RISK ASSESSMENT METHODOLOGY FOR PRIVACY AND SECURITY OF CUSTOMER RELATIONSHIP MANAGEMENT SYSTEMS

Master’s Thesis by Adam Kwiatkowski BMediaArts

October 2017

College of Science and Engineering, Flinders University
Master of Information Technology

Declaration

'I certify that this thesis does not incorporate without acknowledgment any material previously submitted for a degree or diploma in any university; and that to the best of my knowledge and belief it does not contain any material previously published or written by another person except where due reference is made in the text.'

[redacted]

Adam Kwiatkowski October 2017

Abstract

The purpose of a customer relationship management (CRM) system is to provide a benefit (for example, generating a profit) to the organisations that use them through the integration of networks, people, purpose, and process. The literature review identified that currently there is no CRM specific security and assessment methodology. Existing CRM models do not visibility and proactively manage privacy and security risks in a way that facilitates automated compliance with ISO27001. The research evaluated ISO27001 as a possible Information Security Management System (ISMS) for CRMs, given that ISO27001 can be applied to any organisation, technology and CRM. The proposed CRM model addressed the limitations of the existing CRM models and incorporates ISO27001's principle of Plan-Do-Act-Check (PDAC) as a mechanism towards achieving automated compliance. The compliance layer with the proposed CRM model, introduces the proposed risk management methodology. The methodology implements static and dynamic security and privacy controls, that collectively work to reduce the likelihood of a hazard from occurring. This will maintain the confidentiality, integrity, and availability of personal information within the CRM. Data mining was used to enhance the model's performance. The effectiveness of the proposed CRM model and the proposed risk management methodology are evaluated for effectiveness, strengths, and limitations. Three types of types were performed against the proposed risk assessment model, to determine how effectively the model performed, and how well it can facilitate the automation of ISO27001. The proposed risk assessment methodology enabled the privacy and security outcomes to be better aligned with the purpose of a CRM.

Acknowledgements

Thank you Dr Trent Lewis, Lecturer in the College of Science and Engineering at Flinders University, for your guidance, mentoring, and sponsorship of this thesis.

Glossary

APP	Australian Privacy Principles
CRM	Customer (or Contact) Relationship Management
CIA	Confidentiality, Integrity, Accessibility
CIAA	Confidentiality, Integrity, Accessibility, Accountability
IAS	Infrastructure as a Service
IDIC	Identify-Differentiate-Interact-Customise
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISMS	Information Security Management System
KRI	Key Risk Indicator
NIST	American National Institute of Science and Technology
NISTCSF	NIST Cybersecurity Framework
PDAC	Plan – Do – Act – Check
PPDM	Privacy Preserving Data Mining
RC	Risk Control
SAS	Software as a Service
SME	Small to Medium Enterprise

Table of Contents

List of Figures

List of Tables

Chapter 1. Introduction

Since the internet was first connected, the ‘rise of the information age’ commenced (Carron et al. 2016). Information systems are being used in all aspects of modern life, with Government agencies and organisations of all sizes using databases to collect, handle, and distribute personal information (Carron et al. 2016). Roughly, 86% of security breaches involved the loss or theft of customer information (Ponemon 2005 as cited in Romano & Fjermestad 2007, p. 70). Organisations will not spend more than 37% of their expected losses from a security breach to secure their systems (Gordon and Loeb 2002 as cited in Romano & Fjermestad 2007, p. 77). Organisations paid, on average, USD$154 for each stolen or lost record containing sensitive or confidential information (Ponemon 2015). For security and privacy controls to be effective in a CRM, they would need to mitigate any identified risks in a cost-effective and organisationally consistent way.

The objective of this thesis is to propose an alternative CRM model capable of reducing the likelihood of personal information being comprised. The proposed CRM model contains a compliance check layer, that features its own risk management methodology. The effectiveness of the proposed CRM model and risk management methodology will be evaluated through three series of tests, including one that evaluates static controls against dynamic (data mining) controls.

The literature review connects broadly; CRMs, security, privacy, and data mining in an attempt to improve the privacy and security postures of CRMs. The literature review identifies a gap in current research relating to privacy and security assessment methodologies for CRMs, and highlighted a lack of visible privacy and security controls in CRM models.

The research evaluated ISO27001 as a possible ISMS for CRMs, given that ISO27001 can be applied to any organisation, technology, and type of CRM. The proposed CRM model adopts the ISO27001’s PDAC principle as a way of achieving automated compliance with the ISO27001 standard. The proposed risk management methodology demonstrates that through the implementation of multiple controls, the risk of a privacy or security breach (main event) can be mitigated in a cost effective manner.

The ISO27001 ISMS process requires the adoption of a risk management methodology. The proposed CRM model incorporates a risk methodology for performing CRM privacy and security assessments that collectively reduce the likelihood of a main event from occurring, whilst visibly linking identify risks to their controls and business drivers. These are “outcomes based on business needs that an organization *(sic)* has selected from the categories and subcategories” (NIST 2016, p. 5) suited to an organisation’s size and resources. Static and dynamic controls attempt to reduce the likelihood of a main event from occurring that may compromise the confidentiality, integrity, and availability of personal information stored within a CRM. Data mining techniques will be applied to a dynamic control, to determine if dynamic controls can be more effective at reducing risk than static controls.

The goal of this thesis is to facilitate a dynamic privacy and security compliance model for CRMs that is compatible with ISO27001 and creates a CRM specific assessment methodology. The effectiveness, strengths, and limitations of the model are evaluated to determine if automated ISMS compliance within a CRM can be successfully achieved.

This thesis has found that the proposed risk assessment methodology demonstrated that ISO27001 can be partially automated. The test results found that the average number of allowed requests decreased as the number of security and privacy controls increased. Dynamic controls were found to be the most effective individual control. However, they were best suited for supporting existing static controls, due to their unpredictability. Future research is required to determine how the proposed risk assessment methodology and proposed CRM model can generate the documentation (or dashboards) and data required to fully automate the ISO27001 audit process.

Chapter 2. Literature Review

What is a CRM?

A "CRM is the core business strategy that integrates internal processes and functions, and external networks, to create and deliver value to targeted customers at a profit" (Buttle & Maklan 2015, p. 15).

There are three types of CRMs:

- **Strategic** CRMs, which typically focus on customer value, satisfaction and retention through product delivery, operational excellence, and sales activities (Buttle & Maklan 2015, p. 4);
- **Operational** CRMs, which focus on automating customer facing business processes such as marketing, selling, and service (Buttle & Maklan 2015, p. 7);
- **Analytical** CRMs, which aim to capture, process, store, extract information to interpret and report on it, with the goal of achieving greater customer or company value (Buttle & Maklan 2015, p. 11).

CRM Models

Buttle & Maklan (2015) identify four CRM models that describe different processes, functions, and ways CRM objectives can be met:

- The **IDIC CRM Model** relies on profiling customers to achieve differentiation and enables the organisation to the meet the specific needs of each customer.
- The **Value Chain CRM Model** (Figure 1) consists of "five primary stages and four supporting conditions leading towards the end goal of enhanced customer profitability" (Buttle & Maklan 2015, p. 21). Each stage identifies tools that collectively supports the goal of customer profitability.

has been removed due to copyright restrictions

Figure 1 Value Chain CRM Model (Buttle & Maklan 2015, p. 20)

- **Payne and Frow’s 5-process CRM model** (Figure 2) consists of five core processes to increase profitability:
  - Strategy development; applicable for strategic CRMs;
  - Value creation, also applicable for strategic CRMs;
  - Multi-channel integration, applicable for operational CRMs;
  - Performance Assessment, applicable to all CRMs; and
  - Information Management, applicable for analytical CRMs.

has been removed due to copyright restrictions

Figure 2 Payne and Frow’s 5-process model (Buttle & Maklan 2015, p. 21)

- The **Gartner CRM Model** (Figure 3) identifies eight areas that organisations must implement for a CRM to be considered successful.

has been removed due to copyright restrictions

Figure 3 Gartner CRM Model (Buttle & Maklan 2015, p. 21)

- Malthouse et al. (2013) identify the **Social CRM** (Figure 4) that enables customers to become active participants with the organisation in the public sphere. The benefits of the Social CRM model are not fully understood by research. Further work is required to ensure the model can link social engagement outcomes to profitability as Buttle & Maklan (2015, p. 13) argue the Social CRM model is not fundamentally a type of CRM.

has been removed due to copyright restrictions

Figure 4 Social CRM (Malthouse et al. 2013, p. 272)

CRM functions have evolved from sales, finance, and administration, to productivity, and most recently to customer experience management. Security and privacy are not a type of CRM, nor a core feature or function. They are applied within functions of CRMs to enable controls that mitigate risks. In the CRM models identified, privacy and security are secondary to the collection and use of an individual's data for generating profits. Seitz (2006, p. 62) argues

> "the data contained within a CRM application is often a company's most critical asset, yet because of the pivotal role this information plays in day-to-day business activities, it is also often the most vulnerable to security breaches and disruptions."

Each CRM model presents different challenges towards achieving privacy and security, as different risks and associated controls will be applied based on the type and functionality of the CRM.

Security in CRMs

There has been limited research into CRM security. Choon (2004) proposed a performance based ISMS that evaluates the risk of CRMs through a scoring system. Seify (2006) proposed that an ISMS framework for CRMs would be beneficial. However, his research did not highlight how to apply an ISMS to a CRM model.

Seitz (2006) stressed the importance of backups, policies, and monitoring to detect and protect against anomalous patterns in CRM use. However, Seitz's recommendations are simply standard security practices that are not CRM specific.

Romano & Fjermestad (2007) proposed that application of ISO27001 (formerly ISO 17799) standard towards achieving a comprehensive security standard for CRMs to protect the confidentiality, integrity, and availability (CIA principles) of CRM information. ISO27001 was chosen due to the broad application and adaptability of the security framework. ISO27001 is the currently the best-known standard for an ISMS.

Kim (2010) supports the view that there is a lack of research in CRM security, concluding "the specific assessment methodology which focuses on CRM systems has not been identified" (Kim 2010, p. 108).

Wheeler (2011, p. 10) and Romano & Fjermestad (2007) support a depth in defence approach which is aimed towards achieving information security. Compliance is achieved by protecting CRM data, the application, network, and perimeter through many individual and complimentary controls. Adopting the ISO standard and the depth in defence approach, managing risk will require many related privacy and security, which collectively mitigate one or more risks.

ISO27001 is an ISMS that forms the "consensus or general approval of all interests affected by it based on the consolidated results of science, technology, and experience aimed at the promotion of optimum community benefits and approved by a body recognised at the national, regional, or international level" (Boss 2000, p.7). Organisations of all types and sizes "collect, process, store and transmit information in many forms including electronic, physical and verbal" (ISO/IEC 27002, p. 7). Information is a business asset, which is subject to deliberate and accidental threats. Therefore, organisations can choose the controls that they believe will collectively mitigate their risks in the most cost-effective and organisationally consistent way.

Whilst organisations can implement technical controls and business rules that they believe will protect their CRM data against known threats, these controls and business rules will not always protect them against evolving threats. "[M]odern environments present dynamic behaviors *(sic)* at different scales and, in some contexts, many operations on client and mobile hosts are difficult or impossible to be controlled by system administrators" (Pierazzi et al. 2016, p. 29).

Malthouse et el. (2013, p. 276) highlight that there is a trend towards aggregating data through data mining and data sharing activities, increasing the significance, and requirement, for privacy and security controls in the foreseeable future. Implementing CRM security controls requires organisational personnel to understand their CRM model, the applicable security risks, and be aware of evolving or complex threats to their organisation. ISO27001 requires an understanding of security threats, not just technical mitigation controls. CRM applications generally need to be hosted so they can be made centrally available. “Staff [also require] knowledge of hardware, storage, networking, security, and virtualization (*sic*)” to ensure CRM privacy and security risks are adequately mitigated. “It can be very difficult to find employees who have all of this knowledge” (Rountree & Castrillo 2014, p. 42), as well as a broader understanding of organisational goals, budget, and processes (Seitz 2006).

CRM Security

A CRM security assessment method could consider the fundamental pillars of information security (information assurance), known as the CIA Model (Wheeler 2011, p. 10). An ISMS aims to protect against CIA threats towards information (ISO/IEC 27001:2013, p. 5).

The CIA principle comprises of (Donaldson et al. 2015, p.33):

> **Confidentiality –** Assurance that information is not disclosed to unauthorised individuals, processes, or devices;
>
> **Integrity** – Protection against unauthorised creation, modification, or destruction of information;
>
> **Availability** – Timely, reliable access to data and information services for authorised users.

Wheeler (2011) proposes a fourth element, extending the CIA model to include **Accountability**. Accountability is the “[p]rocess of tracing, or the ability to trace, activities to a responsible source” (Wheeler 2010, p. 10). This updated principle is referred to as CIAA. CIAA ensures the accountability component of the model to achieve the enforcement of the CIA principles. The CIAA principle allows organisations to align security with privacy. For example, a user logging into a system is a security control measure that prevents unauthorised access to data. This process maintains the confidentiality and integrity of an organisation’s data, maintaining the privacy of CRM data.

Organisations are being challenged by a more mobile and diverse workforce, which intersects with their employee's personal lives and hardware. Policies and controls are not easily enforced and security is a moving target (Wheeler 2011, p. 18). Modern cybersecurity threats challenge existing rule based controls because they seek to circumvent them in new ways. Attacks have become more covert and sophisticated where potential hackers want to steal data to hold the organisation for ransom (Donaldson et al. 2015, p. 59). More and more, organisations are using cloud based services where their network perimeters are not fixed (Wheeler 2011, p. 17). Real-time analysis and feedback appears essential to keep CRMs secure, as single or multiple controls may not apply to complex situations. Donaldson et al. (2015, n.p.) states,

> "[i]f only the solution were to buy a technology, plug it in to your network, and sit back and relax while technology takes care of the security challenges. Maybe someday some smart researchers will develop such a technology, but it doesn't exist today."

ISO27001 is currently "the best-known standard … for an information security management system" (Gasiorowski-Denis n.d.). ISO standards are internationally recognised and externally certifiable. This would enable CRMs to be assessed, and certified, by an independent third party against a comprehensive set of organisational wide security criteria. An ISMS could be achieved through implementing "a suitable set of controls, including policies, processes, organizational (*sic*) structures and software and hardware functions" (ISO/IEC 27002, p. 6) specific to a CRM. The assessment methodology would prioritise the "limited resources to implement the best security for the available budget" (Donaldson et al. 2015, n.p.), which would be applicable to the different CRM models. This could be challenging, as each organisation will have their own unique risks, controls and resource limitations, and each CRM model presents different considerations. CRM applications that currently exist may not follow the identified models.

Santos-Olmo et al. found that a lack of re-usable resources existed to streamline and simplify the implementation and maintenance processes of an ISMS. This resulted in SME's abandoning an ISMS, like ISO27001, concluding the process was too expensive and complicated for SME (Santos-Olmo et al. 2016, p. 5). Santos-Olmo et al. (2016) also found that by linking risks to their controls, this led towards achieving increased security automation and real-time compliance. In turn, this enabled organisations to implement an ISMS more successfully and at a reduced cost.

