley Overall requirements	Per Section
Effective Internal Investigations	302, 404, and 806
Evidence of Due Diligence	301, 302, and 404
Rapid Response: Expedient, efficient, and	302, 404, and 409

thorough	
Deleted Document Recovery	802
Document Preservation/Retention	802

Again, it is important to remember the following with standards, regulations, and frameworks: Standards tell you somewhat how to comply with their set of requirements, but don't give a standard reporting or metrics to follow or gauge what level of compliance companies are at. Regulations on the other hand, give you no guidance as to how to comply, only mandate that companies do within a certain time frame. Frameworks and guidances give examples of how to build and/or organize polices, procedures, and standards in order to comply with standards and regulations.

The next section of research will cover the frameworks and guidances. The entities covered include the Standard of Good Practice for Information Security (ISF), Control Objectives for Information and related Technology (COBIT), and The Committee of Sponsoring Organizations of the Treadway Commission (COSO).

The Standard of Good Practice for Information Security (ISF v4) is an independent authority on information security that provides practical guidance and solution to overcome the wide-ranging security challenges impacting business information today. Again, this standard of good practice is not required by public or private organizations, rather it acts as a step by step guide of what these organizations need to accomplish in order to create and maintain a successful incident response/forensics program. The ISF is broken down into five categories: security management, critical business applications, computer installations, networks, and systems

development. The following key requirements have been marked as essential for the incident response/forensic policy and process:

'Area SM 5 Malicious Attack

Organizations are often subject to malicious attacks from third parties, for example by viruses of hacking. Consequently, this area covers the security controls required to protect against viruses and other malicious code, provide intrusion detection capabilities, respond to a serious attack, and to manage forensic investigations. The following principles and objectives fall under the requirements needed for incident response and forensic investigations:

Section SM 5.5 Forensic Investigations

Principle: A process should be established for dealing with incidents that require forensic investigations.

Objective: To identify perpetrators of malicious acts and preserve sufficient evidence to prosecute them if required.' ((ISF IS), 7, (2005)).

'Area CB 2 Application Management

Keeping business risks within acceptable limits requires a coherent set of Information security arrangements. Accordingly, this area covers the roles and responsibilities required (including 'business ownership'), integral application controls, and additional controls for handling sensitive material for transferring sensitive information. In addition, this area covers general management controls including change management, incident management, and business continuity.

Section CB 2.4 Incident management

Principle: All incidents of any type should re recorded, reviewed, and resolved using an incident management process.

Objective: To identify and resolve incidents effectively, minimize their business impact and reduce the risk of similar incidents occurring.' ((ISF IS), 12, (2005)).

'Area CI 2 Live Environment

Section CI 2.2 Event logging

Principle: Logs of all key events within the computer installation should be maintained (preferably using automated tools), reviewed periodically and protected against unauthorized change.

Objective: To ensure individual accountability and to enable incidents such as access violation, to be investigated and resolved.' ((ISF IS), 18, (2005)).

'Area CI 3 System Operation

Achieving service targets requires computer installations to be run in accordance with sound disciplines. Accordingly this area covers basic controls over system operations (i.e. handling computer media, back-up, and change management) and arrangements for identifying and resolving incidents (i.e. incident management and emergency fixes).

Section CI 3.4 Incident management

Principle: All incidents of any type should be recorded, reviewed, and resolved using an incident management process.

Objective: To identify and resolve incidents effectively, minimize their business impact and reduce the risk of similar incident s occurring.' ((ISF IS), 20, (2005)).

'Area NW 3 Network Operations

Maintaining continuity of service to users requires computer networks to be run in accordance with sound disciplines. Accordingly this area covers the arrangements needed to monitor network performance and to manage change and incidents. In addition, the area covers the arrangements required to provide physical security, take back-ups, and ensure service continuity.

Section NW 3.3 Incident management

Principle: All network incidents of any type should be recorded, reviewed, and resolved using an incident management process.

Objective: To identify and resolve network incidents effectively, minimize their business impact, and reduce the risk of similar incidents occurring.' ((ISF IS), 26, (2005)).

'Section SM 2.2 Information security function

Principle: A specialist information security function should be established, which has enterprise-wide responsibility for promoting information security.

Objective: To ensure good practice in information security is applied effectively throughout the enterprise.

SM 2.2.2 The information security function should:

e) Investigate major information security incidents.' ((ISF IS), SM 2.2, (2005)).

'Section SM 2.4 Security Awareness

Principle: Specific activities should be undertaken, such as a security awareness program, to promote security awareness to all individuals who have access to the information and systems of the enterprise.

Objective: To ensure all relevant individuals understand the key elements of information security and why it is needed, and understand their personal information security responsibilities.

SM 2.4.1 Specific activities should be performed to promote security awareness (the extent to which staff understand the importance of information security, the level of security required by the organization and their individual security responsibilities ad act accordingly) across the enterprise. These activities should be:

h) Aimed at reducing the frequency and magnitude of incidents' ((ISF IS), SM 2.4 (2005)).

'SM 2.4.4 The effectiveness of security awareness should be monitored by measuring:

b) The effectiveness of security awareness activities, for example by monitoring the frequency and magnitude of incidents experienced.' ((ISF IS), SM 2.4, (2005)).

'SM 3.3.5 Once risks have been identified, information risk analysis methods should help organization to:

a) Select the security controls that will reduce the likelihood of serious incidents occurring' ((ISF IS), SM 3.3, (2005)).

'Area SM 5 Malicious Attack

Organizations are often subject to malicious attack from third parties, for example, by viruses or hacking. Consequently, this area covers the security controls required to protect against viruses and other malicious code, provide intrusion detection capabilities, respond to a serious attack and manage forensic investigations.

Section SM 5.1 Virus protection

Principle: Virus protection arrangements should be established and maintained enterprise-wide.

Objective: To protect the enterprise against the virus attack and ensure it can respond to virus infection within critical timescales.

SM 5.1.2 The risk of virus infection should be reduced by:

e) Implementing emergency procedures for dealing with virus incidents' ((ISF IS), SM 5.1, (2005)).

'Section SM 5.5 Forensic Investigations

Principle: A process should be established for dealing with incidents that require forensic investigation.

Objective: To identify perpetrators of malicious acts and preserve sufficient evidence to prosecute them if required.

SM 5.5.1 A process should be established for dealing with incidents that may require forensic investigations

SM 5.5.2 There should be documented standards/procedures for dealing with incidents that may require forensic investigation, which should cover:

a) Immediate preservation of evidence on discovery of an incident
b) Compliance with a published standard or code of practice for recovery of admissible evidence
c) Maintenance of a log of evidence recovered and the investigation processes undertaken
d) The need to seek legal advice where evidence is recovered
e) Notifying staff that actions may be monitored during the investigation

SM 5.5.3 Evidence should be collected:

a) As if criminal prosecution is pending

b) With respect for all individuals' privacy and human rights

c) From as many IT sources as possible (e.g. active, temporary and deleted files, email, or Internet usage, memory cache, and network logs)

d) From as many non-IT sources as possible (e.g. CCTV, building access logs and eye witness accounts).

