Figure 1 - (CBSS, 2011)

REGULATORY COMPLIANCE LEVERAGING PLATFORM

BTECH 451A Mid-Year Report

Karthik Padullaparty
Kpad470 | 2224454

Academic Supervisor

Lech Janczewski
Associate Professor – Information Systems
Yun-Sing Koh
Senior Lecturer – Computer Science

Industry Mentor

Gabriel Akindeju
Managing Director – Risks Consult Limited

RCL
Business Technology Risk Management

TABLE OF CONTENTS

ABSTRACT

The aim of this research is to create a platform that will assist financial institutions comply with three main regulatory instruments while cutting their costs. In this research I outline the three main instruments I have focused namely Sarbanes-Oxley, Payment Card Industry Data Security Service and ISO 27002 and explained how they can be integrated into this platform along with my reasoning for my decisions. Towards the end of the report I have addressed different technologies that are possibilities for the back-end of this platform and the proposed technology with the reasoning behind my proposition. . Testing in the future would need to be done to determine whether the changes I propose have any impact on the financial institutions and their compliance costs.

Key Words

Information Security, Regulatory Compliance, Platform, ISO 27002, PCIDSS, SOX, HTML, PHP, MySQL, Impact Zones, 11 Essential Controls.

1 INTRODUCTION

Information is the lifeblood of organisations — a vital business asset in today's Information Technology–enabled world. Access to high-quality, complete, accurate and up-to-date information is crucial in supporting managerial decision-making processes that lead to sound decisions. Therefore, having secure information system resources is extremely important to ensure that the company resources are well protected.

With the assistance of an information security management system (ISMS), organisations are able to apply a set of policies that will help them construct, develop and maintain security for their computer systems, both hardware and software. These policies will dictate the use of these resources in the protection of sensitive data.

Information security is not simply protecting your data with a username and password, but a lot more. Most organisations are obligated to impose various privacy and data protection policies and regulations, as they are continuously threatened by worms, viruses, bugs, hackers, and so on. A hacker, also known as an unidentified user, can cause huge losses for organisations by merely altering bits of information, stealing customer/employee data or even pilfering business strategies and selling them to competitors.

Banking and Financial Institutions also require such standards to protect their systems as they are the most at risk. They hold sensitive information not only about their employees, but also about their customers. Financial information is very important to everyone and once compromised it could cost a lot for an organisation.

By comparing existing research and technologies, I will answer the business problem placed by Risk Consult Limited (RCL) and create a solution that will help organisations manage the security of their data. The solution will be presented as a platform that eliminates the recursive costs for a financial institution as well as provides guidelines on which part of their system is not compliant with a certain standard.

The structure of this report is organised as follows. Section 2 gives a small background about the company RCL and their objectives. In Section 3, I list the people who are and have been an integral part of this project and its success. Section 4 I outline the business problem given by RCL, with a proposed solution in Section 5. A brief analysis of the current research in the field of compliance and the technologies that are available similar to the solution I am proposing this report in mentioned in Section 6. I give a brief background into each of the regulatory instruments chosen in Section 7 and in Section 8 I complete a brief analysis and comparison of these instruments and how they tie into the platform. The penultimate section, Section 9, mentions briefly about the technologies I would like to use and implement in the platform. Finally to finish off, I wrap up this report with a timeline and what I have planned to complete in the future.

2 ABOUT RCL

Risk Consult Limited is a Business Technology Risks Management Consulting Practice (RCL, 2014).

It consists of a team of professionals who are Certified Information Systems & Security Professionals (CRISC, CISM, CISSP, CISA, SCF, & PRInCE II) with backgrounds in Information Systems Management, Engineering, System Architecture, Business Process Engineering and Project Management. They have extensive Technology Risk Management & Information Systems Security governance, management and architecture experience from both private and public corporate environments. They also have extensive experience in Financial and Business Audit Support, including but not limited to regulatory support, such as Sarbanes Oxley, BASEL I & II, HIPAA, Cloud Computing Standards, AIPAC SOCs, and so on, as well as industry standards such as ISO 2700x, and PCIDSS.

Their people are world-class, industry thought leaders who have been part of the Big4 Professional Services environment. They have also had the privilege of pioneering and setting up Information Systems Security and Control teams both within New Zealand and internationally.

They have continued to work with a broad understanding that technologies are not only implemented in businesses for the sake of themselves, but also to drive and deliver values. They also understand that these technologies can lead to value leakage if risks are not optimised. They have developed the best-in-breed technology risks optimisation approaches and concepts, and have helped businesses achieve both of these objectives.

Having helped many corporates achieve these objectives, they can help with any business technologies-related risk management activities, including but not limited to:

- Business technology risk assessment along the entire lifecycle of business technology assets from concepts through to asset decommissioning
- Information asset protection strategies, implementation and operations
- Business technology risk management strategies and implementations
- Information security architectures and frameworks – design, implementation and operations

3 PEOPLE INVOLVED

There are several people involved with this project, from either RCL or the University of Auckland. Here are some of the key people that were important to the success of this project.

- **Industry mentor: Gabriel Akindeju**
  Gabriel is the Managing Consulting Director for RCL, who has been assisting me and supporting me throughout this project in terms of both moral support and the resources provided.
- **Academic supervisor: Lech Janczewski**
  Lech is an Associate Professor at the University of Auckland specialising in Information Security. He has been key to my project in terms of the experience he possesses.
- **Academic supervisor: Yun Sing Koh**
  Yun Sing is a Senior Lecturer at the University of Auckland, who also is an expert in her field of data mining. I have kept in constant touch with her during the progress of the project. However, she is not available for the second half of my project.
- **BTech Coordinator: Sathiamoorthy Manoharan (Mano)**
  Mano is the BTech (IT) Coordinator and is the one who manages the BTech 451 project course. He was the one who validated my project.

4 BUSINESS PROBLEM

Regulatory and Industry Standards, including but not limited to Information Security Compliance, are a must for organisations wanting to operate above board to avoid contingent liabilities and to meet and satisfy customers' needs. However, compliance evidencing is a huge cost to businesses, especially when they have to evidence compliance with multiple requirements governed and are policed by different authorities.