Apart from ISO27001, a newer security framework exists, called NISTCSF. NISTCSF focuses on digital information security, and seeks to "[i]dentify and prioritize (*sic*) opportunities for improvement within the context of a continuous and repeatable process" (NIST 2014, p. 4). Like ISO27001, NISTCSF recognises that organisations will have unique risks, tolerances, threats and vulnerabilities, and the application of NISTCSF will differ. Kuligowski (2009) discusses the differences between NISTCSF and ISO27001 standards, highlighting that NISTCSF is primarily used by United States of America Government agencies and or their contractors. Whereas, ISO27001 has been primarily adopted by information technology firms, financial firms, and business industries outside of government. The ISO27001 standard provides for a broader CRM security assessment method, especially in countries where privacy legislation may be different.

Privacy

An agreed definition of what 'privacy' is, does not exist. The term 'privacy' can be traced back to antiquity, where Aristotle (384–327 BCE) made the distinction between the political (public) sphere and the domestic (private) sphere (Romano & Fjermestad 2007, p. 71). The modern concept of information privacy has its origins with the invention of the newspaper and photography, when the law did not protect an individual to control information about themselves (Romano & Fjermestad 2007, p. 72). Arguably, this has become an issue again in contemporary times with the ever-increasing digitisation of information.

Romano & Fjermestad (2007, p. 78) argue that "[t]here is an adage that you cannot ensure privacy if you do not first have security".

There are two long standing theories of privacy. The first theory, **States of Privacy** is described by Margulis (2003, as cited in Romano & Fjermestad (2007, p. 72)) as:

> **Solitude** – an individual separated from the group and freed from the observation of other persons;
>
> **Intimacy** – an individual as part of a small unit;
>
> **Anonymity** – an individual in public but still seeks and finds freedom from identification and surveillance; and
>
> **Reserve** – based on a desire to limit disclosures to others; it requires others to recognise and respect that desire.

The second theory, **Functions of Privacy** is described by Margulis (2003, as cited in Romano & Fjermestad (2007, p. 72)) as:

> **Personal Autonomy** – desire to avoid being manipulated, dominated, or exposed by others or control over when information is made public;
>
> **Emotional Release** – release from the tensions of social life such as role demands, emotional states, minor deviances, and the management of losses and of bodily functions. Privacy, whether alone or with supportive others, provides the "time out" from social demands, hence opportunities for emotional release;
>
> **Self-Evaluation** – integrating experience into meaningful patterns and exerting individuality on events. It includes processing information, supporting the planning process (for example, the timing of disclosures), integrating experiences, and allowing moral and religious contemplation; and
>
> **Limited and protected communication** – limited communication sets interpersonal boundaries; protected communication provides for sharing personal information with trusted others.

Information collection and use is a core function of all CRM models. Once an individual has provided their information to an organisation, they rely on the organisation to respect and protect their privacy. They also trust the organisation to managed their personal information in accordance with the organisation's privacy policy, if they have one. Individuals constantly balance their desire for communication and disclosure with their desire for privacy (Margulis 2003, as cited in Romano & Fjermestad (2007, p. 72)). From a privacy risk mitigation perspective, information can be vulnerable when at rest, during processing, and whilst being transmitted (Wheeler 2011, p. 8). Whilst the CIA principle ensure information is more secure, the Australian Privacy Principles (APPs) ensure that Australian organisations manage personal information in a consistent, transparent, and agreed way. In each and every country, "[p]rivacy is frequently defined and specified by government regulations that include disclosure requirements and penalties for breaches" (Donaldson et al 2015, p. 455). In Australia, the *Privacy Act 1988* (Cth) (*Privacy Act*) regulates privacy principles for handling personal information.

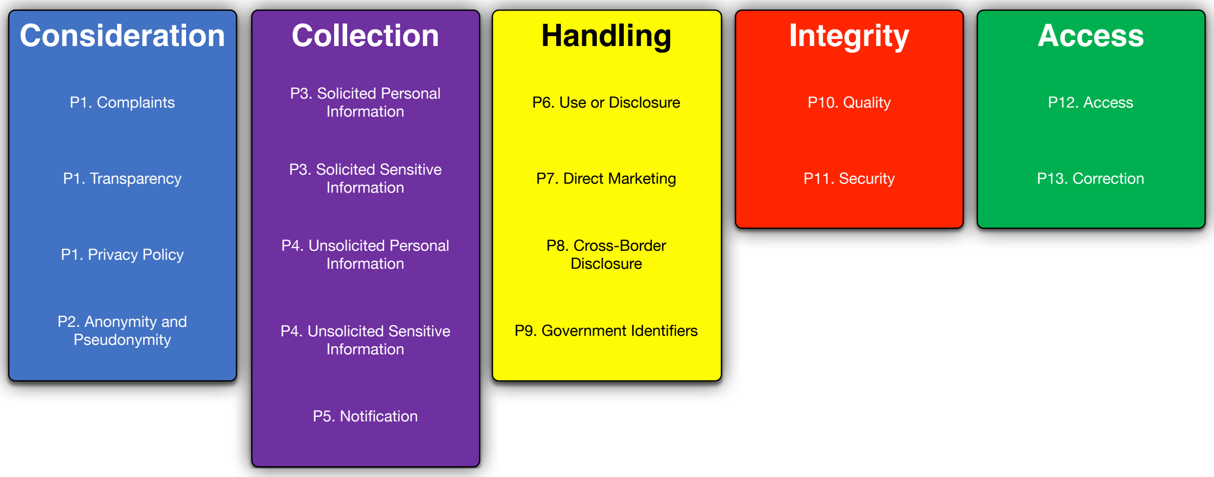
Information Privacy

The *Privacy Act* regulates the protection of privacy and transborder flows of personal information to meet Australia's international law obligations (OAIC 2015b). The purpose of the *Privacy Act* is to "give effect to the right of persons not to be subjected to arbitrary or unlawful interference with their privacy, family, home and correspondence" (preamble to the *Privacy Act*). The *Privacy Act* aims to provide a set of nationally consistent principles, the APPs, as defined in schedule 1 of the *Privacy Act*. The APPs promote the responsible and transparent handling of personal information, balanced with the interests of those carrying out functions or activities. Like ISO27001, the APPs must be interpreted and applied in a cost-effective and organisationally consistent way. Since 25 February 2015, the *Privacy Act* has been amended 13 times (*Privacy Act* endnote 3), demonstrating that privacy compliance is also a continuous improvement process. Therefore, any attempt to automate compliance with the *Privacy Act* will be an iterative process in line with the PDAC principle of ISO27001.

The APPs confer a right on individuals to resolve privacy complaints against those who infringe upon their rights. Most privacy protection requirements can usually be waived by the individual at the time of collection, except for the collection of sensitive information (Kobsa 2001, p. 307). Sensitive information is defined as a record with information containing racial or ethnicity, political opinions or memberships, religious beliefs, philosophical beliefs, sexual orientation, criminal history or health (including genetic) information (*Privacy Act*).

The APPs are a legal compliance requirement for “most Australian and Norfolk Island Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses (collectively called ‘APP entities’)” (OAIC 2015a). When collecting sensitive information, an agency must conform to a higher level of privacy compliance. For example, an agency must not collect sensitive information unless it is reasonably necessary for the functions or activities of the agency (OAIC 2014). Each organisation will have specific compliance requirements under the APPs depending on their functions, the type of information they collect, revenue, and the nature of the organisation. Organisations will need to adapt privacy controls to their legal compliance requirements.

The privacy principles are divided into five broad categories (Figure 5).



Consideration	Collection	Handling	Integrity	Access
P1. Complaints	P3. Solicited Personal Information	P6. Use or Disclosure	P10. Quality	P12. Access
P1. Transparency	P3. Solicited Sensitive Information	P7. Direct Marketing	P11. Security	P13. Correction
P1. Privacy Policy	P4. Unsolicited Personal Information	P8. Cross-Border Disclosure		
P2. Anonymity and Pseudonymity	P4. Unsolicited Sensitive Information	P9. Government Identifiers		
	P5. Notification			

Figure 5 Categories for Compliance (OAIC 2014)

Automating Privacy in CRMs

The W3 consortium attempted to address privacy compliance for web based information systems by drafting the Platform for Privacy Preferences (P3P) framework. P3P is a computer-readable XML format for digital privacy policies, enabling organisations to express their data collection and primary activities (Reagle and Wenning 2000). P3P allowed an individual to set their own privacy preferences via their web browser. When an individual visited a web site, the websites' P3P policy was validated against the individual's privacy preferences. An exception alert was generated when a privacy violation occurred. The individual could choose to provide their consent to proceed, otherwise the web site would be blocked from loading. Whilst the P3P system required an individual to rely on the organisation to protect their privacy, the P3P system allowed an individual to provide their informed consent at the time their personal information was collected. P3P also allowed and individual to understand how their information was being used without reading the organisation's privacy policy. Unfortunately, "P3P only check[ed] if their expectations [were] matched against promises made by the enterprise, and [did] not provide mechanisms to check and prove upfront compliance with fine-grained constraints" (Pearson & Allison 2009, p. 77).

P3P was not widely adopted by the web industry, and from the release of Windows version 10 in July 2015, Microsoft removed P3P support from their web browser (Microsoft 2017). As the P3P standard was not a legal compliance requirement, industry leaders, such as Google and Facebook, provided compliant P3P headers in their web based information systems for older browsers. However, their P3P policies did not actually protect privacy. The P3P header existed to ensure older web browsers did not block their sites from loading. Due to a bug in Internet Explorer, the P3P header would not be blocked when an invalid policy was provided to the browser, ensuring that entities could easily bypass privacy requirements (Cranor 2012). This was done without deceiving an individual. The individual was unaware their privacy controls were being ignored.

Meta Data

The modern risk to privacy is meta data. The *Privacy Act* does not specifically cover meta data. The Australian Privacy Commissioner ruled that meta data can be classed as personal information "if it can be pieced together so that an individuals' identity can be reasonably ascertained" (Nicholson & Puranikmath 2015). The Federal Court in the *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4 (19 January 2017) held that meta-data was not personal information. However, if meta-data is to be considered personal information the Federal Court stated it must be:

(i) held by the organisation;
(ii) "about" the individual who requested access; and
(iii) about and individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

IP addresses, and related meta data, were deemed not to be 'about' an individual and not personal information. The *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* requires that Australian Telecommunication Service Providers keep for at least two years meta data for an individual such as:

- source and destination of communication;
- date, time and duration; and
- location information.

Meta data enables dynamic information delivery (Kobsa 2001, p. 303). For CRMs, meta data could include an individual's cookies, login time, hardware, and location information. This enables a CRM to build a history of an individual's browsing habits and their interests, across multiple web sites (Network Advertising Initiative 2017). Meta data provides highly targeted opportunities for advertising and delivering content to individuals. However, there is a greater opportunity to identify an individual. Whilst meta data is generally non-identifiable when used as a single identification factor, when aggregated it can facilitate easier identification resulting in the ability to contact or precisely locate someone, as well as identify their behaviours (Network Advertising Initiative 2017). "Web browsing … sets are generated as side effects of human interaction with technology, [which] are subjected to the same idiosyncrasies of human behavior (*sic*), and are also sparse and high-dimensional" (de Montjoye 2015 et al., p. 539) with a high unicity score.

Unicity is the term used to quantify how much additional information would be required to identify a specific individual within an anonymised data set (de Montjoye 2015 et al.) and varies depending on the data. High unicity scores are more likely to result in an individual's identification, as it is easier to link individuals to their unique data profile within a large and anonymised data set. "The unicity of [a] data set naturally decreases with its resolution" (de Montjoye 2015 et al., p. 538). However, knowing additional data points within datasets increases the likelihood of re-identification.

de Montjoye's study identified meta data can be used to identify an individual's behaviour over time by analysing credit card transactions. The study analysed 1.1 million credit card transactions spanning a three-month period. The study found that by analysing meta data from four unique transactions, re-identification of 90% of all individuals was possible. The study concluded higher income earners were more easily identified, as were women, which suggests a link with higher credit card use and gender specific spending habits. Categorising customers to differentiate them (a core concept of many CRM models) presents similar privacy challenges.

Linking one data set with another may introduce identifiers that can identify the individual more easily. The APPs define an identifier as a letter, number or symbol, which identifies an individual without using their name or ABN (*Privacy Act*). Entities need to consider the unicity score of their own data sets when collecting data and undertaking data mining activities, especially in relation to non-identifiable and sensitive information. Unicity is a metric which could be used as a scoring metric by the dynamic compliance model to determine the likelihood that a privacy breach will result.

Generally, the collection of meta data typically occurs without express written consent from an individual and is generated because of providing information services to them. An individual has little control over what meta data is collected and can vary greatly between entities. An individual is also unaware of what other systems are linked to the CRM containing their personal information, or how the organisation combines their information internally to decrease the unicity score.

CRM Hosting Environments

Each CRM application identified by Gartner (Figure 6) differs in their implementation of privacy and security features. Controls will vary based on an organisation's maturity, size, and resources. For example, the Microsoft Dynamics CRM can be deployed on premise (IaaS) and in the cloud (SaaS). In contrast, the SalesForce CRM can only be deployed in the cloud (SaaS). Gartner predicts that that 50% of organisations will choose SaaS CRM applications in 2017 (Maoz & Manusama 2016), suggesting CRM security will be largely cloud (SaaS) hosted. Wheeler (2011) and Pierazzi et al's. (2016) argue that security and privacy threats will continue to evolve and dynamic compliance through data mining is required to identify and mitigate new threats.

has been removed due to copyright restrictions

Figure 6 Gartner's leading CRM application providers, which must support web and mobile channels (Maoz & Manusama 2016)

Automatic Classification and Compliance

Pearson & Allison (2009) propose that automatic compliance can be achieved by "checking for specific technology availability and its configuration" (Pearson & Allison 2009, p. 68). Whilst Pearson & Allison recognise automation is complex, automated compliance can be achieved if "a logical combination of subgoals may be satisfied" (Pearson & Allison 2009, p. 65). Organisations could be deemed compliant based on meeting a combination of smaller compliance goals. Compliance checking should verify that the "control is configured correctly, the control is available, the control has not been subverted and there is proper separation of the duties defined for specific roles" (Pearson & Allison 2009, p. 65). Controls that meet the CIAA principle will align to this definition and this approach could support automated compliance of ISO27001.

Data mining can be used to enable dynamic privacy and security controls by predicting the likelihood of a security or privacy incident, through analysing CRM data and meta-data. **Predictive tasks** seek to identify one value, based on the values of other independent variables. **Descriptive tasks** seek to identify and "derive patterns" (Tan, Steinbach & Kumar 2005, p. 7) from the data, which "summarises the underling relationships in the data" (Tan, Steinbach & Kumar 2005, p. 7). The proposed CRM model would require pre-processing capabilities to (Xu et al. 2014, p. 1149):

- Remove noise and inconsistencies from data;
- Be able to select and transform data features (attributes) ready for data mining;
- Extract and evaluate patterns to form new knowledge.

Pierazzi et al. (2016) propose that automated anomaly detection should be linked with preliminary investigations of the data to determine the most suitable algorithm to use. Their model assessed network security alerts to determine which anomaly detection method would best apply. Pierazzi et al. (2016) identified that each data mining algorithm has its own limitations. The proposed CRM model and associated risk management methodology will explore the limitations of using mining of CRM data for security and privacy.