SM 5.5.4 During an investigation steps should be taken to:

a) Establish and document a chronological sequence of events

b) Log investigative actions

c) Demonstrate that appropriate evidence has been collected, preserved, and that no one could have tampered with it.

d) Secure target computer equipment

e) Analysis evidence in a controlled environment (i.e. using a copy or 'image' of the computer media to avoid corruption of the original)

f) Have evidence reviewed by an impartial independent expert to ensure that it meets legal requirements

g) Ensure that processes used to create and preserve evidence can be repeated by an independent third party

h) Limit information about an investigation to a few nominated individuals and ensure it is kept confidential.

SM 5.5.5 All results from the investigation should be reported to senior management and appropriate legal/regulatory bodies.' ((ISF IS), SM 5.6, (2005)).

'Section SM 6.7 Outsourcing

Principle: A process should be established to govern the selection and management of outsource providers supported by documented agreements that specify the security requirements to be met.

Objective: To ensure that security requirements are satisfied and maintained when the running of a particular environment is entrusted to an outsource provider.

SM 6.7.4 Documented agreements, such as contracts, should be established that oblige outsource providers to:

b) Provide information about security incidents' ((ISF IS), SM 6.7, (2005)).

'Section SM 7.2 Security monitoring

Principle: The information security condition of the enterprise should be monitored periodically and reported to top management.

Objective: To provide top management with an accurate, comprehensive and coherent assessment of the security condition of the enterprise.

SM 7.2.3 Information collected for monitoring purposes should include details about:

f) The pattern and business impact of incidents

g) Individual incidents that have had a sever business impact on the enterprise

SM 7.2.4 Information about security condition of the enterprise should:

g) Help calculate the overall cost of security (i.e. the cost of implementing controls plus financial of incidents).' ((ISF IS), SM 7.2, (2005)).

'Section CB 2.4 Incident management

Principle: All incidents of any type should be recorded, reviewed, and resolved using an incident management process.

Objective: To identify and resolve incidents effectively, minimize their business impact, and reduce the risk of similar incidents occurring.

CB 2.4.1 All incidents that affect the application (including malicious attacks, abuse/misuse of systems by staff, loss of power/communications services and errors by users or computer staff) should be dealt with in accordance an incident management process

CB 2.4.2 The incident management process should be documented and cover reporting and recording of incidents, investigation and resolving incidents, reviewing patterns of incidents, and escalation of processes.

CB 2.4.3 Incidents should be:

a) Reported to a single point of contract, such as a help desk, telephone hot line or individual IT specialists.
b) Documented, typically using an automated incident management system
c) Categorized by type (e.g. malfunctions, malicious attack of internal abuse/misuse of systems)
d) Prioritized according to their impact/urgency

CB 2.4.4 The business impact of significant incidents should be assessed by an IT specialist, the application 'owner' and an information security specialist.

CB 2.4.5 The resolution of incidents should include:

a) Investigation their root causes
b) Planning corrective action to ensure security is not affected
c) Restricting access when corrective actions are performed
d) Documenting corrective actions taken
e) Performing a review to ensure that the security of the application has not been affected by the incident or its resolution.

CB 2.4.6 Patterns of incidents should be reviewed to identify potential security breaches and minimize chances of similar incidents disrupting the applications or other applications in the future.' ((ISF IS), CB 2.4, (2005)).

'Section CB 3.4 Security awareness

Principle: Users of the application should be made aware of the key elements of information security and why it is needed and understand their personal information security responsibilities.

Objective: The ensure users of the application apply security controls and prevent the security of information used in the application from being compromised

CD 3.4.4 User of the application should be made aware that they are prohibited from:

k) Tampering with evidence in the case of the incidents that may require investigations.'

'Section CB 5.3 Information risk analysis

Principle: The application should be subject to a structured information risk analysis on a regular basis, the results of which should be documented, reviewed, and agreed by the application 'owner'.

Objective: To identify key information risks associated with the application and determine the security controls required in order to keep those risks within acceptable limits.

CB 3.5 The risk analysis process should help organizations to:

a) Select security controls that will reduce the likelihood of serious incidents occurring.' ((ISF IS), CB 3.4, (2005)).

'Section CB 6.1 Third party agreements

Principle: Connections from third parties(i.e. external organization, such as customers, suppliers and members of the public) should be subject to a risk assessment, approved by the application 'owner' and agreed by both parties in a documented agreement, such as a contract.

Objective: To ensure that only agreed and approved third partied gain access to the application.

CB 6.1.3 The provision of third party access should be supported by documented agreements, 'signed off' by the application 'owner'. Agreements should oblige third parties to comply with good practice for information security and provide information about security incidents.' ((ISF IS), CB 6.1, (2005)).

'CB6.1.4 Third party agreement should include:

b) Arrangements for managing changes and incidents' ((ISF IS), CB 6.1, (2005)).

'Section CI 2.2 Event logging

Principle: Logs of all key events within the computer installation should be maintained (preferably using automated tools), reviewed periodically and protected and protected against unauthorized change.

Objective: To ensure individual accountability and to enable incidents, such as access violations, to be investigated and resolved.' ((ISF IS), CI 2.2, (2005)).

'Section CI 2.6 Hazard protection

Principle: Computer equipment and facilities should be protected against fire, flood, environmental, and other natural hazards.

Objective: To prevent services being disrupted by damage to computer equipment facilities.

CI 2.6.4 The impact of hazards should be minimized by:

a) Located hand-held fire extinguishers so that minor incidents can be tackled without delay.' ((ISF IS), CI 2.6, (2005)).

'Area CI 3 System Operation

Achieving service targets require computer installations to be run in accordance with sound disciplines. Accordingly this area covers basic controls over system operation (i.e. handling computer media, back-up, and change management) and arrangements for identifying and resolving incidents (i.e. incident management and emergency fixes).' ((ISF IS), CI 3.1, (2005)).

'Section CI 3.4 Incident Management

Principle: All incidents of any type should be recorded, reviewed, and resolved using an incident management process.

Objective: To identify and resolve incidents effectively, minimize their business impact, and reduce the risk of similar incidents occurring.

CI 3.4.1 All incidents that affect the installation (including third party attack, internal misuse/abuse, malfunctions, loss of power/communications services, overloads and mistakes by users or computer staff) should be dealt with in accordance with an incident management process.

CI 3.4.2 The incident management process should be documented and cover reporting and recording of incidents, investigating and resolving incidents, reviewing patterns of incidents and escalation processes.

CI 3.4.3 Incidents should be:

a) Reported to a single point of contact, such as a help desk, telephone hot line or individual IT specialist

b) Documented, typically using an automated incident management system

c) Categorized by type (i.e. malfunctions, malicious attack or internal abuse/misuse of systems)

d) Prioritized according to their impact/urgency.

CI 3.4.4 The business impact of significant incidents should be assessed by an IT specialist, the 'owner' of an application supported by the installation and an information security specialist.

CI 3.4.5 The resolution of incidents should include:

a) Investigating their root causes

b) Planning corrective action to ensure security is not affected

c) Restricting access when corrective actions are performed

d) Documenting corrective actions taken

e) Performing a review to ensure that the security of the installation has not been affected by the incident or its resolution.

CI 3.4.6 Patterns of incidents should be reviewed to identify potential security breaches and minimize the chances of similar incidents disrupting the installation – or other installations – in the future.' ((ISF IS), CI 3.4, (2005)).

'Section CI 4.1 Access control arrangements

Principle: Access control arrangements should be established to restrict access by al types of user to approved system capabilities of the computer installation.