Information security is very important for all organisations. There are multitudes of Information Security regulatory and industry standards that most organisations/businesses need to comply with. The costs of compliance audit and evidential proof of compliance could be daunting.

For example, Company X is a financial institution that wants to comply with three main regulatory instruments. Payment Card Industry Security Standards Council is enforcing Company X to comply with their PCI DSS standard due to their credit card transactions. Similarly, since the company has recently started their trading in the United States of America (USA), it was obligatory for them to make sure that they are regulated by the Sarbanes–Oxley Act. The company had already been following ISO 27002 standard to initiate, implement and maintain their information security management systems.

A typical compliance evidence process includes auditing and compliance reporting with typical associated cost profile. The table below lists the average associated costs for each of the standards Company X has to comply with.

The below figures are an estimate that have been retrieved from various websites and are not current costs. (Braintree, 2008), (Financial Executives, 2008), (PivotPoint Security, 2010)

	ISO 27002	***PCI DSS***	***Sarbanes-Oxley Act***	***Total***
Auditing Costs	$12,000	$362,500	$1,500,000	$1,874,500
Ongoing evidential costs	$10,000	$125,000	$250,000	$385,000
Total	**$22,000**	**$487,500**	**$1,750,000**	**$2,259,500**

With more than $1.5 million being spent on compliance, RCL has suggested a proposal of platform that will not only cut down the costs by more than 60%, but will also assist Company X to be compliant with all three at once.

With my proposed platform the estimated costs will be as follows: *the figures are a representation of estimated costs. They are based on the operating cost of the platform, as well the cost the company will be paying to get complied with the three listed regulatory instruments.*

	RCL Platform
Auditing Costs	$400,000
Ongoing evidential costs	$100,000
Total	**$500,000**

This project is the development of a framework to help businesses optimise the value and minimise the cost of review and proofing compliance.

RCL Director Gabriel Akindeju has given me a project to create a platform that allows companies to select a set of regulatory instruments and the industry standards that impact their business. This platform will then be able to perform minimal sets of walk-through reviews that will meet all of the requirements of the identified instruments.

Evidential proof of compliance can then be generated within the period of validity of the review and records to satisfy all of the business stakeholders.

My main task is to analyse a few of these regulatory instruments and industry standards, and classify them. Using this analysis, I am to create a foundation for a platform that can be used, maintained and updated in the future (*refer to Section 5.1 for more details*).

5 PROPOSED SOLUTION

5.1 INDUSTRY

There are many types of instruments for information security as it is a part of all types of industries, ranging broadly from local requirements to industry specifics as well as international standards and regulations. I have chosen to focus on the financial and banking industry as I believe this is where the data needs to be the most secured. With the world shifting towards the technological age, there is a shift from notes to plastic cards that hold important information about an individual. With all this information available, organisations need to take acute precautions to prevent it from falling into the wrong hands.

The best solution for companies is to be compliant with a certain set of regulations and standards. Although with the volatility of the security threats, it is difficult to guarantee security compliance. Depending on the size of the company, their budget for the compliance varies. Obviously, the bigger the company the more they are willing to spend, but also due to the volume of information that they have to protect they need to be all the more secure. Even though there are over 1,200 regulations and standards (MetricStream, 2015), they all have the same objective of protecting information. For the sake of this project, I have chosen to focus on the three main regulations and standards that affect the majority of the financial institutions.

Here I have listed three of the standards/regulations that have some commonality:

✓ISO 27002

✓ Sarbanes-Oxley Act (SOX)

✓ Payment Card Industry Data Security Standard (PCI DSS)

I will be making references to the Privacy Act 1993, the 11 essential controls and the CIA triad. I will also reference other frameworks that companies currently use and give recommendations on why this product is far superior to the ones available on the market currently.

The final product produced at the end of this project will be a web-based platform that will assist organisations with their selected security standards by providing guidelines on improving sections of the business to be better compliant with multiple regulations with half the cost. I will be using the Unified Compliance Frameworks for guidance on the classification of controls that are listed in each of the regulations I have chosen above, which will also enable me to group them together.

6 RELATED WORKS

6.1 CURRENT RESEARCH WORKS – IN THIS INDUSTRY

Financial institutions and regulation compliance go hand in hand and there are multiple researches available, however they cover a variety of different aspects. There are two such reports that I have found are related to my project:

- Information Security Management System Standards: A Comparative Study of the Big Five *Heru Susanto, Mohammad Nabil Almunawar and Yong Chee Tuan, 2011*
- IT Audit Challenges for Small and Medium- Sized Financial Institutions *Petter Lovaas and Suzanne Wagner, 2012*

I have chosen these two research papers as they address different aspects of compliance in the financial and banking industry, and how the security of IT is dealt with in each organisation. I will be referring to other reports and papers as well, but these are the main research I would like to focus on.

The Banking and Financial Sector (BFS) accounts for nearly eight percent of the US annual gross domestic product and is considered a backbone for the world economy. BFS are, according to regulations, required to develop an IT audit program to support its IT infrastructure in order to keep non-public customer information secure. Therefore, protecting the BFS means cooperation between financial regulators and private sector owners and operators. Furthermore, this coalition continuously improves these programs to include current and new threats to the banking and financial sector (Wagner, 2012).

Lovaas & Wagner continue to explain in their research the auditing challenges that small and medium-sized financial institutions (SMEs) face. This research paper is very relevant to my research as, even though they do not address the specific security standards, they address the importance of auditing. Similar to larger firms, SMEs need to perform risk-based IT audits on an ongoing basis. Having sound Internal IT audit examiners ensures that the time spent on regulatory compliance may be reduced (Wagner, 2012).

Information systems have a significant meaning to every organisation and the main purpose of auditing these systems is to review and provide feedback, assurance and suggestions to the organisation regarding the information security posture (Wagner, 2012). The topics that are covered within this review are grouped into the McCumber Cube's CIA. This basic model lists:

- **Confidentiality** – Critical information on any system can only be disclosed to authorized personnel.
- **Availability** – Critical business systems need to be available at all time when they are required. They also need to be well protected against all types of threats.

- **Integrity** – Information on the critical systems needs to always be accurate, reliable and timely. Controls need to be in place to prevent unauthorized modification to software, information or databases.