Whilst CRM data mining has typically been used to enhance profitability, credit card companies use sensitive information such as “credit limit, age, annual income and address” to detect anomalous transactions (Kumar, Steinbach & Tan 2005, p. 11). Non-fraudulent transactions can build a profile of a legitimate user’s behaviour. This method, known as anomaly detection, identifies outliers in the data sets. The observation “differs so much from other observations as to arouse suspicion that it was generated by a different mechanism” (Kumar, Steinbach & Tan 2005, p. 653). The goal of anomaly detection is to achieve a high level of accuracy with minimal false alerts. The quality and type of data available will affect the choice of algorithm, as well as the security and privacy considerations. For example, techniques like the Nearest Neighbour or Naive Bayes classifier are well suited to small datasets based on probabilistic outcomes. By combining prior knowledge of events with their data attributes, it becomes possible to predict the likelihood of events based on past behaviour with reasonable accuracy (Kumar, Steinbach & Tan 2005, p. 228). These classifiers could form one control of an overall control strategy to prevent likelihood of an anomalous event from occurring. This multi-control approach is consistent with the depth in defence approach, so that a single identifier would not become its own security risk.

Each data mining algorithm will have different data and setup requirements. There are four main training models, depending on data requirements:

- **Supervised** – training relies on providing examples to the model which provide the model with classification data. This is useful for identifying known normal and anomalous behaviour, and the model is expected to reproduce this behaviour;
- **Semi-supervised** – is like supervised, except the model consumes unlabelled attributes;
- **Weakly supervised** (or boot strapping) – relies on a minimal training data set, and then positive training examples through re-enforcement;
- **Unsupervised** – learning which aims to finding structures within data, without training data. This learning style looks at the data and classifies it to find patterns or clusters.

Scoring risk using existing CRM data is not as simple as assigning quantitate values to existing data, and then multiplying the likelihood of an event and with the impact or severity. The majority of CRM data is unstructured (Buttle & Maklan 2015, p. 288). Analysis becomes more difficult because the raw data requires pre-processing such as "feature selection, dimensionality reduction, normalisation and data sub setting" (Tan, Steinbach & Kumar 2005 p.3). Quantitative analysis relies on data being available to support analysis which is reliable is available and reliable (Standards Australia 2013, p. 61).

Deriving qualitative data from existing data sets is also restricted by the type of data available and the calculations that can be performed on them:

- **Nominal** – Labels with no quantitative value and good for frequency distribution analysis or mode (determining the most frequent choice);
- **Ordinal** – Relative, order based choices with no quantitative value;
- **Interval** – Order based choices, where the quantitative differences between the values can be measured. For example, the difference between CRM activity date times could be expressed as a measure of seconds. These measurements can also determine mode, median, mean or standard deviation values used in determining risk scores. Interval scales can have addition and subtraction techniques, but not multiplication or division, as there is a no true zero. For example, multiplying a choice by three, would not be equal to three times the first choice;
- **Ratio** – A range of order based choices, where the difference can be quantified, and absolute zero is known.

The proposed risk assessment methodology does not yet feature a mechanism to determine a partial likelihood score. Simple multiplication of the current likelihood score (0 or 1) could calculate a high impact risk with low likelihood to be considered of equal importance as a low impact and highly likely event (Lark 2015, p. 48). This can be explored in future research.

Privacy Preserving Data Mining in CRMs

PPDM is an emerging, and privacy focused, data mining approach that aims to "safeguard sensitive information from unsolicited or unsanctioned disclosure, and meanwhile, preserve the utility of the data" (Xu et al. 2014, p. 1150). Yang & Wu (2006) identify "bioinformatics, CRM/personalization (*sic*) and security applications" (Yang & Wu 2006, p. 602) as current data mining application fields where PPDM might be suitable. They have not identified any requirements for privacy preserving privacy and security assessment methods. Yang & Wu (2006) identify that data accuracy trade-offs exist with PPDM methods and are not well understood or standardised. Ji & Elkan (2010) propose that data can be anonymised by comparing and weighting the data with similar known and published data sources. This preserves the relationships and knowledge within the data. Pathak & Raj (2010) propose a classification algorithm that adopts a differential privacy framework. This adjusts privacy strength with the number of records, allowing the utility of the data to be preserved. Xu et al. (2014) propose privacy preserving roles within the data mining process, identifying some of the PPDM limitations and strategies for different data mining algorithms.

Performance

Al-Shawi (2011) identifies automated detection is challenged by large data sets and diverse variables within the data. IDS and IPS data mining activities are temporal, requiring algorithms to achieve high capacity data driven decisions in real time.

Chapter 3. Prototype CRM

SAS providers are responsible for providing access to a CRM system, typically, through a web browser or mobile application. Maoz & Manusama 2016 argue that 50% of CRMs will be built as SAS products in 2017. SAS providers are responsible for managing and supporting the customer's CRM application, hardware, and hosting, as well as the privacy and security responsibilities of the customer's information available to users.

Prototype CRM Overview

A simple web based prototype CRM was built (per Figure 7) to run on a SAS based architecture (see Figure 17). This prototype enabled the case study to assess the CRM against the ISO27001 framework without having to navigate complex ethical, technical, and commercial considerations as ISO27001, ideally, requires access to commercially sensitive information. The prototype CRM was a reasonable first step to ensure the proposed CRM Model is worth validating with further research and real-world use cases.

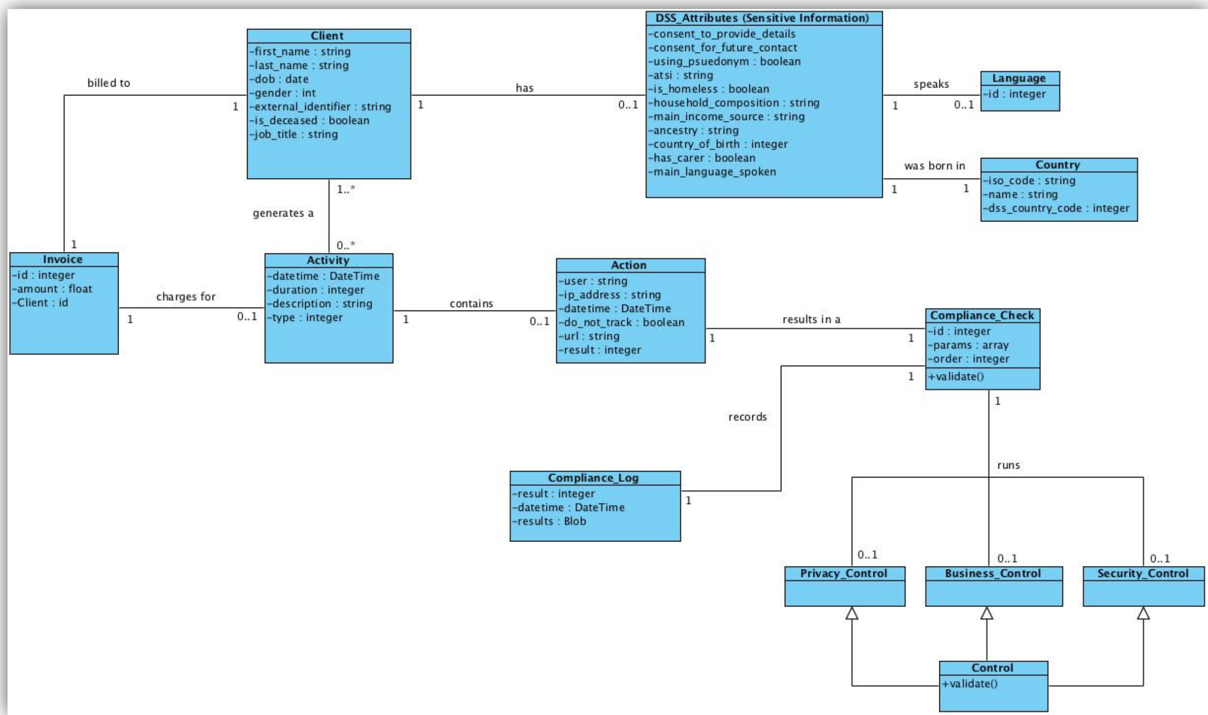


Figure 7 Class diagram for prototype CRM, demonstrating how the compliance check is triggered by a user action or risk scenario (Kwiatkowski 2017a)

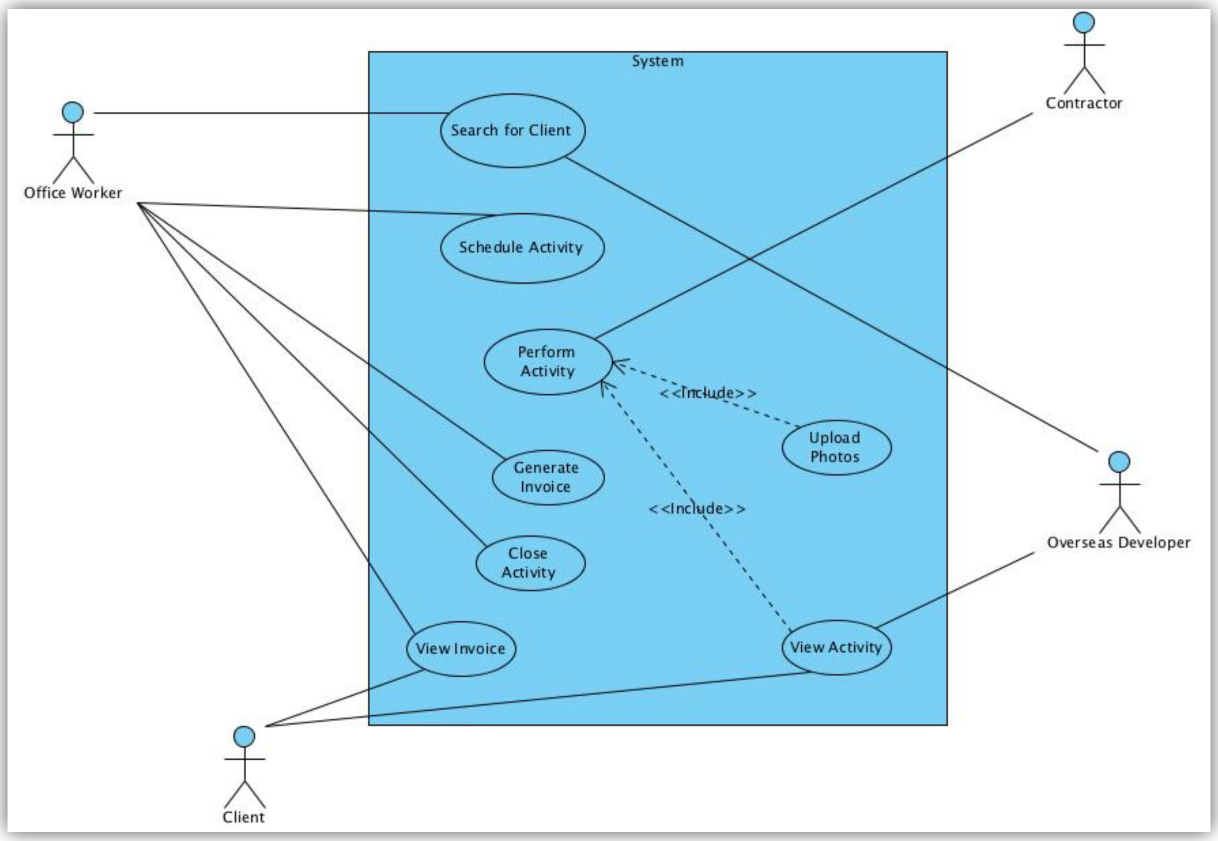


Figure 8 Use case diagram showing different actors accessing the prototype CRM (Kwiatkowski 2017c)

Figure 8 outlines the sample use cases explored to build the prototype CRM. The use case diagram identifies that users (actors) will need to interact with the CRM system and what goals they want to achieve. The prototype CRM applies a compliance check each time the user interacts with the prototype CRM. Figure 9 and Figure 10 show how the compliance check is triggered in the same way for two different use cases.

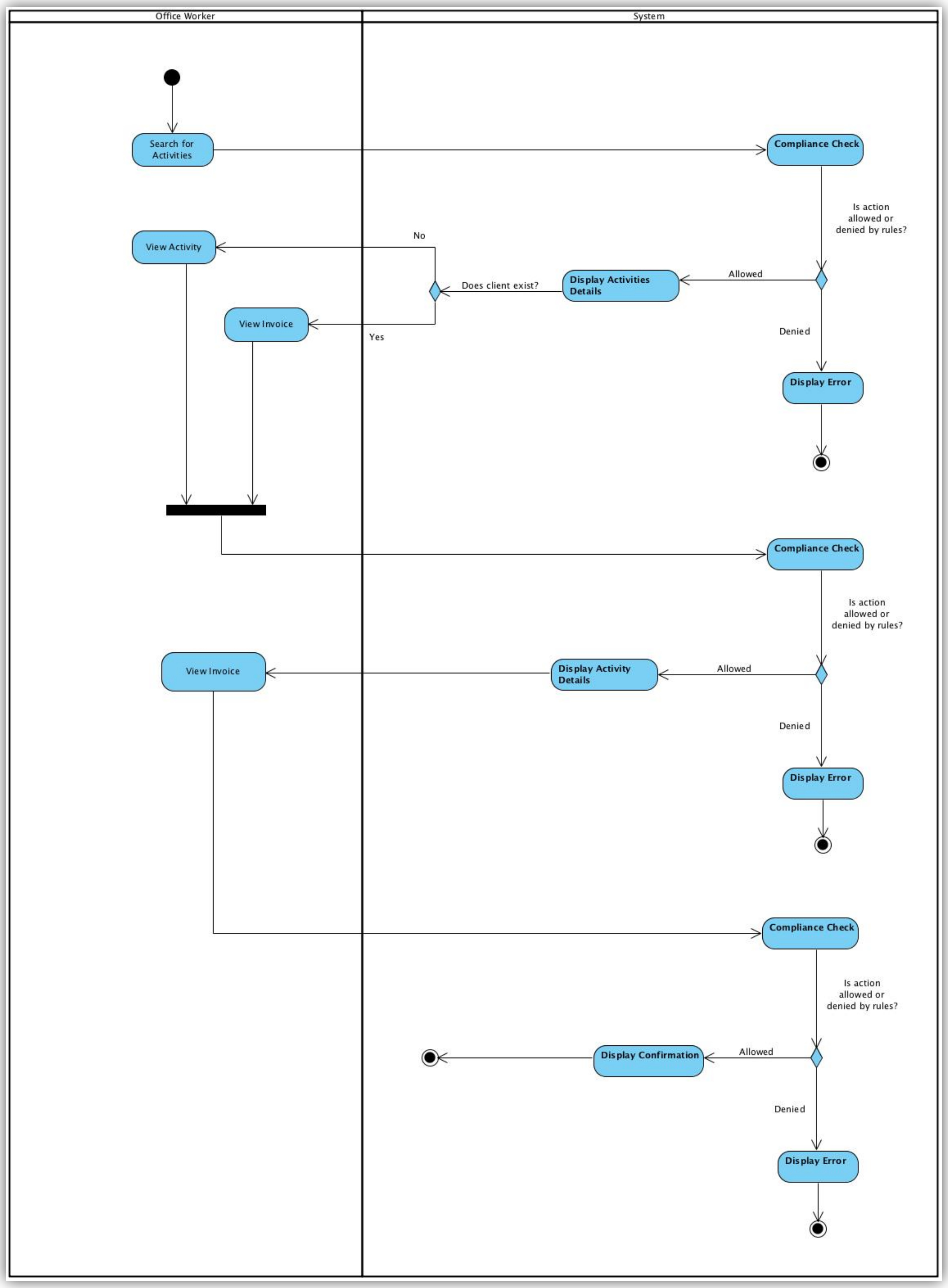


Figure 9 Workflow diagram demonstrating how a user triggers compliance check on each interaction with system (Kwiatkowski 2017d)