Objective: To ensure that only authorized individuals gain access to information or systems within the computer installation, and that individual accountability is assured.

CI 4.1.4 Access control arrangements should:

g) Upgraded in response to new threats, capabilities, business requirements or experience of incidents.' ((ISF IS), CI 4.1, (2005)).

'Section CI 5.2 Security awareness

Principle: Staff running the installation should be made aware of the key elements of information security and why it is needed, and understand their personal information security responsibilities.

CI 5.2.4 Staff employed in the computer installation should be made aware that they are prohibited from:

j) Tampering with evidence in the case of incidents that may require forensic investigation' ((ISF IS), CI 5.2, (2005)).

'Section CI 5.4 Information risk analysis

Principle: The computer installation should be subject to a structured information risk analysis on a regular basic the results f which should be documented, reviewed, and agreed by the installation 'owner'.

Objective: To identify key information risk associated with the computer installation and determine the security controls required in order to keep those risks within acceptable limits.

CI 5.4.6 The risk analysis should help organizations to:

a) Select the security controls that will reduce the likelihood of serious incidents occurring.' ((ISF IS), CI 5.4, (2005)).

'Area NW 3 Network Operations

Maintaining continuity of service of users requires computer networks to be run in accordance with sound disciplines. Accordingly, this area covers the arrangements needed to monitor network performance and to manage changes and incidents. In addition, the area covers the arrangements required to provide physical security, take backups and ensure service continuity.' ((ISF IS), NW 3.1 (2005)).

'Section NW 3.3 Incident management

Principle: All network incidents of any type should be recorded, reviewed, and resolved using an incident management process.

Objective: To identify and resolve network incidents effectively, minimize their business impact and reduce the risk of similar incidents occurring.

NW 3.3.1 All incidents that affect the network (including third party attack, internal misuse/abuse, malfunctions, loss of power/communications services, overloads and mistakes by users or computer staff) should be dealt with in accordance with an incident management process.

NW 3.3.2 The incident management process should be documented and cover reporting and recording of incidents, investigating and resolving incidents, reviewing patterns of incidents and escalation processes.

NW 3.3.3 Network incidents should be:

a) Reported to a single point of contact, such as a help desk, telephone hotline or individual IT specialist

b) Documented, typically using an automated incident management system

c) Categorized by type (e.g. malfunctions, malicious attack or internal abuse/misuse of the network)

d) Prioritized according to their impact/urgency.

NW 3.3.4 The business impact of significant network incidents should be assessed by a network specialist, the network 'owner', 'owners' of the applications supported by the network and an information security specialist.

NW 3.3.5 The resolution of network incidents should include:

a) Investigating their root causes

b) Planning corrective action to ensure security is not affected

c) Restricting access when corrective actions are performed

d) Documenting corrective actions taken

e) Performing a review to ensure that the security of the network has not been affected by the incident or its resolution.

NW 3.3.6 Patterns of network incidents should be reviewed to identify potential security breaches and minimize the chances of similar incidents disrupting the network – or other networks – in the future.' ((ISF IS), NW 3.3, (2005)).

'Section NW 4.2 Security Awareness

Principle: Network staff should be made aware of the key elements of information security and why it is needed and understand their personal information security responsibilities.

Objective: To ensure the network staff apply security controls and prevent the security of information transmitted across the network from being compromised.

NW 4.2.4 Network staff should be made aware that they are prohibited from:

j) Tampering with evidence in the case of incidents that may require forensic investigations.' ((ISF IS), NW 4.2, (2005)).

'Section NW 4.4 Information risk analysis

Principle: The network should be subject to a structured information risk analysis on a regular basis, the results of which should be documented, reviewed, and agreed by the network 'owner'.

Objective: To identify key information risks associated with the network and determine the security controls required in order to keep those risks within acceptable limits.

NW 4.4.6 The risk analysis should help organizations to:

3. Select the security controls that will reduce the likelihood of serious incidents' ((ISF IS), NW 4.4, (2005)).

'Section SD 2.2 Security awareness

Principle: Systems development staff should be made aware of the key elements of information security and why it is needed, and understands their personal information security responsibilities.

Objective: To ensure that systems development staff apply security controls and prevent the security of information used in development activities from being compromised.

SD 2.2.4 Development staff should be made aware that they are prohibited from:

j) Tampering with evidence in the case of incidents that may require forensic investigation' ((ISF IS), SD 2.2, (2005)).

'Section SD 3.5 Information Risk Analysis

Principle: Systems under development should be subject to a structured information risk analysis, the results of which should be documented, reviewed and agreed by the business owner.

Objective: To identify key risks associated with systems under development and determine the security controls required in order to keep those risks within acceptable limits. ((ISF IS), SD 3.5, (2005)).

SD 3.5.6 The risk analysis should help organizations to:

a) Select the security controls that will reduce the likelihood of serious incidents occurring'

'Section SD 6.3 Post-implementation review

Principle: Post-implementation reviews should be conducted for all new systems.

Objective: To check that systems and information security controls function as needed.

SD 6.3.2 Post-implementation reviews should be conducted for all new systems.

c) Security incidents' ((ISF IS), SD 6.3, (2005)).

The next framework analyzed is The Control Objectives for Information and Related Technology (COBIT). 'COBIT has been developed as a general accepted standard for good Information Technology (IT) security and control practices that provides a reference framework for management, users, and IS audit, control, and security practitioners. The COBIT framework is broken down into four domains: planning and organization (PO), acquire and implement (AI), deliver and support (DS), and monitor and evaluate (ME).' (www.isaca.org). Within each domain, are control objectives with detailed control processes. Under the deliver and support

domain is where incident response high level and low level control objectives and control processes reside:

'DS10-Manage Problems and Incidents

Control over the IT process of managing problems and incidents that satisfies the business requirement to ensure that problems and incidents are resolved, and the cause investigated to prevent any recurrence is enabled by a problem management system that records and progresses all incidents and takes into consideration:

- Audit trails of problems and solutions
- Timely resolution of reported problems
- Escalation procedures
- Incident reports
- Accessibility of configuration information
- Supplier responsibilities
- Coordination with change management

Control Objective: 1 -10.1. Problem Management System

Description: IT management should define and implement a problem management system to ensure that all operational events that are not part of the standard operation (incidents, problems, and errors) are recorded, analyzed, and resolved in a timely manner. Emergency program change procedures should be promptly tested, documented, approved, and reported. Incidents reports should be established in the case of significant problems.

Control Practices:

1. The requirements for a problem management system are identified by the IT management through consultation with the business, and a system is implemented and maintained to ensure that events that are not part of standard operations are recorded, analyzed, and resolved in a timely manner.

2. Clear, unambiguous procedures are in place to ensure that there is a standard method for categorizing, prioritizing, recording, maintaining, and managing different types of incidents and problems. The procedures are clearly communicated throughout the organization, with the appropriate personnel receiving training, as required. Procedures are assessed periodically and enhanced as appropriate.

3. The roles and responsibilities for addressing problems and incidents are defined and assigned. The required skills for this task are available to the organization through internal resources and/or external service providers. An incident/problem manager is responsible for managing the work of the support staff, monitoring the efficiency and the effectiveness of the problem management system and developing and maintaining the problem management system. The work of the manager and the support staff is assessed through actual performance being compared to service level agreements.