The general issue that we understand from this paper is that, even though there are frameworks available for BFS, they have their limitations. For example, none of the models are customized to provide feedback for both adequacy and compliance, and there are none that include human factors of auditing, especially towards small and medium-sized BFS.

TRADITIONAL VS RISK-BASED AUDIT APPROACH

Traditional	Risk-Based
Audit focus	Business focus
Transaction-based	Process-based
Financial account focus	Customer focus
Compliance objective	Risk identification, process improvement objective
Policies and procedures focus	Risk management focus
Multi-year audit coverage	Continual risk-reassessment coverage
Policy adherence	Change facilitator
Budgeted cost center	Accountability for performance improvement results
Career auditors	Opportunities for other management positions
Methodology: Focus on policies, transactions and compliance	Methodology: Focus on goals, strategies, and risk management processes

Figure 2 - Traditional vs Risk-Based Auditing (Wagner, 2012)

Another key point raised in this paper was the difference between traditional auditing and risk-based auditing. Figure 2 outlines the main differences between the newer methodologies compared to the more traditional one. Lovaas and Wagner highlight the importance of risk-based auditing for financial institutions and define it as an approach that focuses on the response of the organisation to the risks they face when achieving their goals and objectives.

With a large shift towards technology, businesses need to make sure they follow risk-based auditing as this will ensure that they are volatile with their changes and do not have to spend large sums of money to change systems and other aspects of their business.

Haru Susanto suggests that most common security standards are ISO 27001, BS 7799, COBiT, ITIL and PCIDSS. Although the report does not detail the controls of each of the standards, it gives a brief overview of each and their usability level in the world. The comparative study determines their respective strengths, focus, main components and their adoption based on Information Security Management System (ISMS).

ISO 27001 is the most used and well-known security standard available around the world with 163 countries using it. It is designed to protect the information assets and is applicable to all types of organisations, either private or public. BS 7799 is the predecessor to ISO 27001, ISO adopted their standards from BS 7799 and BS 7799-2. Both the standards implement the Plan-Do-Check-Act (PDCA), which aims to establish, implement, monitor and improve the effectiveness of an organisation's ISMS.

Julia Allen, states that the PDCA is a tried and trusted approach to security improvement that can be effectively used during deployment and operations. It is a set of minimum requirements for security hygiene and several security implementation frameworks that can be used in concert with the other articles in this content area (Allen, 2006).

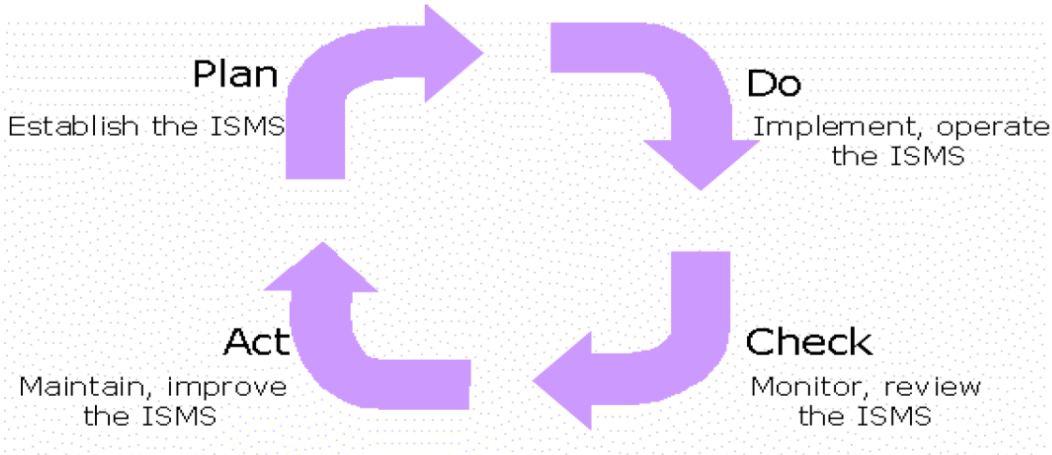


Figure 3 - PDCA Model (Allen, 2006)

Payment Card Industry Data Security Standard (PCIDSS) is also a security standard, but it is focused more towards helping organisations process card payments and to prevent credit card fraud through data compromise (Heru Susanto, 2011). Depending on the size of the organisation, they have to be assessed either by a Qualified Security Assessor (QSA) or by using a Self-Assessment Questionnaire (SAQ).

According Matthew Schwartz from Network Computing, 67% of companies that are PCI- regulated are still not in full compliance with the standard (Schwartz, 2011). He goes on to state that 50% of security professionals claim this to be a burden, which proves to me that due to the lack of clarity professionals find that they are not too sure what they are complying with. This claim opens a loop hole — professionals may not find compliance a burden if they had a system that would investigate for them.

The last two listed by Susanto are not standards, but instead are frameworks that assist organisations by giving them a guideline to follow so that their data can be secure. Information Technology Infrastructure Library (ITIL) is a set of concepts and practices for Information Technology Services Management (ITSM). Figure 4 illustrates the key components of ITIL. The listed components are a basic structure to achieving security for an organisation's complex systems. ITIL gets their motivation from the 11 essential controls specified below and has fashioned their structure based of that.

Figure 4- The ITIL components. (Heru Susanto, 2011)

Control Objectives for Information and related Technology (COBIT), similar to ITIL, is also a framework that is a supporting toolset that allows managers to bridge the gap between control requirements, technical issues, business risks and security issues. Basically, no matter how many controls there are, without a sound framework they are rendered useless.

The five main governance areas that COBIT focuses on are:

- Strategic alignment
- Value delivery
- Resource management
- Risk management
- Performance management

All five focus on making sure that the security risks are mitigated by aligning these with the business plans.

Heru Susanto defined 11 essential control, called by 11EC, that should be implemented by an organization, as requirements and compliance of the information security criteria by the standard body of ISMS. Most organisations need to adhere to all these controls to ensure their information is secure and they can be compliant with the standards.