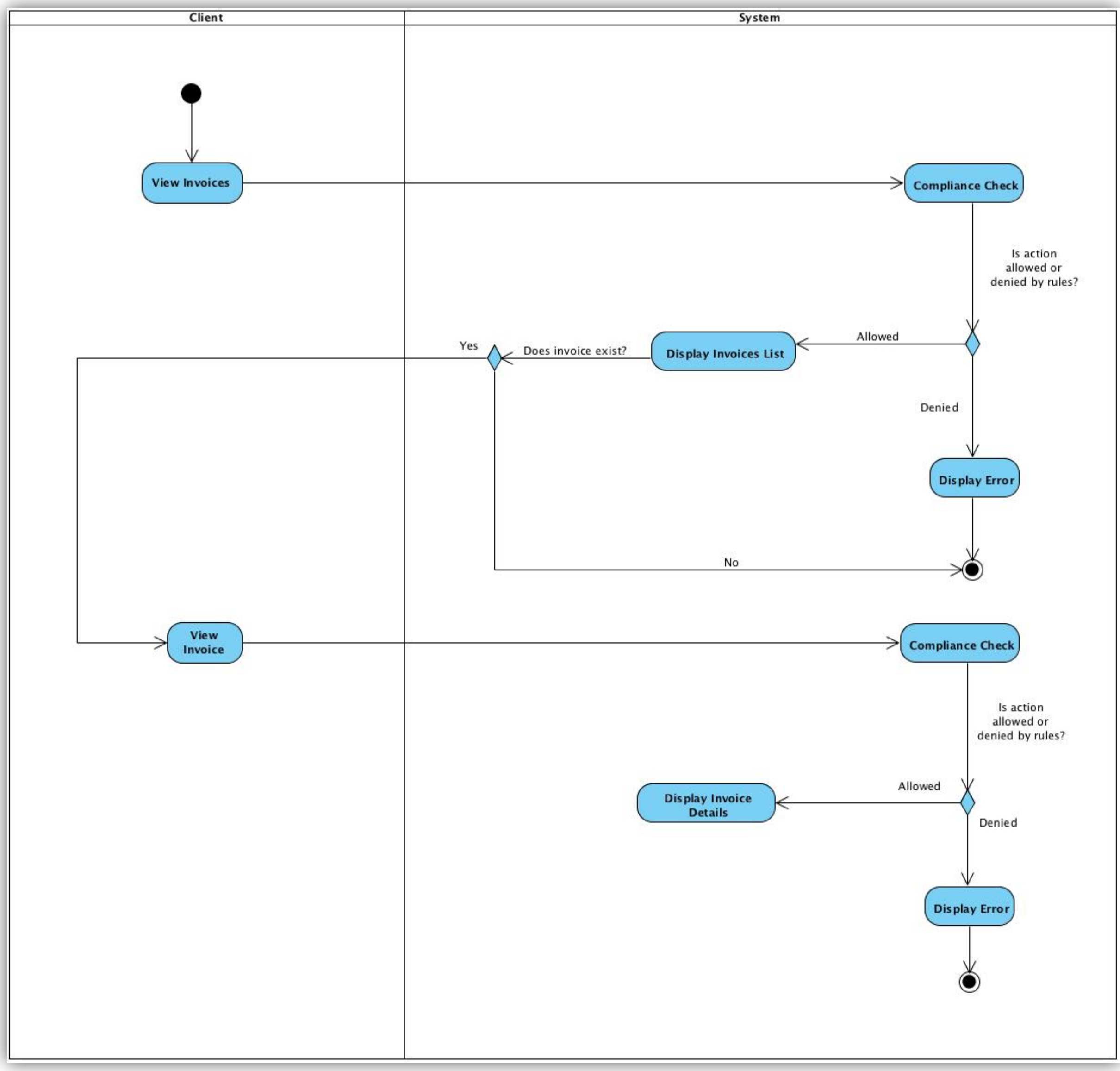


Figure 10 Workflow diagram for when a client accesses the prototype CRM. The purpose of the diagram is to illustrate the similarity with Figure 9 when triggering a compliance check for a different action and role (Kwiatkowski 2017e.

Proposed CRM Model

Rather than building the prototype CRM based on an existing CRM model, a new proposed CRM model was created to address the lack of compliance, evaluation and reporting within them. The proposed CRM model remedied the lack of visible privacy and security controls required to achieve ISO27001 automation. Whilst existing CRM models could have been evaluated against ISO27001 standard, the literature review identified that CRM risks should be linked to corresponding mitigation controls, which will help evaluate their effectiveness and achieve real-time compliance. This will make it possible for organisations to increase their ISMS implementation success rate and decrease implementation costs (Santos-Olmo et al. 2016), especially for SMEs.

The initial proposed CRM model (Figure 11) was the first attempt to build a new CRM model to address privacy and security gaps in existing CRM models. The initial model increased the visibility of the privacy and security functions (compared to existing CRM models), and provided a mechanism to perform real-time compliance checks. Compared to the proposed CRM model in Figure 12, the initial model lacked the tools and processes required for a CRM to function. The differences between Figure 11 and Figure 12 highlight that a CRM is more than just a web site system with a compliance checking layer.

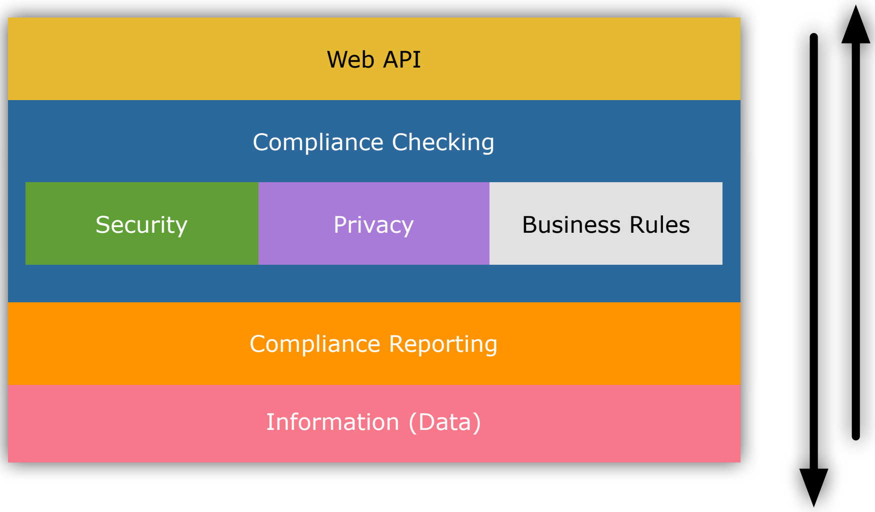


Figure 11 Initial model (Kwiatkowski 2016)

The proposed CRM model in Figure 12 incorporates the key capabilities of the existing CRM models in Figure 1, Figure 2, Figure 3 and Figure 4.

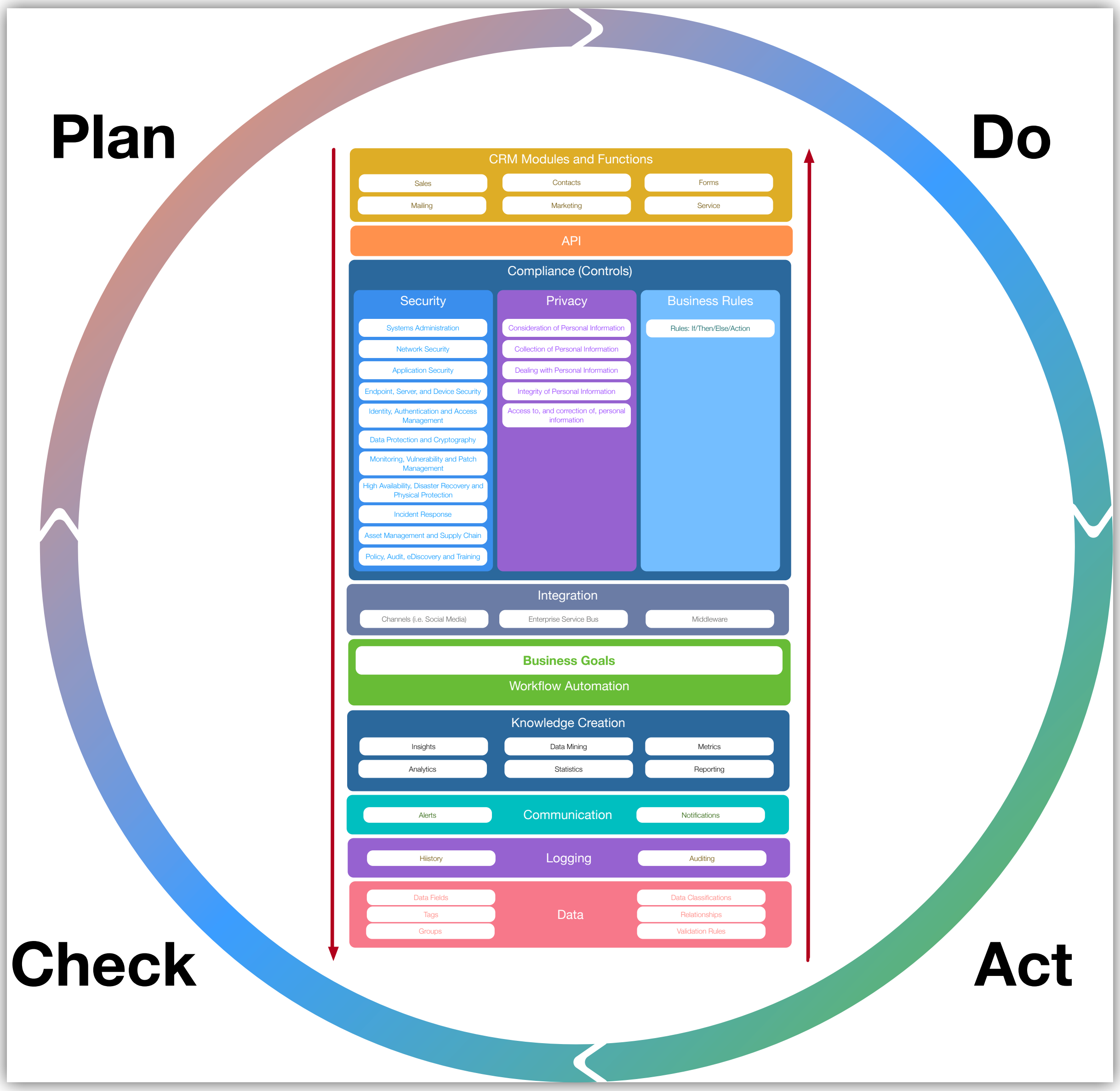

Plan
Do
Check
Act
CRM Modules and Functions
Sales
Contacts
Forms
Mailing
Marketing
Service
API
Compliance (Controls)
Security
Systems Administration
Network Security
Application Security
Endpoint, Server, and Device Security
Identity, Authentication and Access Management
Data Protection and Cryptography
Monitoring, Vulnerability and Patch Management
High Availability, Disaster Recovery and Physical Protection
Incident Response
Asset Management and Supply Chain
Policy, Audit, eDiscovery and Training
Privacy
Consideration of Personal Information
Collection of Personal Information
Dealing with Personal Information
Integrity of Personal Information
Access to, and correction of, personal information
Business Rules
Rules: If/Then/Else/Action
Integration
Channels (i.e. Social Media)
Enterprise Service Bus
Middleware
Business Goals
Workflow Automation
Knowledge Creation
Insights
Data Mining
Metrics
Analytics
Statistics
Reporting
Alerts
Communication
Notifications
Hiistory
Logging
Auditing
Data Fields
Tags
Groups
Data
Data Classifications
Relationships
Validation Rules

Figure 12 Proposed CRM Model (Kwiatkowski 2017f)

The proposed CRM model in Figure 12 requires that information must be brokered through the compliance layer at each stage of the transaction(s). This keeps information secure, which ensures privacy personal information is maintained (Romano & Fjermestad 2007, p. 78). In the existing CRM models, privacy and security are assumed to be functions of the information technology layer, or supporting processes. For example, the Value Chain CRM Model (Figure 1 *above*), Payne's and Frow's 5-process CRM model (Figure 2 *above*), and Gartner's CRM Model (Figure 3 *above*) defer privacy and security to the information technology layer without it being evident as to how security and privacy compliance is managed. Information systems are not typically designed to be secure and comply with the ISO standard (ISO/IEC 27002, p. 7).

By moving compliance to its own layer, the focus can move towards reactive and preventative security controls as data leaves or enters the CRM. The compliance layer ensures the CRM's "statement of overall intentions and direction" (ISO31000 2009, pg. 2) align with the risk attitude to "pursue, retain, take or turn away from risk" in real-time (ISO31000 2009, pg. 2). This visibility facilitates the automated continuous improvement requirement recommended by Santos-Olmo et al. (2016). This will save on ISO27001 implementation cost and reduce complexity, especially for SMEs. Customer information, meta data, and processes that were previously leveraged to create profit generation can also be leveraged to apply privacy and security controls specific to individuals and their behaviours. The dynamic control is an example of this.

Appendix A outlines the many logical steps and processes required to implement the ISO27001 standard. Figure 13 provides an easier to follow overview of the compliance process, artefacts and visualisation of the PDAC principle.

Figure 13 ISO27000 ISMS Framework (Lark 2015)

ISO27001 was evaluated for this thesis because when ISO standards can become aligned with business drivers, the result can be increased revenue and capacity. This is consistent with CRM goals. Greater profitability can be achieved through greater efficiency, increased quality, reduction of errors, easier compliance, and increased customer confidence and loyalty (ISO 2014). ISO27001 is also applicable to organisations of all sizes in many countries with different types of CRM software.

ISO27001 does not mandate the technology or controls required for CRMs. The framework provides a mechanism for organisations to hold themselves accountable to their own security practices that can then be externally audited. Every organisation will have different levels of risks, resources, and controls design to mitigate risks. ISO27001 has the advantage of providing governments, organisations, and consumers with confidence that personal information is being managed internally according to international best practice. It provides the flexibility required for each organisation to mitigate their strategic, operational, and analytic CRMs with controls specific to their circumstances and resources. Conversely, this subjective nature of ISO27001 does not guarantee a CRM will be secure by its use, and the controls chosen must be adequate to mitigate the risks an organisation faces. From a customer's perspective, ISO27001 demonstrates the organisation's commitment to security risk management.

When implementing ISO27001, significant resources are spent implementing "control measures to prevent attacks being successful, but relatively little time talking about detecting and responding to attacks when they occur. Preventative controls are good, but they will not actually stop a determined attack" (Donaldson et al. 2015, p. 31). The performance of the proposed CRM model is evaluated to demonstrate how the model detects and responds to attacks in real-time. This is the first logical step in achieving automated compliance with ISO27001.

Risk Management Methodology

The 2013 revision of ISO27001 requires organisations to select their preferred risk management methodology. Currently, no CRM specific risk assessment methodology currently exists. For the same reasons ISO27001 was adopted, ISO31000 risk management framework was chosen. ISO31000 is also compatible with ISO27001. The risk management process seeks to identify, analyse, and group "the effect of uncertainty on objectives" (ISO 31000:2009, 2015 p. 13) within the proposed risk assessment methodology, by evaluating, ranking and developing controls that mitigate the uncertainty and consequence (Flaus 2013, p. 20). ISO31000 also supports the PDAC principle through the risk management activities of planning, implementation, monitoring and review, and improvement.