4. The problem management system identified appropriate approaches for the timely addressing of incidents and the analysis of underlying causes.

5. The problem management system is periodically reviewed by management to identify potential areas of increased effectiveness and efficiency and to ensure that it continues to meet business requirements.

6. The problem management system provides for a clear, predefined classification of problems and incidents, so consideration of priorities and problem areas can be determine in a structured way.

7. The problem management system provides for an incident report procedures for critical events and communication to the affected users.

8. The problem management system is in line with the other IT processes, especially for AI6 Manage Changes, DS9 Manage the Configuration, and DS13 Management Operations.

Control Objective 2- 10.2. Problem Escalation

Description: IT Management should define and implement problem escalation procedures to ensure that identified problems are solved in the most efficient way on a timely basis. These procedures should ensure that these priorities are appropriately set. The procedures should also document the escalation process for the activation of the IT continuity plan.

Control Practices:

1. Appropriate escalation procedures are defined and implemented by IT management through consultation with business units, including consideration of the role of

external service providers. The authorizations, roles, and responsibilities for escalating problems are clearly defined and assigned.

2. There is a coding system for categorization, based on the type of problem incident (i.e. server or workstation) to facilitate identification of the possible cause and the assignment of support staff to the problem. The priority of a problem or incident is based on the impact of the problem on the business (i.e. number of roles of affected users) and the urgency to the business with which a resolution is needed.
3. Procedures are in place to ensure a correct allocation of staff and resources to manage incidents and programs according to their classification and prioritization.
4. Procedures are in place for hierarchical escalation, if more effort or resources are needed, and for functional escalation, if other expertise is needed. For functional escalation, incidents are dispatched from first line (service desk) to second line (IT specialist) and, if applicable, to third line (external specialists and suppliers). The procedures include actions to be taken for problems that remain open for a long time, including escalation and rerouting.
5. Standard forms and work instruction are available for frequent incidents so they can be solved in an efficient and standardized way (i.e. password resets).
6. The problem escalation process is communicated widely to ensure all appropriate parties understand it. Communication protocols support the timely notification of problems to all affected users.
7. IT management is notified of a high-impact incident, i.e., the impact on users is extreme or disruption can be excessive. The IT manager arranges a formal meeting

with all parties involved (key support staff, vendor support staff, business management, etc) to determine the best course of action.

8. Action and decision made during escalation are recorded in the problem management system. The configuration management database (CMDB) is accessible to assist in analyzing and diagnosing cause and to determine the impact and urgency of a problem or incident.
9. The problem escalation process is periodically reviewed by management or skilled auditors to identify potential areas for increased effective ness and efficiency and to ensure that the process still meets business requirements.

Control Objective: 3- 10.3 Problem Tracking and Audit Trail

Description: The problem management system should provide for adequate audit trail facilities that allow tracking from incident to underlying cause (i.e. package release or urgent change implementation) and back. It should work closely with change management, availability management, and configuration management.

Control Practices

1. All reported problems and incidents are recorded in an automated tool (application) with information captured including, but not limited to, type (i.e. hardware, software) status (i.e. new, assigned, escalated, closed) and the incident/problem owner.
2. Support staff reacts only to incident and problems that are notified to them through agreed channels.

3. Details of closed problems or incidents are recorded in the organization's problem management system.
4. Sufficient staff and resources are available to prevent handling of the underlying problems taking second place to ad hoc incident handling.
5. The status of a problem or incident is reported to the affected users. Involved support personnel can access relevant information in the problem management system on a need-to-know basis.
6. A history of problem ticket modification is available, i.e. status change, priority change, time spent on escalation.
7. The problem management application is capable of appropriate statistics and trends reporting for senior management.
8. Support contracts and service level agreements are in place with vendors to ensure appropriate input to the problem tracking and resolution process.
9. Fault detection mechanisms are implemented on systems and network components for automatic incident logging and alerting.
10. Diagnostic tools are available for effectively diagnosing the cause of the problem or incident.

Control Objective: 4- 10.4. Emergency and Temporary Access Authorizations

Description: Emergency and temporary access authorizations should be documented on standard forms and maintained on file, approved by appropriate managers, securely communicated to the security function and automatically terminated after a predetermined period.

Control Practices:

1. The procedures for emergency and temporary access authorization are clearly defined, properly documented, supported, and approved by management.
2. The responsibility for approval of emergency and temporary access authorizations is clearly defined, properly documented, and supported by management.
3. Automatic detailed logging and authorization changes, including start/finish times and actions taken, are implemented and subject to regular independent reviews.
4. Emergency and temporary access authorization are monitored for accuracy and effectiveness, reported to and analyzed by the security function and appropriate management, and regularly updated with the results from the analysis.
5. Mechanisms are in place to automatically remove emergency and temporary access authorizations immediately after the associated problem is solved.
6. The emergency and temporary access authorization matrix (roles and responsibilities chart) is updated for personnel changes.

Control Objective: 5- 10.5. Emergency Processing Priorities

Description: Emergency processing priorities should be established, documented, and approved by appropriate program and IT management.

Control Practices:

1. Priority resolution criteria are defined to achieve the proper attention to emergency processing requirements. Priority criteria are documented and approved.
2. Simple and easy-to-use procedures and standard forms are available for quick and effective response to emergency incidents.

3. Required support staff, including specialists and management, has been identified and procedures established to ensure that staff is available in case of an emergency incident.
4. Actions taken to manage emergency incidents are manually documented in the problem management system is not readily available, with retrospective updating of the system at the earliest opportunity.

The management of emergency incidents is reviewed and evaluated, and lesson learned are used to improve the emergency response procedures.' ((COBIT), DS10, (2005)).

'DS5- Ensure Systems Security

Control over the IT process of ensuring systems security that satisfies the business requirement to safeguard information against unauthorized use, disclosure or modification, damage or loss is enabled by logical access controls that ensure that access to systems, data and programs is restricted to authorized users and takes into consideration:

- Confidentiality and privacy requirements
- Authorization, authentication and access control
- User identification and authorization profiles
- Need-to-have and need-to-know
- Cryptographic key management
- Incident handling, reporting and follow-up
- Virus prevention and detection
- Firewalls
- Centralized security administration

- User training
- Tools for monitoring compliance, intrusion testing and reporting

Control Objective 6- 5.11 Incident Handling

Description: Management should establish a computer security incident handling capability to address security incidents by providing a centralized platform with sufficient expertise and equipped with rapid and secure communication facilities. Incident management responsibilities and procedures should be established to ensure an appropriate, effective and timely response to security incidents.

Control Practices:

1. Reported security incidents (breaches) are reviewed promptly by a central team with sufficient expertise to minimize damage and find/eliminate the root cause for the security breach.

2. Management is informed of all significant security breaches.

3. There is an adequately communicated formal disciplinary process for employees who are found to have violated organizational security policies and procedures; employees and contractors are made aware of this process.' ((COBIT), DS5, (2005)).