These 11 essential controls are:

1. Information Security Policy
2. Communications and Operations Management
3. Access Control
4. Information Systems Acquisition, Development and Maintenance
5. Organization of Information Security
6. Asset Management
7. Information Security Incident Management
8. Business Continuity Management
9. Human Resources Security
10. Physical and Environmental Security
11. Compliance

By understanding these 11EC, I am able to distinguish the criteria that are followed by the organisations to be secured against threat. These 11EC also tie very closely to the components of ITIL, because the essence of these controls is to integrate technology into a business without affecting its growth as depicted in Figure 4 and, as a whole, link in with the CIA triangle.

6.2 COMPARISON OF THE RESEARCH PAPERS

Both Lovaas & Wagner and Heru Susanto explain in detail the effect of compliance in IT. Although they both address the issue in different ways, the common point they make is for an organisation's data to be secure, they need to be compliant with security stands and follow certain standards and protocols. Lovaas & Wagner describe the effect of the major security standards on small and medium financial institutions, as well as suggest the best way to audit such institutions.

On the other hand, Heru Susanto explains the difference between the major security standards and frameworks that can be used in all industries, not just limited to financial institutions. If we understand the difference between a standard and framework, we can decide which is more important in an organisation. First, we need to understand the basic difference between the two. A dictionary definition for a standard is '*something used as a measure, norm, or model in comparative evaluations*'. By this definition, we can understand that organisations need to attain a certain level of quality and that level is defined by a standard. Similarly, when a methodology is adopted by an organisation then it is their standard (Ajim, 2013).

A framework, on the other hand, is defined as 'a basic structure underlying a system, concept or text'. It is a general guideline that an organisation can adopt and it can consist of many components (Ajim, 2013). By this definition, we can understand that standards are accepted as the best practices or a perfect system, whereas a framework consists of practices that can be employed by an organisation in the real world. Susanto goes on to compare each of them using the 11EC of information security and how they tie into ISMS as a whole.

With both research papers claiming ISO series and PCIDSS to be major standards that organisations need to be compliant with, I believe my choice of comparing the two is not wrong. Another key thing to note was both paper used frameworks and standards together. However, my platform is solving the issue of being compliant with certain security standards and regulations. In conclusion, the basic message that is presented by both Susanto and Lovaas & Wagner is that if a company is able to abide by the controls of specific security standards, then they will not be faced with data loss when breached.

6.3 CURRENT TECHNOLOGIES / PLATFORMS

Similar to the research papers, there are a few platforms that are available to organisations. These platforms provide data as a service and assist internal auditors with controls over financial reporting. There are many platforms and services available, but they all are for different purposes or regulatory compliance is incorporated into a bigger package.

Strevus is one of the few platforms that is very close to the platform I want to create. It provides a highly secure and scalable infrastructure for financial institutions to collect, validate, maintain and share their compliance data and documentation (Strevus, 2014). The platform helps customers navigate through the sea of regulatory compliance in today's shifting landscape and deploy an effective solution that meets the unique challenges of each of the organisations.

Strevus's main selling point is the Enhanced KYC/AML due diligence for Bitcoin. Bitcoin is a form of currency, created and held electronically. With many large companies accepting Bitcoin they need conduct KYC/AML due diligence along with existing global regulatory compliance.

Although the platform is important, it is essential to realise the dynamics behind the whole platform. Strevus claim that they are committed to ensuring the confidentiality, integrity and security of customers and system data. This ties in very well with what Lovaas & Wagner covered in their research paper. Strevus go on to state that by adhering to the highest standards for security they ensure organisations can rely on electronic-based compliance and confidence.

The information security policies listed by Strevus are very close to the 11 essential controls listed above. I did a small comparative analysis of both Strevus and 11EC, (*Table 1*), and found although Strevus do not address all of them, they cover the main important controls when information security is concerned.

Table 1

Strevus	11 Essential Controls
Community Policing	Information Security Policy
Data Centre Security	Physical and Environmental Security
System Hardening	Asset Management
Comprehensive Network Protection	Organization of Information Security
Full Lifecycle Auditing and Reporting	Business Continuity Management
Data Encryption	Access Control
Security Policies and Configurations	Information Systems Acquisition, Development and Maintenance

In the same way, MetricStream are a market-leading organisation that developed a cloud app for Governance, Risk and Compliance. They integrate GRC technologies and programs across businesses, IT and security functions. With their regulatory compliance app, they are very close to the product solution I have detailed. The only difference I have observed from my research is that their focus is on supporting compliance management through document control, compliance training, ongoing auditing and recording as well as reporting of exception events (MetricStream, 2015).

MetricStream have many services and applications, one of them that seemed relevant was their IT security and governance function. It ensures, establishes and enforces security policies, standards and procedures. Also, assisting managers continuously monitor all the components of the IT infrastructure for compliance and security threats, and take appropriate action.

IT-GRC solution by MetricStream provides a few of the following capabilities:

- Policy Management
    - All policies can be mapped to frameworks and regulations like COBIT, ISO, SOX, and PCI.
    - These policies can be broken down into sections and sub-sections, and mapped to controls.
- Risk Management
    - Provides a framework that simplifies the identification and analysis of all risks related to IT operations and information security.
    - Provides risk identification to mitigation and reporting.
- Compliance Management
    - Provides a common framework and an integrated approach to manage all IT compliance regulations and mandates.

I highlighted these capabilities, as they are common with my proposed solution. Policy management describes the use of the standards and regulations being mapped to policies. According to a Unified Compliance Framework, they have already grouped close to 9300+ controls from 1200+ regulations

to make data retrieval easy (MetricStream, 2015). This is what MetricStream used to help them classify the regulations into a set of essential controls. Everything mentioned above about MetricStream links back to the 11 essential controls of information security.

MetricStream also follows the PDCA methodology closely, by mapping the policies to the controls they are able to plan well ahead of any risks. By having the app, they are able to both Do and Check the progress and threats affecting their systems and come up with a plan to mitigate them, which is the final step.

6.4 COMPARISON OF THE TECHNOLOGIES

My understanding of the entire process followed by both Strevus and MetricStream is that they followed the 11 essential controls closely and have based their platforms on them. Strevus covers compliance of the financial institutions but only a single aspect of it, by looking at the transactions of Bitcoins. MetricStream on the other hand looks at the variety of standards and regulations tailored to the organisation, which enables the companies to have flexibility.