While ISO27001 defines the iterative process to manage privacy and security, ISO31000 provides a framework (steps and process) to manage the risk within it. Risk results from the deficiency in information related to the consequences and likelihood of an event (Lark 2015, p. 12). Objectives are derived by an organisation's strategic plan, which typically links revenue targets, compliance, legal requirements, and other strategic goals related to organisational governance. This enables the risk management process to be linked directly to business drivers, manage uncertainty associated with risk, and support organisational goals at different levels (Lark 2015, p. 12). Linking controls to organisation goals is critical for ISO27001 success, especially for SMEs (Santos-Olmo et al. 2016).

Uncertainty is a key element of risk and can result from information being unavailable, inaccessible or inaccurate (like CIA). The risk can be reduced by determining the likelihood of an event occurring and the potential consequences related to CIA principles. Based on the perceived value of the information, appropriate controls can be implemented to reduce the risk. Tolerable risks should be reduced, if not cost prohibitive, and acceptable risks require no reduction (Flaus 2013, p. 45). Risk controls should outline the decisions to be made, document the risk criteria to be applied, define accountability and circumstances for the decision. Risk scoring could enable the assessment of objectives against acceptable and unacceptable risk, where distributions (a range of numbers) can be used to indicate risk tolerance rather than a single value (Standards Australia 2013, p. 60). A scoring system for the proposed risk assessment methodology could be explored in future research.

Figure 14 shows the proposed risk assessment methodology to be evaluated. The methodology is based on the Bow Tie method to manage risk. The methodology links CRM risks to their controls and controls to their impacts, as recommended by Santos-Olmo et al. (2016). The Bow Tie method has been used within “process industries not only to analyse risk but also to communicate hazard and risk findings to a broad audience” (Sutton 2015, Chapter 5, Section 16, para. 1). Figure 14 provides an overview on how each control will be used collectively to reduce the likelihood of the main risk event occurring. The hazards must be present (pre-conditions) for the main event to be able to occur, such as the CRM being connected to the internet and an existing user being active in the system. The proposed risk assessment methodology visually links many individual controls to their impact, such as loss of sales, key risk indicators (KRIs). For example, a KRI of “Increased Spam Email” might mean the risk of “Malware” or a “Remote Malicious” attack is more likely in the risk environment.

The proposed risk assessment methodology enables a number of control strategies as recommended by Donaldson et al. (2015). These include:

- **Preventative** controls, which block threats;
- **Detective** controls, which detect risks and generate alerts;
- **Forensic** controls, which verify the effectiveness of controls and enable investigations; and
- **Audit** controls, which seek to limit ongoing risks.

The evaluation of the proposed risk assessment methodology will determine the effectiveness of using preventative and detective controls. Forensic and audit controls can be explored as part of future research.

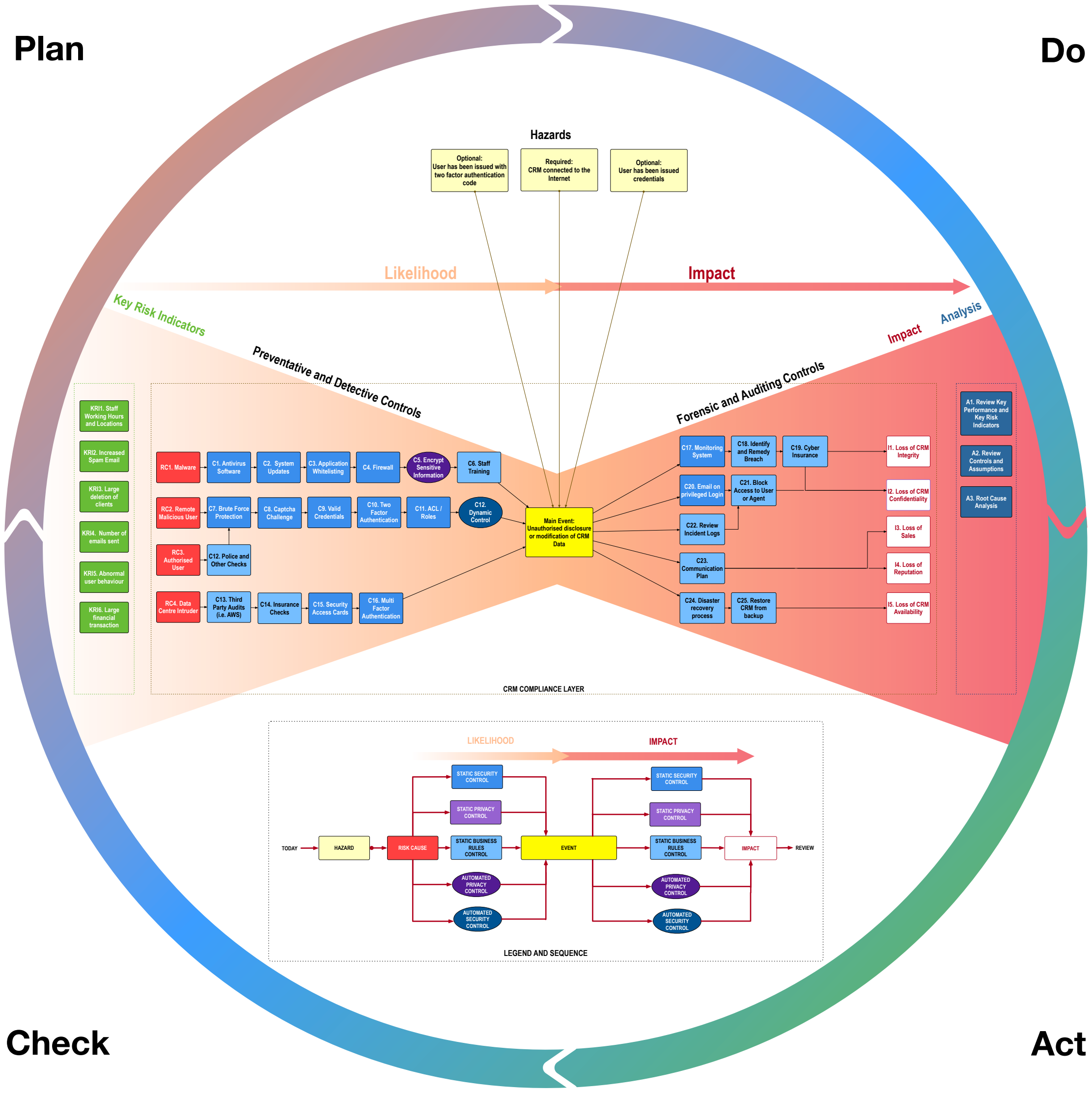

Plan
Do
Check
Act
Hazards
Optional: User has been issued with two factor authentication code
Required: CRM connected to the Internet
Optional: User has been issued credentials
Likelihood
Impact
Key Risk Indicators
Preventative and Detective Controls
Forensic and Auditing Controls
Impact
Analysis
KRI1. Staff Working Hours and Locations
KRI2. Increased Spam Email
KRI3. Large deletion of clients
KRI4. Number of emails sent
KRI5. Abnormal user behaviour
KRI6. Large financial transaction
RC1. Malware
C1. Antivirus Software
C2. System Updates
C3. Application Whitelisting
C4. Firewall
C5. Encrypt Sensitive Information
C6. Staff Training
RC2. Remote Malicious User
C7. Brute Force Protection
C8. Captcha Challenge
C9. Valid Credentials
C10. Two Factor Authentication
C11. ACL / Roles
C12. Dynamic Control
RC3. Authorised User
C12. Police and Other Checks
RC4. Data Centre Intruder
C13. Third Party Audits (i.e. AWS)
C14. Insurance Checks
C15. Security Access Cards
C16. Multi Factor Authentication
Main Event: Unauthorised disclosure or modification of CRM Data
C17. Monitoring System
C18. Identify and Remedy Breach
C19. Cyber Insurance
C20. Email on privileged Login
C21. Block Access to User or Agent
C22. Review Incident Logs
C23. Communication Plan
C24. Disaster recovery process
C25. Restore CRM from backup
I1. Loss of CRM Integrity
I2. Loss of CRM Confidentiality
I3. Loss of Sales
I4. Loss of Reputation
I5. Loss of CRM Availability
A1. Review Key Performance and Key Risk Indicators
A2. Review Controls and Assumptions
A3. Root Cause Analysis
CRM COMPLIANCE LAYER
LIKELIHOOD
IMPACT
TODAY
HAZARD
RISK CAUSE
STATIC SECURITY CONTROL
STATIC PRIVACY CONTROL
STATIC BUSINESS RULES CONTROL
AUTOMATED PRIVACY CONTROL
AUTOMATED SECURITY CONTROL
EVENT
STATIC SECURITY CONTROL
STATIC PRIVACY CONTROL
STATIC BUSINESS RULES CONTROL
AUTOMATED PRIVACY CONTROL
AUTOMATED SECURITY CONTROL
IMPACT
REVIEW
LEGEND AND SEQUENCE

Figure 14 Proposed Risk Assessment Methodology (adapted from the Bow Tie method) (Kwiatkowski 2017g).

The proposed risk management methodology supports the PDAC process of ISO31000 in Figure 15 in a similar way to ISO27001. This is required to achieve automated compliance.

has been removed due to copyright restrictions

Figure 15 The ISO31000:2009 Risk Management Process (Lark 2015)

Compliance Layer

Figure 16 shows the link between the prototype CRM use cases, proposed CRM model and the proposed risk assessment methodology. The compliance check in the use cases triggers the CRM model's "compliance layer" when a user interacts with the system. The required controls are evaluated in accordance with the the proposed risk assessment methodology.

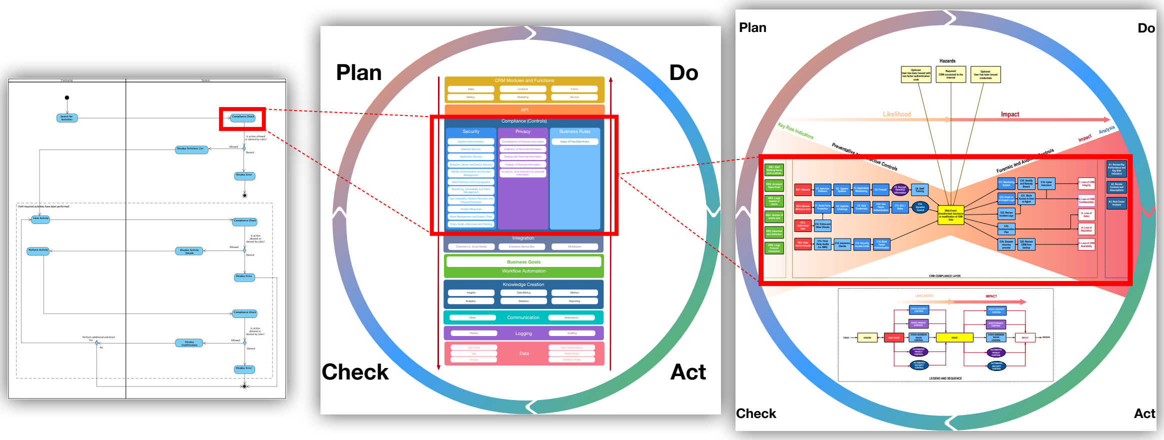


Figure 16 Prototype CRM (left) linked to the Proposed CRM Model (middle) linked to the Proposed Assessment Methodology (right) (Kwiatkowski 2017h).

Chapter 4. Methodology

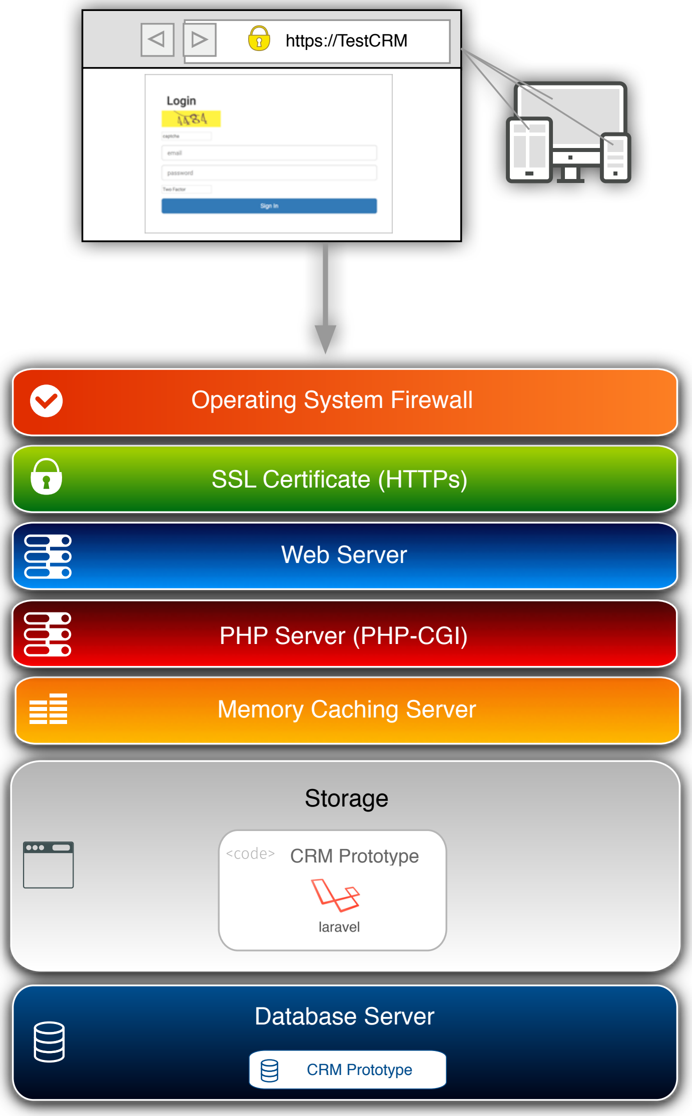


Figure 17 Technology stack for the CRM prototype (Kwiatkowski 2017b).

The prototype CRM was built as a web based software application to enable the proposed risk assessment methodology to be evaluated. The prototype CRM infrastructure is similar to other SAS based CRM products, like Salesforce (as identified by Gartner in the literature review), which are also delivered through a web browser. The prototype CRM code was written in the PHP programming language. PHP is a server-side scripting language that can be run on all major operating systems (PHP n.d.) and powers approximately 82% of web sites world-wide

(W3Techs 2017). By mirroring key elements of the SAS environment and using readily available technologies, the findings should be more easily adapted to existing SAS based CRMs. The prototype CRM also supports the IASS infrastructure model, where organisations can self-host and manage the CRM themselves. This requires greater technical expertise to manage than SAS, which SME may not have.