'COSO is a private sector initiative established in 1985 by five financial professional associations. COSO's goal is to improve the quality of financial reporting through a focus on corporate governance, ethical practices, and internal control.' (http://www.coso.org). COSO is a popular framework that corresponds/maps to the COBIT framework. The two frameworks do

not map 100%, but, they are the most acceptable frameworks used in the commercial sector, so the mapping that does exist, is used on a frequent basis. The COSO framework is divided into five domains: Control Environment, Risk Assessment, Control Activities, Information and, Communications, and Monitoring. 'The first domain, Control Environment, creates the foundation for effective internal control, establishes the "tone at the top" and represents the apex of the corporate governance structure. The issues raised in the control environment component apply throughout an organization. The second domain, Risk Assessment, involves the identification and analysis by management of relevant risks to achieve predetermined objectives, which form the basis for determining control activities. It is likely that internal control risks could be more pervasive in the IT organization than in other areas of the organization. Risk Assessment may occur at the company level (for the overall organization) or at the activity level (for a specific process or business unit). The Control Environment primarily addresses the company level. The third domain, Control Activities, are the policies, procedures and practices that are put into place to ensure that business objectives are achieved and risk mitigation strategies are carried out. Control Activities are developed to specifically address each control objective to mitigate the risks identified. COSO states that information is needed at all levels of an organization to run the business and achieve the entity's control objectives. However, the identification, management and communication of relevant information represent an ever-increasing challenge to the IT department. The determination of which information is required to achieve control objectives, and the communication of this information in a form and time frame that allow people to carry out their duties, support the other four components of the COSO framework. The last domain, Monitoring, which covers the oversight of internal control by management through continuous and point-in-time assessment processes, is becoming

increasingly important to IT management.' (www.itgi.org). There are two types of monitoring activities: continuous monitoring and separate evaluations. From the above incident response/forensic COBIT mappings, the following COSO domains map accordingly:

COBIT Control Objectives	COSO Domains
DS10-Manage Problems and Incidents	Control Activities, Information and Communication, and Monitoring
Control Objective: 1 -10.1. Problem Management System	Control Activities, Information and Communication, and Monitoring
Control Objective 2- 10.2. Problem Escalation	Control Activities, Information and Communication, and Monitoring
Control Objective: 3- 10.3 Problem Tracking and Audit Trail	Control Activities, Information and Communication, and Monitoring
Control Objective: 4- 10.4. Emergency and Temporary Access Authorizations	Control Activities, Information and Communication, and Monitoring
Control Objective: 5- 10.5. Emergency	Control Activities, Information and Communication, and Monitoring

Processing Priorities	
Control Objective 6- 5.11- Incident Handling	Control Activities, Information and Communication, and Monitoring

The last guidance researched for this matrix is the Payment Card Industry requirements. With the every increasing rise of identify theft, the credit card industry have created their own set of security requirements. 'The new Payment Card Industry (PCI) Data Security Standard outlines best practices for credit card data that is stored, processed, or transmitted. It consolidates and supersedes the requirements of the previously developed MasterCard Site Data Protection (SDP) Program and the Visa Cardholder Information Security Program (CISP). As such, the new standard contains IT security requirements and guidelines for all major credit card issuers, including Visa, MasterCard, American Express, Diners Club and Discover. These card issuers joined forces to develop the new requirements as part of an industry-wide standard for protection of cardholders' credit card account and transaction information.' ('Columbitech' 2005).

'Maintain an Information Security

12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.

12.9.1 Create an incident response plan to be used in the event of system compromise. Ensure the plan addresses, at a minimum, specific response procedures, business recovery and continuity

procedures, data backup processes, roles and responsibilities, and communication and contact strategies (i.e. informing Acquirers and credit card associations).

12.9.2 Test the plan at least annually.

12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to compromise alerts.

12.9.4 Provide appropriate training to staff with security breach response responsibilities.

12.9.5 Include alerts from intrusion, detection, intrusion prevention, and file integrity monitoring systems.

12.9.6 Have a process to modify and evolve the incident response plan according to lessons learned to incorporate industry developments.' (PCI, pages 50-51).

Now that the relevant requirements have been identified, a common language must be created in order to map the regulations, standards, frameworks, guidances, and requirements effectively. The tables below note the common language requirements and the detailed mappings.

Incident response /computer forensic/privacy requirements	FFIEC	ISO 17799:2005	SOX	HIPAA	GLBA
1. Incident response and computer forensics definitions are documented in the Information Security (IS) Policy,	Intrusion Detection and response;	5.1.1	Sections 301, 302, 404,	164.308(a)(6) Response and Reporting-R, 164.308(a)(1) Information Systems Activity Review-R	16 CFR Part 314.1, 314.2(c), 314.3(a) Manage and Control Risk

SOP's, internal controls, etc.	pages 68-75 , Appendix A		409, and 806		
2. The IS Policy should be reviewed whenever the organization's infrastructure/environment changes.	Intrusion Detection and response; pages 68-75, Appendix A	5.1.2	Sections 301, 302, 404, 409, and 806	164.308(a)(6) Response and Reporting-R, 164.308(a)(1) Information Systems Activity Review-R	16 CFR Part 314.1, 314.2(c), 314.3(a) Manage and Control Risk
3. Organizations should keep open communication with external security entities (i.e., LE, special interest groups, and customers') when an incident occurs.	Intrusion Detection and response; pages 68-75, Appendix A	6.1, 6.1.6, 6.1.7	Sections 301, 302, 404, 409, and 806	164.308(a)(6) Response and Reporting-R, 164.308(a)(1) Information Systems Activity Review-R	16 CFR Part 314.1, 314.2(c), 314.3(a) Manage and Control Risk
4. Incident response/forensic activities should be multi-disciplinary, with cooperation	Intrusion Detection and	6.1.2	Sections 301, 302,	164.308(a)(6) Response and Reporting-R, 164.308(a)(1) Information Systems Activity	16 CFR Part 314.1, 314.2(c), 314.3(a) Manage and

throughout the organization.	response; pages 68-75, Appendix A		404, 409, and 806	Review-R	Control Risk
5. All security requirements should be documented, monitored, and reviewed before granting access to external entities, third parties, and/or contractors. Only relevant/pertinent access should be granted to external entities when helping with an incident/forensics.	Intrusion Detection and response; pages 68-75, Service Provider Oversight; pages 64-66, Logical and Admin, Appendix A Access Control; pages 15-	6.2.1., 6.2.2, 6.2.3	Sections 301, 302, 404, 409, and 806	164.308(a)(6) Response and Reporting-R, 164.308(a)(1) Information Systems Activity Review-R	16 CFR Part 314.1, 314.2(c), 314.3(a) Manage and Control Risk

	38, Appendix A				
6. Management is responsible for any change regarding third parties, contracts, and the in-house IS policy.	Intrusion Detection and response; pages 68-75, Appendix A	6.2.1, 6.2.2, 6.2.3, 10.8.2	Sections 301, 302, 404, 409, and 806	164.308(a)(6) Response and Reporting-R, 164.308(a)(1) Information Systems Activity Review-R	16 CFR Part 314.1, 314.2(c), 314.3(a) Manage and Control Risk
7. Legal requirements and consequences, including incident/forensic definitions, should be taken into account when logging and monitoring pertinent information for investigations/forensics.	Intrusion Detection and response; pages 68-75, Logging and Data Collection; pages 64-66, Appendix	10.2.2, 10.2.3, 10.10.2	Sections 301, 302, 404, 409, 802, and 806	164.308(a)(6) Response and Reporting-R, 164.308(a)(1) Information Systems Activity Review-R	16 CFR Part 314.1, 314.2(c), 314.3(a) Manage and Control Risk