The Strevus platform was explained as a basic overview of the platform itself. We saw that it was referring to the customer data model and ETL mapping that reads the customer data and writes to the ERP system. This is based on NoSQL that allows users to easily find and manage their assets in one place. A summary of the whole platform was integrating this platform into a company's existing ERP system.

Although my solution is tied in very closely with the output of the MetricStream platform, I will be focusing on providing guidelines for the company to make sure they are compliant with their chosen security standards. In the future, I might plan to implement a dashboard that gives the managers a visual representation of the key systems that need to be addressed to achieve the certification for certain regulations. It will be closely following the 11 essential controls as well as referring to the CIA triad.

7 BACKGROUND

7.1 STANDARDS

Figure 5 - (McMeley, 2013)

Standards are introduced to regulate the governance over the information security, which is very important to all organisations. Although there are many regulations and standards widely available, they are not adopted by most organisations for a variety of reasons, mainly being the cost involved. In evaluating the many options for network security solutions, it is essential to understand and consider the role of security standards. The growth in distributed computing and the ensuing increase in computer crime have led to legislation and regulations that establish legal requirements for network and data security (Kozlay, 2014).

.

7.1.1 PCIDSS

The PCI DSS is a set of requirements for enhancing security of payment customer account data. It was developed by the founders of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa to help facilitate global adoption of consistent data security measures. PCI DSS includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

The below controls will be used in building the matrix, and I will determine how they link together with the 15 impact zones and with the other two controls.

1. Build and Maintain a Secure Network
    a. Install and maintain a firewall configuration to protect cardholder data
    b. Do not use vendor-supplied defaults for system passwords and other security parameters
2. Cardholder Data
    a. Protect stored cardholder data
    b. Encrypt transmission of cardholder data across open, public networks
3. Maintain a Vulnerability Management Program
    a. Use and regularly update anti-virus software or programs
    b. Develop and maintain secure systems and applications
4. Implement Strong Access Control Measures
    a. Restrict access to cardholder data by business need-to-know
    b. Assign a unique ID to each person with computer access
    c. Restrict physical access to cardholder data
5. Regularly Monitor and Test Networks
    a. Track and monitor all access to network resources and cardholder data
    b. Regularly test security systems and processes
6. Maintain an Information Security Policy
    a. Maintain a policy that addresses information security for employees and contractors

The above controls will be used in building the matrix, and I will determine how they link together with the 15 impact zones and with the other two controls.

7.1.2 SOX

The Sarbanes-Oxley Act, 2002, is designed to protect investors and the public by increasing the accuracy and reliability of corporate disclosures. It was enacted after the high-profile Enron and WorldCom financial scandals of the early 2000's. It is administered by the Securities and Exchange Commission, which publishes SOX rules and requirements defining audit requirements and the records businesses should store and for how long (Seider, 2004). This standard can be used for multiple purposes but for this report, I will be referring to the general controls that overlook Information Technology.

There are two levels of controls that need to be considered when attempting to comply with SOX – the company level and the general level.

There are four main categories that need to be considered the company-level:

- Control Environment
    - The control environment creates the foundation for effective internal control, establishes the "tone at the top", and represents the apex of the corporate governance structure.
- Information and Communication
    - The identification, management and communication of relevant information represents an ever-increasing challenge to the IT department.
- Risk Assessment
    - Risk assessment involves the identification and analysis by management of relevant risks to achieve predetermined objectives, which form the basis for determining control activities.
- Monitoring
    - 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.

At the general level, the general controls are commonly defined as being the controls that are applicable across all IT systems and are essential to ensuring integrity, reliability and quality of the systems. These controls are standardised across the company and are centrally administered, controlled and repeatable (Seider, 2004).

Figure 6 - (Assuria, 2015)

The IT general controls are:

- Acquire or Develop Application Software
- Acquire Technology Infrastructure
- Procedures
- Install and Test Application Software and Technology Infrastructure
- Manage Changes
- Define and manage service levels
- Manage third-party services
- Ensure systems security

- Manage the configuration
- Manage problems and incidents
- Manage data
- Manage operations

The granularity of the expansion of general controls depends on how the company operates. As a result, a consumer soft goods manufacturer can be expected to have a number of significantly different controls than an internet service provider (Seider, 2004).

For this project, I will be using the above listed controls and comparing them to the other standards and how they are associated with the 15 impact zones.

7.1.3 ISO 27002

ISO 27002, although it belongs to the same family of standards, varies slightly to ISO 27001. You cannot get certified with ISO 27002 because it is not a management standard, which means that it does not define how to run a system. Also, ISO 27001defines the Information Security Management System (ISMS), unlike ISO 27002 (Kosutic, 2010).

Figure 7 - (Manske, 2007)

Although I mentioned that I am referring to ISO 27002 above, their controls listed are a derivative form of ISO 27001. The ISO 27002 standard describes a comprehensive set of information security control objectives and a set of generally accepted good practice security controls. It contains 12 main sections:

1. Risk assessment
2. Security policy
    a. Management direction for information security
3. Organization of information security
    a. Internal Organisation
    b. Mobile devices and teleworking
4. Asset management
    a. Responsibility of assets
    b. Information classification
    c. Media handling
5. Human resources security
    a. Prior to employment
    b. During employment
    c. Termination and change of employment
6. Physical and environmental security
    a. Secure areas
    b. Equipment security
7. Communications and operations management
    a. Operational procedures and responsibilities
    b. Protection of malware
    c. Backup
    d. Logging and monitoring
    e. Control of operational software
    f. Technical vulnerability management
    g. Information systems audit considerations

8. Access control
    a. Business requirements of access control
    b. User access management
    c. User responsibilities
    d. System and application access control
9. Information systems acquisition, development and maintenance
    a. Security requirements of information systems
    b. Security in development and support processes
    c. Test data
10. Information security incident management
    a. Management of information security incidents and improvements
11. Business continuity management
    a. Information security continuity
    b. Redundancies
12. Compliance
    a. Compliance with legal and contractual requirements
    b. Information security reviews

8 COMPARISON OF THE STANDARDS

8.1 CONTROLS GROUPING

With 1200+ standards and more than 9600 controls, it is difficult to keep track. However, I have found a way to classify them into 15 impact zones. Each of these of impact zones deals with the one area of policies, standards and procedures technology acquisition, physical security, continuity, records management, etc.