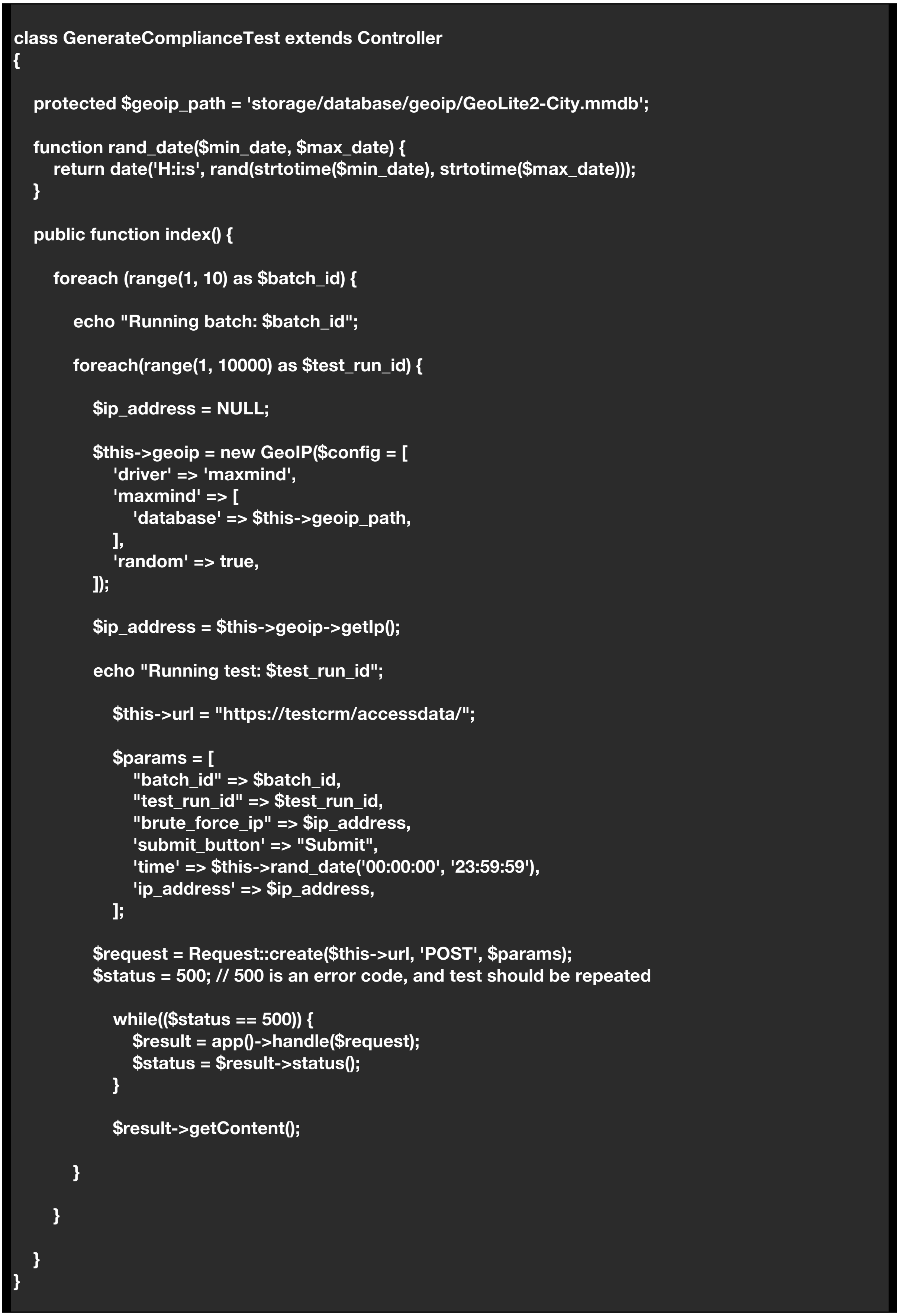
In Figure 17, the code “CRM Prototype” in the storage layer runs when the user requests access to the prototype CRM through their web browser. The user’s web browser connects to the web server. Then the web server passing the request to the PHP server. The PHP server executes the PHP code and returns the results back to the web server process. The web server then delivers the rendered content to the user through their web browser.

PHP supports a range of third party technologies such as database and memory caching extensions. The prototype CRM used the PHP MySQL extension, to connect the MySQL database server. The database was used to store client data, logging and meta data (PHP n.d.). The PHP Memcached extension was used to cache the training data for the dynamic control. The cache stopped the dynamic control from retrieving the training data set from the database on every user request, which greatly decreased the execution time to run the tests.

The CRM prototype was built utilising the Laravel framework, which provides “powerful tools needed for large, robust applications” (Otwell n.d.) that are beneficial when building PHP applications. The PHP Machine Learning (Kondas 2017) library was used to facilitate the creation and evaluation of dynamic controls. The library offered a variety of machine learning algorithms without having to build them. The Laravel-Captcha (Igoshev 2017) library was used to generate and validate the captcha control. The GeoIP library (Jalan 2017) provided access to the GeoIP lite database, which contained global IP address location information. This data was required by the dynamic control to calculate the distance between the server location (data location) and the user’s IP address on each request. Distance calculations were performed using the PHPGeo library (Jaschen 2017), which calculated the distance between IP addresses using the longitude and latitude values from the GeoIP database. In testing, some IP addresses had no longitude or latitude values, which meant the distance could not be calculated. These exceptions were set to a distance of 40,000km is roughly the size of the earth's circumference (Longhorn and Hughes 2015, p. 175). The large value is expected to highlight these exceptions easily in the results and should cause the control to fail, given that no training data will exist to pass these values.

Test Plan

The batch testing code in Figure 18 was executed to evaluate the effectiveness of the proposed risk assessment methodology in a variety of scenarios. This code executed 10 batches of 10,000 individual web requests against the prototype CRM system, with each request simulating a user attempting to login to the system.



```
class GenerateComplianceTest extends Controller
{

    protected $geoip_path = 'storage/database/geoip/GeoLite2-City.mmdb';

    function rand_date($min_date, $max_date) {
        return date('H:i:s', rand(strtotime($min_date), strtotime($max_date)));
    }

    public function index() {

        foreach (range(1, 10) as $batch_id) {

            echo "Running batch: $batch_id";

            foreach(range(1, 10000) as $test_run_id) {

                $ip_address = NULL;

                $this->geoip = new GeoIP($config = [
                    'driver' => 'maxmind',
                    'maxmind' => [
                        'database' => $this->geoip_path,
                    ],
                    'random' => true,
                ]);

                $ip_address = $this->geoip->getIp();

                echo "Running test: $test_run_id";

                    $this->url = "https://testcrm/accessdata/";

                    $params = [
                        "batch_id" => $batch_id,
                        "test_run_id" => $test_run_id,
                        "brute_force_ip" => $ip_address,
                        'submit_button' => "Submit",
                        'time' => $this->rand_date('00:00:00', '23:59:59'),
                        'ip_address' => $ip_address,
                    ];

                $request = Request::create($this->url, 'POST', $params);
                $status = 500; // 500 is an error code, and test should be repeated

                    while(($status == 500)) {
                        $result = app()->handle($request);
                        $status = $result->status();
                    }

                    $result->getContent();

            }

        }

    }
}
```

Figure 18 Test plan code for Prototype CRM (Kwiatkowski 2017i)

On each request made to the prototype CRM by the user, a series of controls were evaluated to aimed to prevent the main event from occurring per Figure 19.

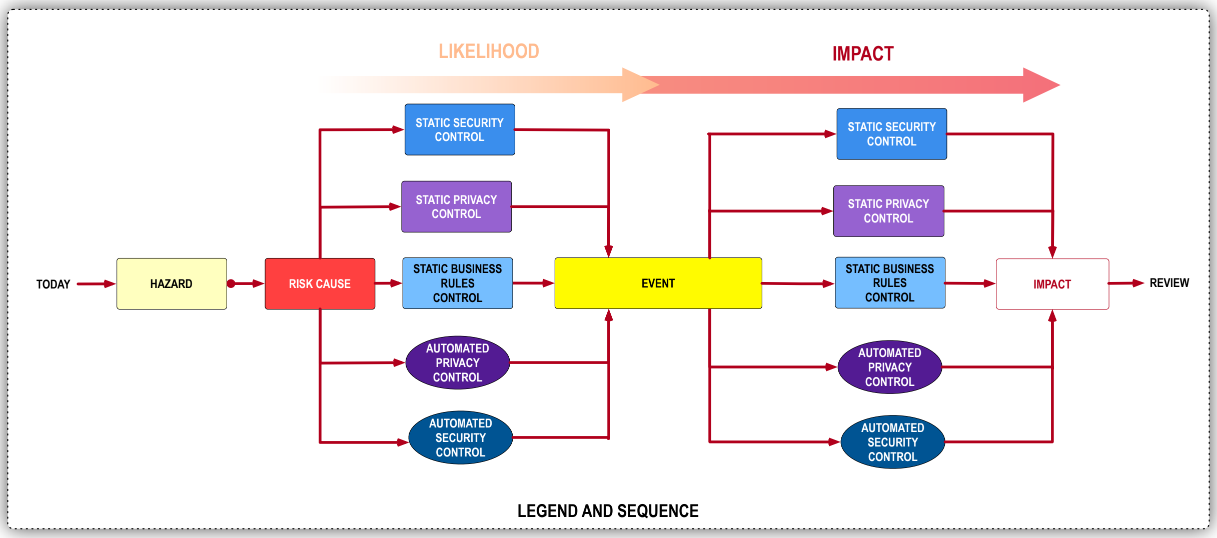


Figure 19 Proposed Assessment Methodology legend and sequence (Kwiatkowski 2017j)

$$\mathbf{r = (f1 <= c1) \;\&\; (f2 <= c2) \;\&\; (f3 <= c3) \;\&\; (f4 <= c4) \;\&\; (c5 = 1 \mid 0)}$$

f = is a random probability between the supplied min and max likelihood of the specific control failing at the time.

c = a random probability between 1 and 100 of the specific control failing at the time.

r = Is the likelihood (1 or 0) of the compliance check failing, determined by a bit wise operation on the result of each control.

Figure 20 The methodology used to determine the effectiveness of multiple controls working together, to collectively block the risk event from occurring. If any control fails then the request will be denied (Kwiatkowski 2017k)

Figure 20 outlines the formula used to calculate the compliance check result. To test the overall effectiveness of the CRM risk management methodology, each control was set to fail within a set range of probabilities (f). The validator would also generate a random number (c) - If c was less than or equal to f, then the control would fail. This enabled the model to be tested with a variety of failure probabilities, where each control could operate independently with a different failure rate.

Figure 21 applies the formula shown in Figure 20 to the controls evaluated in Figure 14. All controls may pass the compliance check, for the overall compliance check to pass.

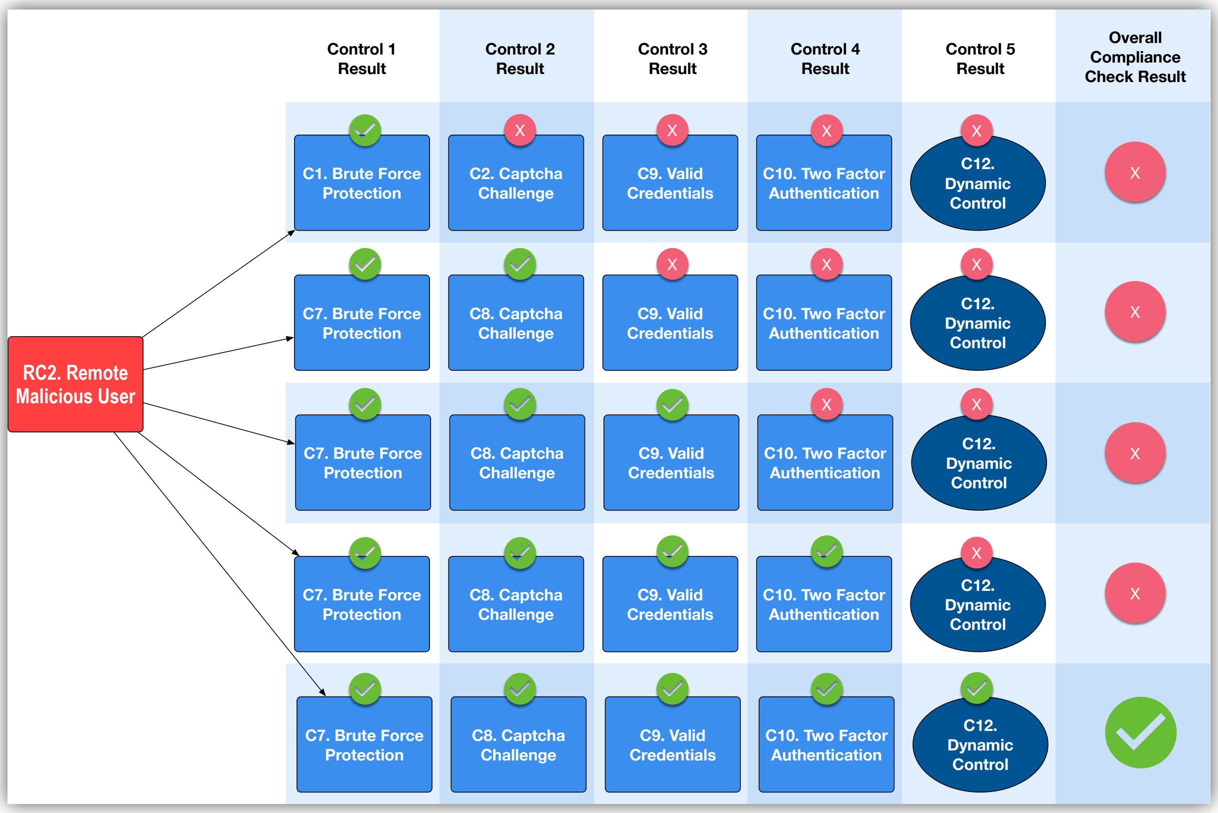


Figure 21 The compliance layer within the Proposed Assessment Methodology that validates a series of controls. All controls must be successful for the user action to be successful (Kwiatkowski 2017l)

Test Cases

Table 1 outlines the strengths and weaknesses of each of the controls being evaluated. The brute force protection control (C7) will detect and determine when a single IP submits a request more times than is allowed within a specified time frame. This control can easily be overcome by using dynamic IP addresses or slowing down the rate of attack. Similarly, the CAPTCHA challenge (Completely Automated Public

Turing test) (C8) aims to distinguish humans from machines by requiring the user to enter the code presented on the login form, as shown in Figure 23. Starostenko el at. (2015) found they could break the CAPTCHA through automated means with an accurate score ranging from 31% to 94%. Two factor authentication (C10) requires the user to enter a unique code that has been sent to the them for the login. It is possible for an attacker to intercept two-factor authentication codes that are sent to users by the mobile phone network, using the SS7 exploit (Thomson 2017). This exploit has been used by hackers to successfully transfer money from a victim's bank account to the attacker's bank account in Germany.

To simplify the testing process, the control role check (C11) was not included in the evaluation. It was presumed the user accessing the CRM would have access to view and download data within the prototype CRM.

Control Number	Test 1. Static Control Baseline Test		Test 2. Static Control Variability Test		Test 3. Static Control Variability Test with Dynamic Control		Control Weakness	Control Strengths
	Min	**Max**	**Min**	**Max**	**Min**	**Max**		
C7. Brute Force Protection	50	50	1	95	1	95	Stops brute force attacks from a single IP address.	A single source can attack by reducing attack speed.
C8. Captcha Challenge	50	50	1	85	1	85	Aims to verify a machine is not attacking the prototype CRM.	Can be broken by machine learning algorithms, or determined attackers.
C9. Valid Credentials	50	50	1	50	1	50	Unique per user. A valid username and password is required to login to the CRM.	Credentials can be stolen without user awareness.
C10. Two Factor Authentication	50	50	1	10	1	10	The second factor code is constantly changing, making it difficult to steal like a password.	SMS two factor can be intercepted.
C12. Dynamic Control	*Not performed*	*Not performed*	*Not performed*	*Not performed*	Result determined by classifier		Can identify specific user traits using CRM data and/or meta data to enhance existing controls.	Algorithms require selection, training and validation to learn expected behaviour. May not handle edge cases or suitable for all data types.