	A				
8. Each incident should be evaluated (risk assessment) when contemplating its vulnerability to the organization.	Intrusion Detection and response; pages 68-75, Appendix A	12.6.1	Sections 301, 302, 404, 409, and 806	164.308(a)(6) Response and Reporting-R, 164.308(a)(1) Information Systems Activity Review-R	16 CFR Part 314.1, 314.2(c), 314.3(a) Manage and Control Risk
9. Reporting of security breaches should be documented and channeled through management.	Intrusion Detection and response; pages 68-75, Appendix A	13.1.1, 13.1.2	Sections 301, 302, 404, 409, 802 and 806	164.308(a)(6) Response and Reporting-R, 164.308(a)(1) Information Systems Activity Review-R	16 CFR Part 314.1, 314.2(c), 314.3(a) Manage and Control Risk
10. All roles and responsibilities are defined and documented in regards to incident response/investigations/forensics.	Intrusion Detection and response;	13.2.1	Sections 301, 302, 404,	164.308(a)(6) Response and Reporting-R, 164.308(a)(1) Information Systems Activity Review-R	16 CFR Part 314.1, 314.2(c), 314.3(a) Manage and Control Risk

	pages 68-75, Appendix A		409, and 806		
11. Evidence collection, traceability, testing, preservation, and retention should be documented and follow the legal statues in place. Evidence collection, testing, backups, etc should be documented in a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) as well.	Intrusion Detection and response; pages 68-75, BCP page 74, Electronic and Paper Media Handling, pages 62-64, Appendix A	12.2.3, 14.1.1, 14.1.4, 14.1.5	Sections 301, 302, 404, 409, and 806	164.308(a)(6) Response and Reporting-R, 164.308(a)(1) Information Systems Activity Review-R	16 CFR Part 314.1, 314.2(c), 314.3(a) Manage and Control Risk
12. Security awareness and training/lessons learned are necessary for the entire organization and not only for	Intrusion Detection and response;	8.2.1, 13.2.2	Sections 301, 302, 404,	164.308(a)(6) Response and Reporting-R, 164.308(a)(1) Information Systems Activity Review-R	16 CFR Part 314.1, 314.2(c), 314.3(a) Manage and Control Risk

members of the investigative/forensic process.	pages 68-75, Appendix A		409, and 806		
13. Physical security must be taken into account in regards to detecting an incident but also to safeguard forensic evidence.	Intrusion Detection and response; pages 68-75, Physical Security pages 44-48, Appendix A	13.1.2	Sections 301, 302, 404, 409, 802 and 806	164.308(a)(6) Response and Reporting-R, 164.308(a)(1) Information Systems Activity Review-R	16 CFR Part 314.1, 314.2(c), 314.3(a) Manage and Control Risk
14. Organizations should consider the possibility of insurance in regards to security breaches, etc.	Intrusion Detection and response; pages 68-75, Insurance;	6.1.2	Sections 301, 302, 404, 409, 802, and 806	164.308(a)(6) Response and Reporting-R, 164.308(a)(1) Information Systems Activity Review-R	16 CFR Part 314.1, 314.2(c), 314.3(a) Manage and Control Risk

	pages 75-77				
15. Media disposal (after the fact) should be consistent and disposed of only after the designated timeframe.	Intrusion Detection and response; pages 68-75, Appendix A	12.2.3	Section 802	164.308(a)(6) Response and Reporting-R, 164.308(a)(1) Information Systems Activity Review-R	16 CFR Part 314.1, 314.2(c), 314.3(a) Manage and Control Risk

Figure 1 Detailed mapping to standards and regulations

Incident response /computer forensic/privacy requirements	CA SB 1386/ NY AB 4254	COBIT	COSO	Basel II	PCI	ISF v 4.1
1. Incident response and computer forensics definitions are documented in the Information Security (IS) Policy, SOP's, internal controls, etc.	X	DS10.1, DS10.2, DS 10.3, DS 10.4,	CA, IC, M	P14	12.9.1, 12.9.6	SM5.5, CB2.4.1 and CB2.4, CI3.4 and CI3.4.2,

		DS 10.5				NW3.3
2. The IS Policy should be reviewed whenever the organization's infrastructure/environment changes.	X	DS10.1, DS10.2, DS 10.3, DS 10.4, DS 10.5	CA, IC, M		12.9.1, 12.9.6	SM5.5, CB2.4.1 and CB2.4.2, CI3.4 and CI3.4.2, NW3.3
3. Organizations should keep open communication with external security entities (i.e., LE, special interest groups, and customers') when an incident occurs.	X	DS10.1, DS10.5	CA, IC, M	P14	12.9.1	CB2.4.2
4. Incident response/forensic activities should be multi-disciplinary, with cooperation throughout the organization.	X	DS10.5	CA, IC, M	P14	12.9.1	SM5.5, CB2.4.1 and CB2.4, CI3.4 and CI3.4.2, NW3.3
5. All security requirements should be documented,	X	DS10.1, DS10.4	CA, IC, M	P14	12.9.6	CB12.2, CB2.4.3,

monitored, and reviewed before granting access to external entities, third parties, and/or contractors. Only relevant/pertinent access should be granted to external entities when helping with an incident/forensics.						CB6.1
6. Management is responsible for any change regarding third parties, contracts, and the in-house IS policy.	X	DS10.1, DS10.2	CA, IC, M	P14	12.9.6	CI3.4, NW3.3, CB2.4, and SM5.5
7. Legal requirements and consequences, including incident/forensic definitions, should be taken into account when logging and monitoring pertinent information for investigations/forensics.		DS10.1, DS10.2	CA, IC, M	P14	12.9.4, 12.9.5	SM5.5.5, SM7.2, CI2.2
8. Each incident should be evaluated (risk assessment) when contemplating its vulnerability to the organization.		DS10.1, DS10.2	CA, IC, M	P14	12.9.1	CB2.4.3. CD2.4.4, CI5.4 and

						CI5.4.6, NW4.4 and NW 4.4.6, SD 3.5 and SD 3.5.6
9. Reporting of security breaches should be documented and channeled through management.	X	DS10.1, DS10.2	CA, IC, M	P14	12.9.1	CI3.4, NW3.3, CB2.4, and SM5.5
10. All roles and responsibilities are defined and documented in regards to incident response/investigations/forensics.	X	DS10.1, DS10.2	CA, IC, M	P14	12.9.3	CI3.4, NW3.3, CB2.4, and SM5.5
11. Evidence collection, traceability, testing, preservation, and retention should be documented and follow the legal statues in place. Evidence collection, testing, backups, etc should be documented in a Business Continuity Plan (BCP)	X	DS10.2	CA, IC, M	P14	12.9.1, 12.9.2, 12.9.5	SM5.5.2 and SM5.5.3

and Disaster Recovery Plan (DRP) as well.						
12. Security awareness and training/lessons learned are necessary for the entire organization and not only for members of the investigative/forensic process.	X	DS10.1, DS10.5	CA, IC, M		12.9.4	SM2.4.1, SM2.4.4, CB3.4, NW4.2, SD2.2, CI5.2
13. Physical security must be taken into account in regards to detecting an incident but also to safeguard forensic evidence.						CI2.6
14. Organizations should consider the possibility of insurance in regards to security breaches, etc.						
15. Media disposal (after the fact) should be consistent and disposed of only after the designated timeframe.						CI3, SM5.5.4

Figure 2 Detailed mappings to frameworks, guidances, and requirements

Now that the requirements have been identified and mapped, a high level policy can be created that should give organizations the confidence that the common language requirements

created sufficiently map to existing regulations, standards, frameworks, and guidances. Not only can organizations pass the mandatory audits for certain regulations, but also, their policies, processes, and procedures will help them when creating, documenting, and possibly prosecuting an incident.