I had a little assistance from the Unified Compliance Framework when trying to understand the different impact zones and how they can be effective in associating the different compliance standards and their controls.

The impact zones that I found apply to this solution and its potential growth in the future to cater to other industries and their regulations and standards (Unified Compliance Framework, 2015).

The impact zones are:

- Leadership and high level objectives
- Audits and risk managements
- Monitoring and measurement
- Technical security
- Physical and Environmental protection
- System continuity
- Human resources management
- Operational management
- System Hardening through configuration management
- Records management
- Systems design, build and management
- Acquisition or sale of facilities, technology, and services
- Privacy protection for information and data
- Compliance and Governance Manual of Style
- Third Party and supply chain oversight

- Although the three standards I have chosen do not fit into all of the 15 impact zones, they fit into a few of them. With the assistance of the 11 essential controls to help me demarcate the controls grouping, I have classified each of the controls into each of the 15 impact zones.
- In Section 7, I had outlined the main sections of each of the regulatory instruments, but these are not the main controls that the company has to adhere to. However, in Section 8.2 I will be classifying all the controls and their sub-controls into the 15 impact zones and how they can be combined to form one big instrument that companies can comply with.

8.2 CLASSIFICATION OF REGULATORY INSTRUMENTS (MATRIX)

Table 2 – Classification Matrix

Impact Zones	PCI DSS	SOX	ISO 27002
Leadership and high level objectives		- Define and manage service levels (16)	

Audits and risk managements	Maintain a policy that addresses information security for all personnel (12)	- Develop and maintain policies and procedures (13) - Manage problems and incidents (20)	Security Policy (5) Information Security incident management (13)
Monitoring and measurement	Track and monitor all access to network resources and cardholder data (10) Regularly test security systems and processes (11)	- Manage Changes (15)	Organisation of Information Security (6.1)
Technical security	Firewall Configuration (1)	- Ensure systems security (18)	
Physical and Environmental protection	Restrict physical access to data (9)		Asset Management (7) Physical and Environmental Security (9)
System continuity			Business Continuity management (14)
Human resources management			Human Resources Security (8)
Operational management		- Manage operations (22)	Communications and Operations Management (10)
System Hardening through configuration management	Use of anti-virus (5)	- Install and test application software and technology infrastructure (14) - Manage the configuration (19)	
Records management	Assign a unique ID to each person with computer access (8)		
Systems design, build and management	Develop and maintain secure systems and applications (6)	- Acquire or Develop - Application Software (11)	
Acquisition or sale of facilities, technology, and services		- Acquire Technology Infrastructure (12)	Information System acquisition, development and maintenance (12)

Privacy protection for information and data	Not using vendor-supplied defaults for system passwords (2) Protect stored cardholder data (3) Encrypt transmissions of data across open, public networks (4) Restrict access to cardholder data by business need to know (7)	- Manage data (21)	Access Control (11)
Compliance and Governance Manual of Style			Compliance (15)
Third Party and supply chain oversight	Shared hosting providers must protect the cardholder data environment (A.1)	- Manage third-party (17) services	Organisation of Information Security (6.2) Communications and Operations Management (10.2)

As we can notice from the main sections of each of the three regulatory instruments, we can see that they cover almost all the 15 impact zones, and some of the zones have controls from each of the instruments. This suggests that there are a few commonalities in the controls and what they are covering. Obviously the financial institutions are having to spend a lot of money on spending on checks which are duplicated in each of these specified controls. However, my platform will be incorporating a more detailed matrix that will be embedded in the back end database.

This matrix will assist me in providing a more detailed guidelines for the institutions to comply with all their selected instruments at once based on the 15 impact zones.

9 PLATFORM DESIGN

9.1 TECHNOLOGIES

The best way of presenting this solution is using a web-based platform, which enables organisations to track their systems and check the compliance without having to install any software as such. There are benefits and limitations of having such platform. I will discuss them in more detail and outline what makes it very suitable for RCL.

We can list a few benefits that are common knowledge like the lack of upgrades, security, uptime, backups and 'IT guys' stuff. With cloud computing taking over the technological world currently, quite a few businesses are shifting towards it. Companies prefer to have information on a centralized location that will allow them to access this information from any geographical location.

Although app-based platforms are preferred, I will be creating a web-based platform as it is more robust and modular. Also, the platform does not need to be used while on the move, so an app-based platform is not required.

The technologies that are available for web-based platforms are:

- ASP.NET with SQL
- HTML/CSS with AJAX
- PHP with MYSQL (incorporating HTML and CSS)

By investigating further into each of these technologies, I would be able to better decide which option is better suited for my project. In this project, the use of a database is very important as I need to store the controls for each of the regulatory instruments. Hence, I have included some sort of database engine in all my options. Although currently I am only focused on solving the issue of three regulatory compliances, I would be considering expanding this to integrate other instruments that are required for other major industries like Health, Tourism and so on

9.1.1 ASP.NET with SQL

When creating a web application with ASP.NET, we are introduced to a framework known as MVC (Model, View and Controller). This framework makes it easier to manage the complexity by dividing the application into a model, view and controller.

- The **Model** is the part of the application that handles the logic for the application data. Often model objects retrieve data, and store data, from a database.
- The **View** is the part of the application that handles the display of the data. Most often the views are created from the model data.
- The **Controller** is the part of the application that handles user interaction. Typically controllers read data from a view, control user input, and send input data to the model.

Below I have listed some of the advantages and disadvantages of using ASP.NET MVC:

Table 3 - (Anand, 2011)

Advantages	Disadvantages
Separation of Concerns - The MVC framework provides a clean separation of the UI , Business Logic , Model or Data	**Large data in the view state:** Frustrating site visitors with slower response times and increasing the bandwidth demands of the server.
More Control - provides more control over the HTML, JavaScript and CSS than the traditional Web Forms.	**Limited control over HTML:** HTML output usually failed to comply with web standards or make good use of CSS, and server controls generated unpredictable and complex ID values that are hard to access using JavaScript.
Testability - provides better testability of the Web Application and good support for the test driven development too.	**Leaky abstraction:** Web Forms tries to hide away HTML and HTTP wherever possible. As you try to implement custom behaviours, you frequently fall out of the abstraction, which forces you to user to use the traditional post back mechanism to generate the desired html
Lightweight - does not use View State and thus reduces the bandwidth of the requests to an extent.	