Table 1 Test Plan strategy overview (Kwiatkowski 2017m)

Compliance Checking Process

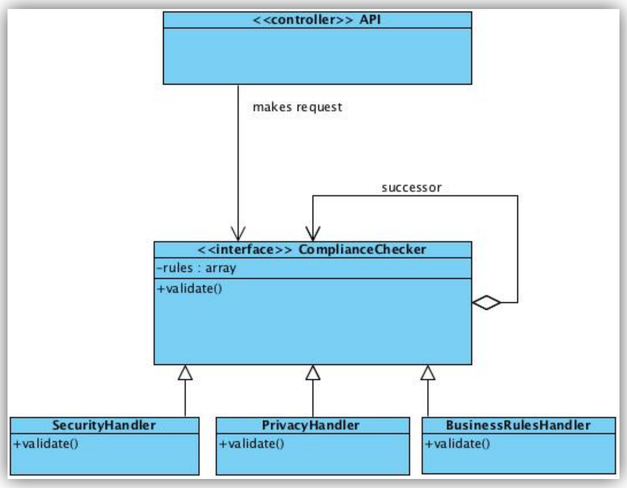


Figure 22 The compliance check process is triggered when a user makes a request against the Prototype CRM (Kwiatkowski 2017n)

Figure 22 demonstrates how the compliance check code was structured in the prototype CRM to perform compliance checks. The login page shown in Figure 23 implements a series of the controls which were added to the compliance checker in Figure 22. This is demonstrated by the code shown in Figure 24 where controls can be individually added to the compliance check for a particular resource or event.

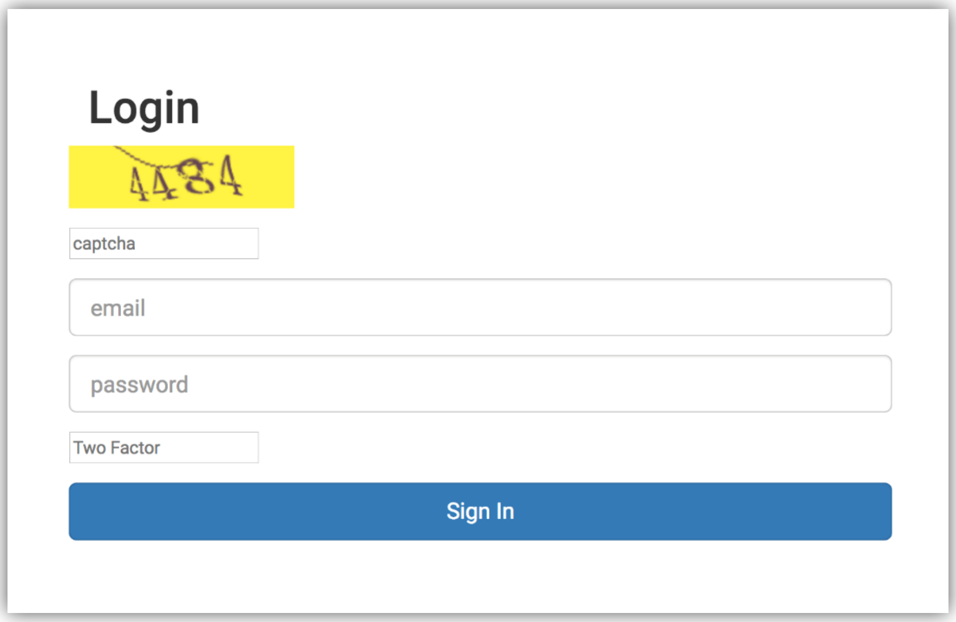
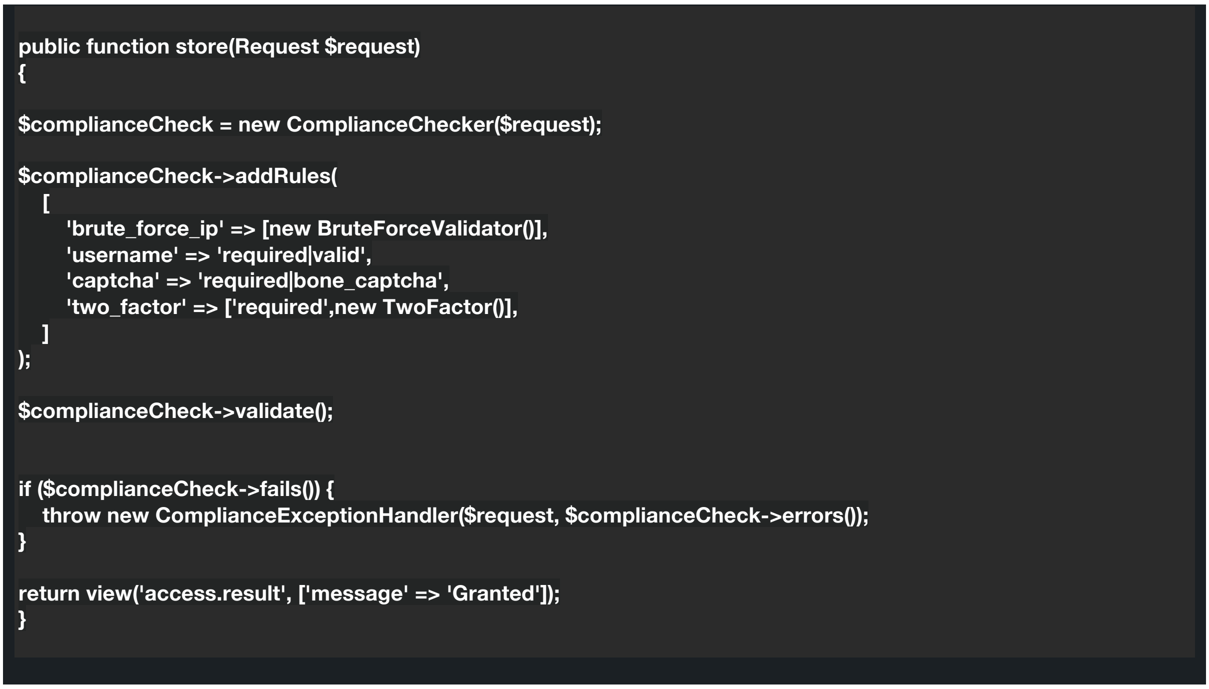


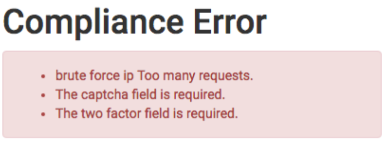
Figure 23 Testing the dynamic CRM compliance model. The login screen controller contains the controls designed to limit the likelihood of the main risk event (Kwiatkowski 2017o)

When a user submits the login form, the compliance check will validate the request by executing the code shown in Figure 24. If the compliance check fails, the user will be displayed the access denied error Figure 25. The user will be denied access to the information stored within the prototype CRM.



```
public function store(Request $request)
{

$complianceCheck = new ComplianceChecker($request);

$complianceCheck->addRules(
    [
        'brute_force_ip' => [new BruteForceValidator()],
        'username' => 'required|valid',
        'captcha' => 'required|bone_captcha',
        'two_factor' => ['required',new TwoFactor()],
    ]
);

$complianceCheck->validate();


if ($complianceCheck->fails()) {
    throw new ComplianceExceptionHandler($request, $complianceCheck->errors());
}

return view('access.result', ['message' => 'Granted']);
}
```

Figure 24 Compliance layer code (Kwiatkowski 2017p).



Compliance Error

- brute force ip Too many requests.
- The captcha field is required.
- The two factor field is required.

Figure 25 The login form validation results, shown when the user submits the login form. A compliance error is displayed to the user for each validation check that failed (Kwiatkowski 2017q)

Test Limitations

The web requests originated from a single test client (single computer), which communicated with the web server using a single IP address. It was not practical to manipulate the operating system time and IP address to generate the variations conditions required by the test plan. Each web request allowed the client to post data to the prototype CRM. The client set the IP address and access time randomly on each request. The IP address was generated randomly using the GeoIP database, and the access time randomly generated with a value between 0:00 and 23:59 hours. These random values were designed to simulate a user accessing the CRM from a different address, at random times world-wide.

Training the Dynamic Control

A dynamic security control was evaluated to protect privacy of information in the absence of a static control. The dynamic control used the k-nearest classifier algorithm, which is useful for anomaly detection. The algorithm can predict if the user should be accessing the prototype CRM based on past successful behaviour. The model was trained using supervised data, where 10,875 randomly generated and classified IP addresses, were passed to the model in the pattern shown in Table 2 and mapped for easier understanding in Figure 26. As Australia is geographically distant from other countries, Christmas Island was included to provide a possible edge case, where IP addresses from this region were geographically closer to Indonesia than the source of the data. The data was assumed to be hosted in Sydney's Amazon Data Centre. The training data simulated successful logins to the prototype CRM between 9am and 4.59pm, Australian Eastern Standard Time. The distribution of login times represented a good mix of login behaviour, where users would login to the prototype throughout the day. Future research could examine how this model would perform in countries with closer boundaries such as the European Union and with different work hours. The model could also be tested and applied specifically for each user, specific to their existing login behaviours.

Number of Records	Country of login	Login time by hour (24 hour)	Average Distance from Information (km)	Result
864	Australia	9	891.449306	Pass
853	Australia	10	878.651208	Pass
848	Australia	11	880.581333	Pass
880	Australia	12	850.392386	Pass
889	Australia	13	943.287942	Pass
880	Australia	14	896.001511	Pass
1	Christmas Island	14	5304.81	Pass
869	Australia	15	968.861772	Pass
1	Christmas Island	15	5304.81	Pass
1	Christmas Island	16	5304.81	Pass
873	Australia	16	868.708511	Pass

Table 2 Sample training data used by the Dynamic Control, which were classified as a pass (Kwiatkowski 2017r)

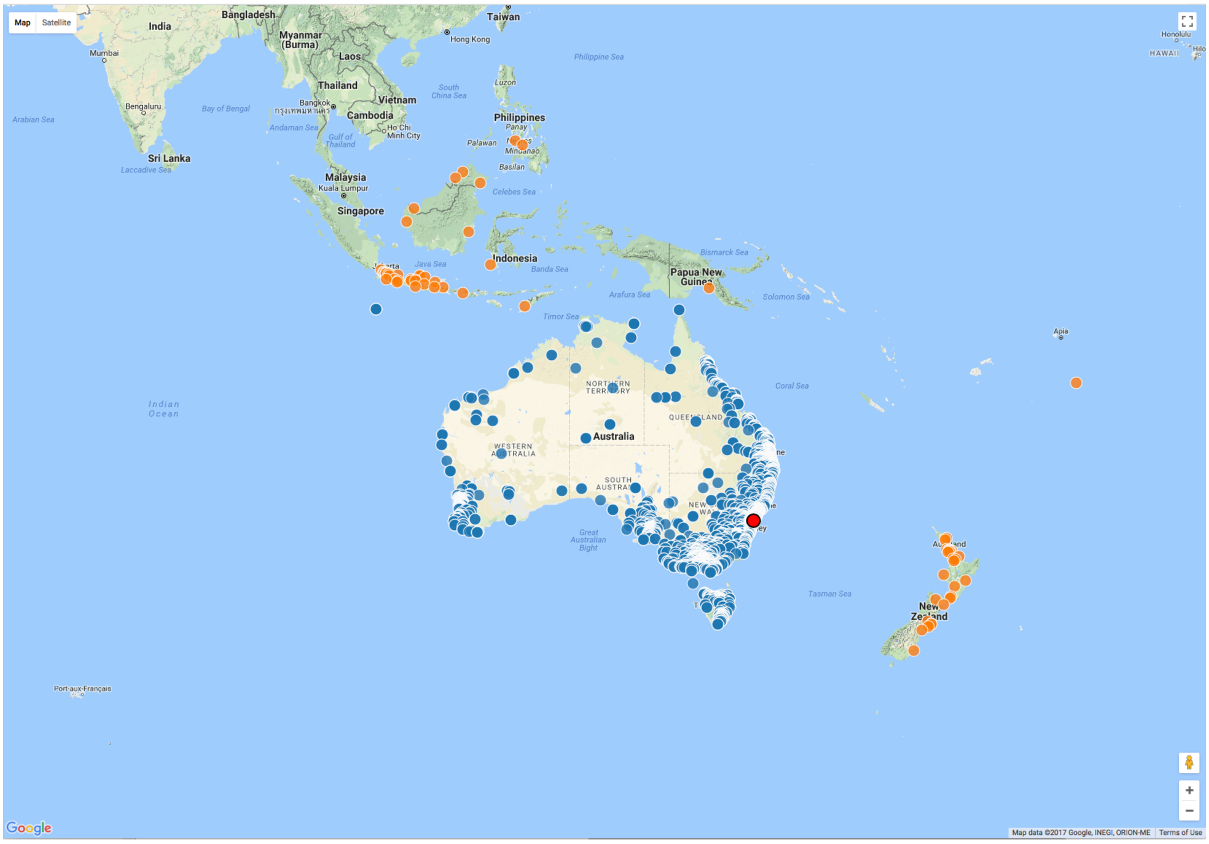


Figure 26 Map of training data (Kwiatkowski 2017ag)

[Blue = Pass, Orange = Fail, Red = Data Centre. Mapping software courtesy: Google Maps]

Table 3 shows a summary of the 3916 supervisor training records that were classified as known failures to the classifier. These simulated logins, from a malicious user, at a random time of the day.

Number of Records	Country	Login Hour (Min)	Login Hour (Max)	Average Distance from Information (km)	Result
922	United States	0	23	14503.02084	Fail
462	France	0	23	16987.17323	Fail
268	Germany	0	23	16374.34026	Fail
201	Italy	0	23	16371.28771	Fail
162	United Kingdom	0	23	17000.00006	Fail
145	Russia	0	23	13457.51069	Fail
134	Canada	0	23	15229.64254	Fail
123	Sweden	0	23	15763.19756	Fail
116	Brazil	0	23	14020.89371	Fail
104	Spain	0	23	17656.46664	Fail
94	Mexico	0	23	12975.93851	Fail
92	Netherlands	0	23	16623.54641	Fail
84	India	0	23	9691.336667	Fail
77	Poland	0	23	15702.30416	Fail
61	Norway	0	23	15890.90853	Fail
59	Hungary	1	22	15779.78695	Fail
55	Japan	0	23	7878.785091	Fail
48	Austria	0	23	16123.66875	Fail
47	Belgium	0	22	16737.14192	Fail
46	Switzerland	0	23	16627.74717	Fail
43	Czechia	0	23	15987.52488	Fail
43	Indonesia	0	23	5505.926744	Fail
40	Portugal	0	23	18106.41025	Fail
30	New Zealand	0	22	2172.825333	Fail
28	Finland	0	23	15161.73036	Fail
25	Turkey	0	21	14482.7816	Fail
25	South Africa	0	20	10922.5404	Fail
21	Argentina	0	23	11633.92619	Fail
20	Philippines	0	23	6206.072	Fail
18	China	0	20	8658.231667	Fail
17	Romania	1	21	15390.30588	Fail
16	Denmark	1	22	16167.605	Fail
15	Thailand	2	23	7582.022667	Fail

14	Slovakia	2	19	15756.09429	Fail
14	Malaysia	1	22	6406.602857	Fail
11	Greece	2	17	15436.43182	Fail
10	Vietnam	1	22	7236.243	Fail
226	Other (Combined)	0	23	13794.18245	Fail

Table 3 Sample training data used by the Dynamic Control, which were classified as a fail (Kwiatkowski 2017s)

Figure 27 shows the visual representation of the supervised training data supplied to the dynamic control. The training data did not include any IP addresses that did not have longitude and latitude information. Future research could test how the control would respond in these edge cases, or how other meta data could be used to enhance results.