COMPANY ABC Incident Response/Forensic Policy; version 1

Purpose and objectives of the policy: To create a repeatable, effective incident response/forensic policy that maps to regulations, standards, and frameworks as well as to the organization's Standard Operating Procedures (SOP's) and processes.

Scope of the policy (to whom and what it applies and under what circumstances): This policy applies to all individuals under the Information Security, Threat Management, Compliance, Legal, Corporate Security, and Ethic Departments.

Definition of computer security incidents and their consequences within the context of the organization: A computer security incident will be classified by performing a risk assessment on the suspect activity or a reported claim of fraudulent activity. Dependent on the classification of the incident, the extent of the damage or liability, as well as previous documented incidents by the same individual or organization will determine the level of action taken.

Defined incident response/forensic requirements:

Requirement/Policy statements: Incident response and computer forensics definitions are documented in the Information Security (IS) Policy, SOP's, internal controls, etc. This Policy should be reviewed whenever the organizations infrastructure/environment changes.

Requirement/Policy statements: Each incident should be evaluated (risk assessment) when contemplating its vulnerable to the organization.

Requirement/Policy statements: All roles and responsibilities are defined and documented in regards to incident response/investigations/forensics. Each incident should be evaluated (risk assessment) when contemplating its vulnerable to the organization. Reporting of security breaches should be documented and channeled through management. Organization should consider the possibility of insurance in regards to security breaches, etc.

Requirement/Policy Statements: Organizations should keep open communication with external security entities (i.e., LE, special interest groups). Incident response/forensic activities should be multi-disciplinary, with cooperation throughout the organization. All security requirements should be documented, monitored, and reviewed before granting access to external entities, third parties, and/or contractors. Legal requirements and consequences, including incident/forensic definitions, should be taken into account when logging and monitoring pertinent information for investigations/forensics. Evidence collection, traceability, testing, preservation, and retention should be documented and followed the legal statues in place. Evidence collection, testing, backups, etc should be documented in a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) as well. Only relevant/pertinent access should be granted to external entities when helping with an incident/forensics. Media disposal (after the fact) should be consistent and disposed of only after the designated timeframe.

Incident Response/Forensics Steps to Evidence Collection/Analysis/Retention: Physical Security Requirement/Policy Statements Requirement/Policy Statements: Physical security must be taken into account not only to detect an incident but also to safeguard forensic evidence.

Security Awareness and Training: Requirement/Policy Statement: Security awareness and training/lessons learned are necessary for the entire organization and not only for members of the investigative/forensic process.

In conclusion, this proposed thesis has demonstrated that a high-level incident response/forensic policy should start with an understanding of the current regulations, standards, and frameworks relevant to the organization's vertical. In addition, commonalities between such regulations, standards, and frameworks should be analyzed and condensed to create a common language that can be used to create a high level policy that will uphold during an assessment and/or audit for compliance.

References/Copyright

1. Hoffman, Mark. *A Standard of Information Security Management Info- Tech White Papers.* 2003.
2. Hoffman, Mark. *A Standard of Information Security Management Info- Tech White Papers.* 2003.
3. Hoffman, Mark. *A Standard of Information Security Management Info- Tech White Papers.* 2003.
4. Information Technology Security Techniques Code of Practice for information security management BS ISO/IEC 17799:2005, 7, (2005).
5. Information Technology Security Techniques Code of Practice for information security management BS ISO/IEC 17799:2005, 8, (2005).
6. Information Technology Security Techniques Code of Practice for information security management BS ISO/IEC 17799:2005, 9, (2005).
7. Information Technology Security Techniques Code of Practice for information security management BS ISO/IEC 17799:2005, 10, (2005).
8. Information Technology Security Techniques Code of Practice for information security management BS ISO/IEC 17799:2005, 12, (2005).
9. Information Technology Security Techniques Code of Practice for information security management BS ISO/IEC 17799:2005, 13, (2005).
10. Information Technology Security Techniques Code of Practice for information security management BS ISO/IEC 17799:2005, 14, (2005).
11. Information Technology Security Techniques Code of Practice for information security management BS ISO/IEC 17799:2005, 16, (2005).
12. Information Technology Security Techniques Code of Practice for information security management BS ISO/IEC 17799:2005, 17, (2005).

13. Information Technology Security Techniques Code of Practice for information security management BS ISO/IEC 17799:2005, 18, (2005).

14. Information Technology Security Techniques Code of Practice for information security management BS ISO/IEC 17799:2005, 26, (2005).

15. Information Technology Security Techniques Code of Practice for information security management BS ISO/IEC 17799:2005, 40, (2005).

16. Information Technology Security Techniques Code of Practice for information security management BS ISO/IEC 17799:2005, 41, (2005).

17. Information Technology Security Techniques Code of Practice for information security management BS ISO/IEC 17799:2005, 50, (2005).

18. Information Technology Security Techniques Code of Practice for information security management BS ISO/IEC 17799:2005, 67, (2005).

19. Information Technology Security Techniques Code of Practice for information security management BS ISO/IEC 17799:2005, 88, 90, (2005).

20. Information Technology Security Techniques Code of Practice for information security management BS ISO/IEC 17799:2005, 91, (2005).

21. Information Technology Security Techniques Code of Practice for information security management BS ISO/IEC 17799:2005, 92, (2005).

22. Information Technology Security Techniques Code of Practice for information security management BS ISO/IEC 17799:2005, 93, (2005).

23. Information Technology Security Techniques Code of Practice for information security management BS ISO/IEC 17799:2005, 94, (2005).

24. Information Technology Security Techniques Code of Practice for information security management BS ISO/IEC 17799:2005, 94, (2005).

25. Information Technology Security Techniques Code of Practice for information security management BS ISO/IEC 17799:2005, 95, (2005).

26. Information Technology Security Techniques Code of Practice for information security management BS ISO/IEC 17799:2005, 97, (2005).

27. Information Technology Security Techniques Code of Practice for information security management BS ISO/IEC 17799:2005, 98, (2005).

28. *The Federal Financial Institutions Examination Council's (FFIC) Web Site.* Retrieved November 6, 2005 from http://www.ffiec.gov/.