For this project, I will not be considering this technology as it does not meet the requirements of the solution.

9.1.2 HTML/CSS with AJAX

Hypertext Mark-up Language (HTML) is a mark-up language that is useful for describing web documents. It is a set of mark-up tags that describes different document content. HTML is preferred by many developers due to its flexibility and its wide usage, established on almost all websites. However, there are a few drawbacks to this language. When another language replaces the original work of the tag, it becomes deprecated tag, common when used in conjunction with Cascading Style Sheets (CSS).

AJAX (Asynchronous Javascript and XML) is a collection of old technologies with slight deviations to each of these technologies. These groups of technologies comprise of the following aspects, namely:

- HTML and CSS
- Javascript
- XML and XSLT
- XMLHttpRequest

AJAX allows displaying web pages with interactive, efficient and quick interfaces. Web giants like Google effectively utilize AJAX in their web applications like Gmail and Google Maps (JScripters, 2011).

Table 4 - (JScripters, 2011)

Advantages	Disadvantages
Better interactivity AJAX allows easier and quicker interaction between user and website as pages are not reloaded for content to be displayed.	**The back and refresh button are rendered useless** With AJAX, as all functions are loaded on a dynamic page without the page being reloaded or more importantly a URL being changed (except for a hash symbol maybe), clicking the back or refresh button would take you to an entirely different web page or to the beginning of what your dynamic web page was processing. This is the main drawback behind AJAX but fortunately with good programming skills this issue can be fixed
Easier navigation AJAX applications on websites can be built to allow easier navigation to users in comparison to using the traditional back and forward button on a browser.	
Compact With AJAX, several multi-purpose applications and features can be handled using a single web page, avoiding the need for clutter with several web pages.	**It is built on JavaScript** While JavaScript is secure and has been heavily used by websites for a long period of time, a percentage of website surfers prefer to turn JavaScript functionality off on their browser rendering the AJAX application useless, a work around to this con is present as well, where the developer will need to code a parallel non-JavaScript version of the dynamic web page to cater to these users.
Backed by reputed brands Several complex web applications are handled using AJAX, Google Maps is the most impressive and obvious example.	

Although I have mentioned the advantages and disadvantages of Ajax, I will not be considering it for this project.

9.1.3 PHP with MySQL

Hypertext PreProcessor (PHP) is a widely-used open source general-purpose scripting language that is especially suited for web development and can be embedded into HTML. Rather than the use of HTML code, PHP allows the programmer to create a more dynamic system. What distinguishes PHP from something like client-side JavaScript is that the code is executed on the server, generating HTML which is then sent to the client. The client would receive the results of running that script, but would not know what the underlying code was. You can even configure your web server to process all your HTML files with PHP, and then there is really no way that users can tell what you have up your sleeve.

Below I have listed some of the pros and cons of using PHP:

Table 5 - (PHP-Tutorial, 2015)

Advantages	Disadvantages
Open source: It is developed and maintained by a large group of PHP developers, this will helps in creating a support community, abundant extension library.	Security : Since it is open sourced, so all people can see the source code, if there are bugs in the source code, it can be used by people to explore the weakness of PHP
Speed: It is relative fast since it uses much system resource.	Not suitable for large applications: Hard to maintain since it is not very modular.
Easy to use: It uses C like syntax, so for those who are familiar with C, it's very easy for them to pick up and it is very easy to create website scripts.	Weak type: Implicit conversion may surprise unwary programmers and lead to unexpected bugs. For example, the strings "1000" and "1e3" compare equal because they are implicitly cast to floating point numbers.
Stable: Since it is maintained by many developers, so when bugs are found, it can be quickly fixed	
Built-in database connection modules: You can connect to database easily using PHP, since many websites are data/content driven, so we will use database frequently, this will largely reduce the development time of web apps.	

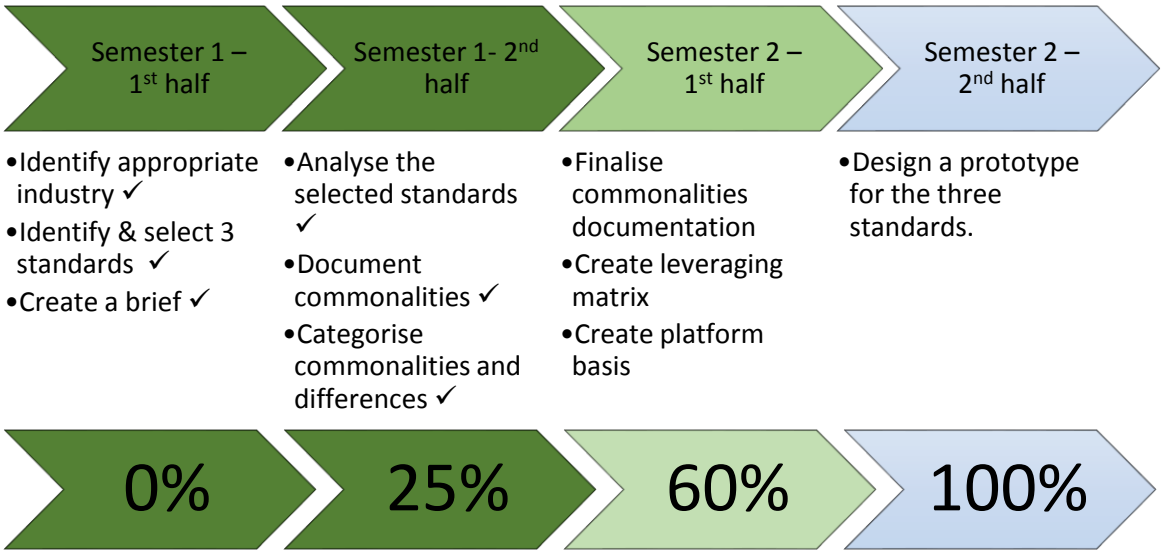
9.1.4 Platform

After researching the advantages and disadvantages of the technologies listed above, I have decided to use PHP due to its ability to have Built-In database connection modules, the other two listed technologies required a much longer process to establish such connection. A database is very crucial for my project, as I will be need to be able to group the internal controls based on each of the impact zones.