29. The Federal Financial Institutions Examination Council's Information Security Handbook (FFIEC), 28, (2002).

30. The Federal Financial Institutions Examination Council's Information Security Handbook, 45, (2002).

31. The Federal Financial Institutions Examination Council's Information Security Handbook, 64, (2002).

32. The Federal Financial Institutions Examination Council's Information Security Handbook, 65, (2002).

33. The Federal Financial Institutions Examination Council's Information Security Handbook, 66, (2002).

34. The Federal Financial Institutions Examination Council's Information Security Handbook, 66, (2002).

35. The Federal Financial Institutions Examination Council's Information Security Handbook, 67, (2002).

36. The Federal Financial Institutions Examination Council's Information Security Handbook, 74, (2002).

37. The Federal Financial Institutions Examination Council's Information Security Handbook, 76, (2002).

38. The Federal Financial Institutions Examination Council's Information Security Handbook, 77, (2002).

39. The Federal Financial Institutions Examination Council's Information Security Handbook, A-5, (2002).

40. The Federal Financial Institutions Examination Council's Information Security Handbook, A-7, (2002).

41. The Federal Financial Institutions Examination Council's Information Security Handbook, A-13, (2002).

42. The Federal Financial Institutions Examination Council's Information Security Handbook, A-15, (2002).

43. The Federal Financial Institutions Examination Council's Information Security Handbook, A-16, (2002).

44. The Federal Financial Institutions Examination Council's Information Security Handbook, A-17, (2002).

45. The Federal Financial Institutions Examination Council's Information Security Handbook, A-18, (2002).

46. The Federal Financial Institutions Examination Council's Information Security Handbook, A-19, (2002).

47. The Federal Financial Institutions Examination Council's Information Security Handbook, A-21, (2002).

48. Patzakis, J. (2003, September). *New Incident Response Best Practices Patch and Proceed is No Longer Acceptable Incident Response Procedures.* Retrieved November 6, 2003 from http://www.guidancesoftware.com/corporate/downloads/whitepapers/IRBestPractices.pdf

49. Baumler, J., Bradley, S., Brown, S., Filkins, B., Grenert, R.H., Gross, C., et al. (2004). *SANS Step-by-Step Series HIPAA Security Implementation Version 1.0.* US: SANS Press.

50. Baumler, J., Bradley, S., Brown, S., Filkins, B., Grenert, R.H., Gross, C., et al. (2004). *SANS Step-by-Step Series HIPAA Security Implementation Version 1.0.* US: SANS Press

51. *The Gramm-Leach Bliley Act.* Retrieved November 6, 2005 from http://www.ftc.gov/privacy/privacyinitiatives/glbact.html.

52. *The Gramm-Leach Bliley Act: The Safeguards Rule.* Retrieved November 6, 2005 from http://www.ftc.gov/privacy/privacyinitiatives/safeguards.html.

53. *Financial Institutions and Customer Data: Complying with the Safeguard Rule.* Retrieved November 6, 2005 from http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm

54. 'Technology Commentaries California Raises the Bar on Data Security and Privacy-The California Finan', Mondaq Business Briefing. 15 Sept. 2003.

55. 'Technology Commentaries California Raises the Bar on Data Security and Privacy-The California Finan', Mondaq Business Briefing. 15 Sept. 2003.

56. 'Technology Commentaries California Raises the Bar on Data Security and Privacy-The California Finan', Mondaq Business Briefing. 15 Sept. 2003.
57. "New York Enacts Data Security and Notification Law." Mondaq Business Briefing. 19 August 2005.

58. Limongelli, Victor, Patzakis, John. 'Internal Computer Investigations as a Critical Control Activity Under Sarbanes-Oxley.' March 2004. http://www.guidancesoftware.com.

59. Limongelli, Victor, Patzakis, John. 'Internal Computer Investigations as a Critical Control Activity Under Sarbanes-Oxley.' March 2004. http://www.guidancesoftware.com.
60. Limongelli, Victor, Patzakis, John. 'Internal Computer Investigations as a Critical Control Activity Under Sarbanes-Oxley.' March 2004. http://www.guidancesoftware.com.
61. Limongelli, Victor, Patzakis, John. 'Internal Computer Investigations as a Critical Control Activity Under Sarbanes-Oxley.' March 2004. http://www.guidancesoftware.com.
62. Limongelli, Victor, Patzakis, John. 'Internal Computer Investigations as a Critical Control Activity Under Sarbanes-Oxley.' March 2004. http://www.guidancesoftware.com.

63. The Standard for Good Practice for Information Security (ISF IS), 7, (2005).

64. The Standard for Good Practice for Information Security (ISF IS), 12, (2005).

65. The Standard for Good Practice for Information Security (ISF IS), 18, (2005).

66. The Standard for Good Practice for Information Security (ISF IS), 20, (2005).

67. The Standard for Good Practice for Information Security (ISF IS), 26, (2005).

68. The Standard for Good Practice for Information Security (ISF IS), SM 2.2, (2005).

69. The Standard for Good Practice for Information Security (ISF IS), SM 2.4, (2005).

70. The Standard for Good Practice for Information Security (ISF IS), SM 2.4, (2005).

71. The Standard for Good Practice for Information Security (ISF IS), SM 3.3, (2005).

72. The Standard for Good Practice for Information Security (ISF IS), SM 5.1, (2005).

73. The Standard for Good Practice for Information Security (ISF IS), SM 5.6, (2005).

74. The Standard for Good Practice for Information Security (ISF IS), SM 6.7, (2005).

75. The Standard for Good Practice for Information Security (ISF IS), SM 7.2, (2005).

76. The Standard for Good Practice for Information Security (ISF IS), CB 2.4, (2005).

77. The Standard for Good Practice for Information Security (ISF IS), CB 3.4, (2005).

78. The Standard for Good Practice for Information Security (ISF IS), CB 3.5, (2005).

79. The Standard for Good Practice for Information Security (ISF IS), CB 6.1, (2005).

80. The Standard for Good Practice for Information Security (ISF IS), CB 6.1, (2005).

81. The Standard for Good Practice for Information Security (ISF IS), CI 2.2, (2005).

82. The Standard for Good Practice for Information Security (ISF IS), CI 2.6, (2005).

83. The Standard for Good Practice for Information Security (ISF IS), CI 3.1, (2005).

84. The Standard for Good Practice for Information Security (ISF IS), CI 3.4, (2005).

85. The Standard for Good Practice for Information Security (ISF IS), CI 4.1, (2005).

86. The Standard for Good Practice for Information Security (ISF IS), CI 5.2, (2005).

87. The Standard for Good Practice for Information Security (ISF IS), CI 5.4, (2005).

88. The Standard for Good Practice for Information Security (ISF IS), NW 3.1, (2005).

89. The Standard for Good Practice for Information Security (ISF IS), NW 3.3, (2005).

90. The Standard for Good Practice for Information Security (ISF IS), NW 4.2, (2005).

91. The Standard for Good Practice for Information Security (ISF IS), NW 4.4, (2005).

92. The Standard for Good Practice for Information Security (ISF IS), SD 2.2, (2005).

93. The Standard for Good Practice for Information Security (ISF IS), SD 3.5, (2005).

94. The Standard for Good Practice for Information Security (ISF IS), SD 6.3, (2005).

95. *Control Objectives for Information and related Technology.* Retrieved on Feb. 5, 2006 from http://www.isaca.org.

96. Control Objectives for Information and related Technology (COBIT), DS10, (2005).

97. Control Objectives for Information and related Technology (COBIT), DS5, (2005).

98. *The Committee of Sponsoring Organizations of the Treadway Commission.* Retrieved Feb. 5, 2006 from http://www.coso.org.

99. *IT Goverance Institute.* Retrieved Feb. 5, 2006 from http://www.itgi.org.

100. 'Columbitech Offers End-to-End Wireless VPN Solution to Address Payment Card Industry Data Security Standards.' Business Wire. 25 May 2005.

101. Payment Card Industry Security Audit Procedure, 50-51, (2004).