10 WHAT IS NEXT?

10.1 TIMELINE DETAILING MY PROGRESS AND FUTURE WORKS.

10.1.1 Timeline



I have achieved 25% of the project that I had planned to complete. The most time consuming part of this semester was the research and literature review. I had issues with finding research that is somewhat related to the topics I was covering in this report.

I have covered some of the technologies that are currently available in the market as well as researching the correct language required to create this platform. I have chosen to program the platform using the PHP language and with MySQL as the back end of the database.

10.1.2 Future Work

After completing the research aspect of this project, I believe I have positioned myself to complete the platform with ease. My aim for the next semester is to finalise the matrix with the controls, rather than the numbers as shown in Table 2. I will create an Excel sheet, where each of the controls from the different regulatory instruments will be combined to form one compliance platform.

For the formation of platform basis I will need to look into the usability of the platform and implement a basic architecture, which will involve the retrieval of data from the database and then give the correct guidelines to the internal auditors of the financial institutions.

The final part of is the actual design work of the platform, where I will be implementing the three standards. Here I will be looking at PHP coding for the basic UI part of the platform, however for the back end where the transactions with the database will be handled by MYSQL.

The platform will need to include some aspect of security to make sure, that the information is not available to everyone and to only to the parties that have subscribed for this platform.

11 REFERENCES

37 Signals. (n.d.). *Web-based software is better than your regular software.* Retrieved from https://37signals.com/webbased

Ajim, M. (2013, January 14). *Redefining Project Management*. Retrieved from What are the differences between standard, framework, and methodology?: http://blog.sukad.com/20130114/differences-between-standard-framework-methodology/

Allen, J. H. (2006). *Plan, Do, Check, Act.*

Anand, B. (2011, October 19). *Disadvantages of ASP.NET Web Forms*. Retrieved from ASP.NET Rocks World of Web Development: http://aspnet-rocks.blogspot.co.nz/2011/10/disadvantages-of-aspnet-web-forms.html

Assuria. (2015). *Assuria helps secure the integrity of reporting for Sarbanes–Oxley (SOX)*. Retrieved from http://www.assuria.com/compliance/sox.html

Basel Committee on Banking Supervision. (2005). *Compliance and the compliance function in banks.*

Braintree. (2008, June 25). *What does it cost to become PCI Compliant?* Retrieved from Braintree: https://www.braintreepayments.com/blog/what-does-it-cost-to-become-pci-compliant

CBSS. (2011). *CBSS*. Retrieved from CBSS Web Site: http://2cbss.com/

Dalling, T. (2009, May 31). *Model View Controller Explained*. Retrieved from http://www.tomdalling.com/blog/software-design/model-view-controller-explained/

Financial Executives. (2008, April 4). *FEI Survey: Average 2007 SOX Compliance Cost $1.7 Million*. Retrieved from FEI : http://www.financialexecutives.org/KenticoCMS/News---Publications/Press-Room/2008-press-releases/FEI-Survey--Average-2007-SOX-Compliance-Cost-$1-7-.aspx

Heru Susanto, M. N. (2011). *Information Security Management System Standards: A Comparative Study of the Big Five.*

JScripters. (2011). *AJAX PROS AND CONS*. Retrieved from Jscripters: http://www.jscripters.com/ajax-disadvantages-and-advantages/

JScripters. (2011). *WHAT IS AJAX?* Retrieved from JScripters: http://www.jscripters.com/what-is-ajax/

Kosutic, D. (2010, September 13). *ISO 27001 vs. ISO 27002*. Retrieved from 27001 Academy: http://www.iso27001standard.com/blog/2010/09/13/iso-27001-vs-iso-27002/

Kozlay, D. (2014). *The Importance of Security Standards.*

Lovrić, Z. (2012). *Model of Simplified Implementation of PCI DSS by Using ISO 27001 Standard.*

Manske, M. (2007, September 7). *International_Organization_for_Standardization*. Retrieved from http://en.wikipedia.org/wiki/International_Organization_for_Standardization#/media/File:ISO_english_logo.svg

McMeley, R. G. (2013, December 13). *PaymentLawAdvisor*. Retrieved from PCI DSS 3.0: Business as Usual?: http://www.paymentlawadvisor.com/2013/12/16/pci-dss-3-0-business-as-usual/

MetricStream. (2015). *MetricStream Regualtory Compliance Management Software Solution*. Retrieved from www.metricstream.com/solutions/regulatory_compliance.htm

PHP-Tutorial. (2015, March 9). *PHP Introduction*. Retrieved from https://phptutorialpoints.wordpress.com/2015/03/09/php-introduction/

PivotPoint Security. (2010, July 26). *ISO-27001 Cost Estimate: $48,000 Information Security Confidence: Priceless*. Retrieved from http://www.pivotpointsecurity.com/risky-business/iso-27001-cost-estimate-48000-information-security-confidence-priceless

RCL. (2014). *Risks Consult Limited*. Retrieved from Risks Consult Limited: http://www.risksconsult.com/about-us/

Schwartz, M. (2011, April 20). *Network Computing*. Retrieved from http://www.networkcomputing.com/networking/67--of-companies-fail-credit-card-security-compliance/d/d-id/1097292?

Seider, D. (2004). *Sarbanes-Oxley Information Technology.* Las Vegas: SANS Institute.

Strevus. (2014). *Strevus*. Retrieved from www.strevus.com

Unified Compliance Framework. (2015). Retrieved from https://www.unifiedcompliance.com/

W3Schools. (n.d.). *PHP 5 Introduction*. Retrieved from http://www.w3schools.com/php/php_intro.asp

Wagner, P. L. (2012). *IT Audit Challenges for Small and Medium- Sized Financial Institutions.*

Weistein, E. (n.d.). *PHP in Action* . Retrieved from Codecademy: http://www.codecademy.com/en/tracks/php