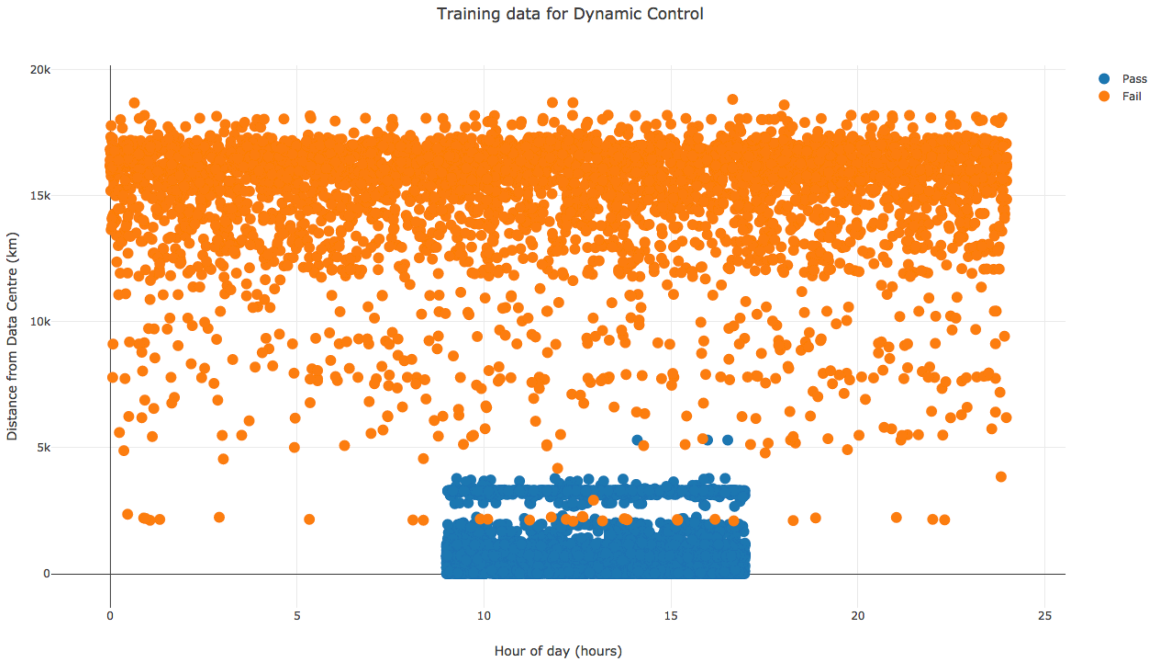


Figure 27 Dynamic control training data visualisation, with majority of pass results in Australia and Christmas Island (Kwiatkowski 2017t)

Testing Hardware and Software Specifications:

The test plan per Figure 18 took approximately 30 hours to generate the 100,000 test required on a system with the following specifications:

- iMac Retina 5K Late 2015
- 32GB system memory
- 1TB solid state hard disk
- 1 x 4Ghz processor with 4 cores.

The prototype CRM was built and tested using the following software versions:

- Apache 2.4, packaged with MAMP Pro version 4.2.1 (Gmbh 2017)
- PHP version 7.0, packaged with MAMP Pro version 4.2.1 (Gmbh 2017)
- Memcached version 1.4.32, packaged with MAMP Pro version 4.2.1 (2GB memory allocated to cache storage).
- MySQL version 5.6.35, packaged with MAMP Pro version 4.2.1 (Gmbh 2017)
- Laravel version 5.5 (Otwell 2017)
- BoneCMS captcha 1.1 (Igoshev 2017)
- PHP Geo 2.0 (Jaschen 2017)
- GeoIP 2.5 (Jalan 2017)
- PHP Machine Learning, version master (Kondas 2017)
- Google Chrome version 61.0.3163.100

Limitations

ISO27001 certification is performed as a two-stage audit process where documentation is reviewed, and then activities (controls) implemented by the organisation are checked against the documentation. This process must be followed by an internal auditor, and again by the management review team which implementation corrective and preventative actions identified through an audit (Kosutic, 2015). As ISO27001 is an organisational wide ISMS, the proposed risk assessment methodology may not be able to handle all aspects of ISO27001 compliance for the organisation. Some organisations are likely to have unique risks and controls, and the findings may not be relevant to them.

Randomisation lead to a higher number of IP addresses based in the United States of America in the training data per Table 3. This is presumably because the region has more IP addresses. The full impact of the limitation will need to be explored through additional research.

Chapter 5. Results

** indicates the **round half up** method was applied the number in the table. For example, this method would round the number 1.5 to 2, and the number 1.4 to 1.*

Summary of Test Results

Table 4 shows the average number of pass results for the three test types. The result shows the average of 10,000 requests for a total of 10 tests (10 x 10,000 per test type).

Controls	Test 1. Static Control Baseline Test	Test 2. Static Control Variability Test Results	Test 3. Static Control Variability Test with Dynamic Control
C7	5011*	4781*	4799*
C7, C8	2495*	2045*	2064*
C7, C8, C9	1248*	513*	532*
C7, C8, C9, C10	630*	29*	31*
C7, C8, C9, C10, C12	Not performed	Not performed	1*

Table 4 The average number of requests that were allowed by the compliance layer across the ten batches of tests for each test type (Kwiatkowski 2017u).

Figure 28 shows the data from Table 4 rendered in a bar graph format. Each column represents the average number of requests that were allowed by the compliance layer, for each test type. This compared how the variability of each control affected the uncertainty of overall risk.

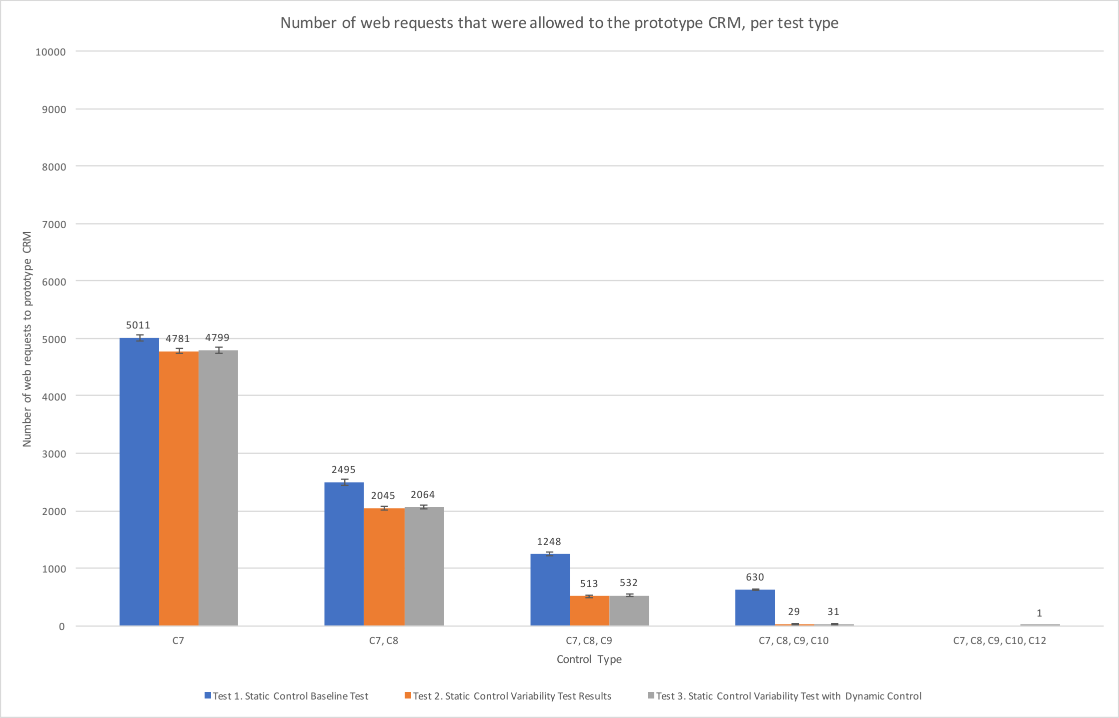


Figure 28 Comparison of the average number of requests that were allowed by the compliance layer for the three test strategies (Kwiatkowski 2017v)

Figure 29 shows the average number of requests allowed by the compliance layer between for all three tests, and the deviation between test types.

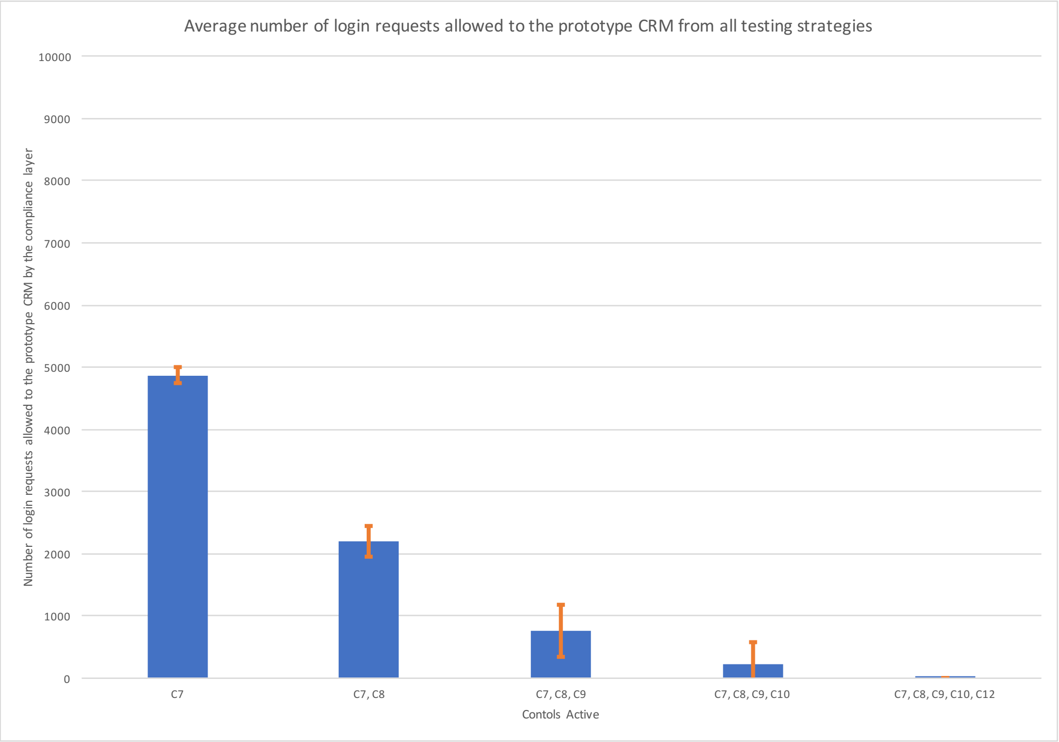


Figure 29 The average number of login requests allowed to the prototype CRM for all testing strategies (Kwiatkowski 2017w)

Effectiveness of Single Controls

Figure 30 shows the number of requests allowed by the compliance layer for each individual control, when operating independently.

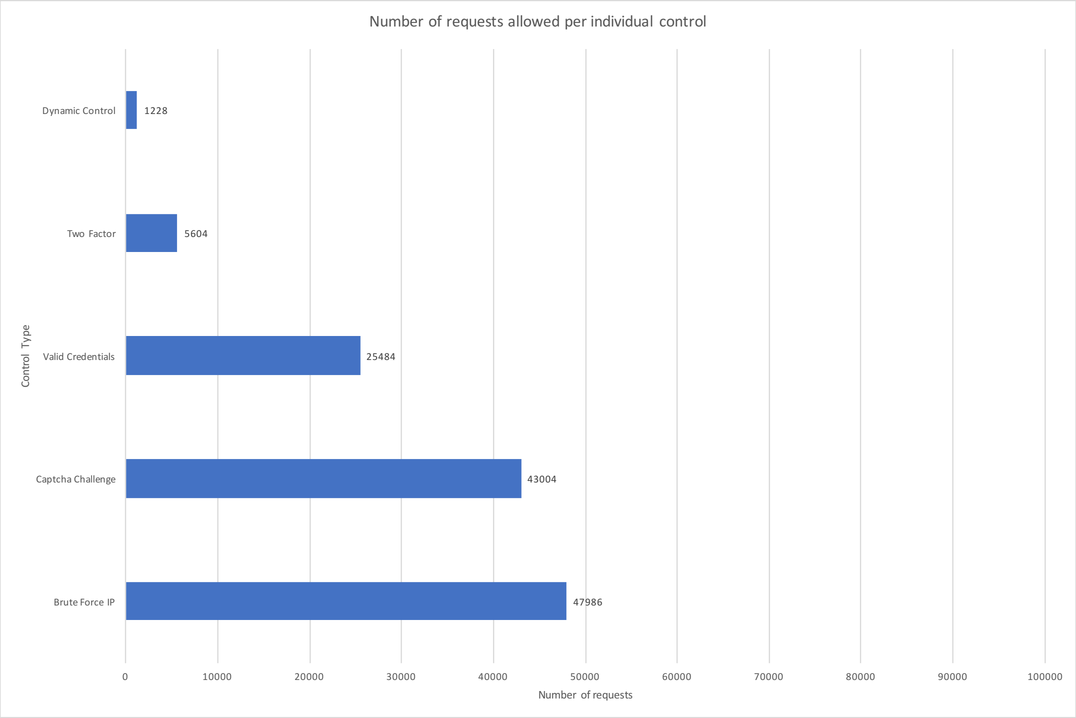


Figure 30 The number of requests that were allowed by the compliance layer for each control operating independently (not in combination with other controls) (Kwiatkowski 2017x)

Test 1. Static Control Baseline Test

Number of allowed requests granted by the compliance layer for Test 1.

Controls	Batch 1	Batch 2	Batch 3	Batch 4	Batch 5	Batch 6	Batch 7	Batch 8	Batch 9	Batch 10	Total	Average	Standard Deviation
C7	5056	5035	4946	4967	5063	4913	5025	5064	5084	4960	50113	5011*	60*
C7, C8	2542	2492	2459	2474	2541	2437	2589	2499	2472	2441	24946	2495*	49*
C7, C8, C9	1249	1237	1228	1237	1287	1212	1277	1275	1262	1215	12479	1248*	26*
C7, C8, C9, C10	640	612	600	616	626	627	649	633	661	633	6297	630*	18*
C7, C8, C9, C10, C12	Not performed												

Table 5 Test 1 results for the Static Control Baseline test (Kwiatkowski 2017y)

Test 2. Static Control Variability Test Results

Number of allowed requests granted by the compliance layer for Test 2.

Controls	Batch 1	Batch 2	Batch 3	Batch 4	Batch 5	Batch 6	Batch 7	Batch 8	Batch 9	Batch 10	Total	Average	Standard Deviation
C7	4721	4824	4724	4761	4782	4763	4766	4833	4793	4838	47805	4781*	42*
C7, C8	2038	2006	2021	2082	2021	2022	2105	2056	2041	2058	20450	2045*	31*
C7, C8, C9	500	504	532	522	520	478	546	514	518	495	5129	513*	19*
C7, C8, C9, C10	27	27	26	35	35	28	29	32	34	19	292	29*	5*
C7, C8, C9, C10, C12	Not performed												

Table 6 Test 2 results for Static Control Variability test (Kwiatkowski 2017z)

Test 3. Static Control Variability Test with Dynamic Control

Controls	Batch 1	Batch 2	Batch 3	Batch 4	Batch 5	Batch 6	Batch 7	Batch 8	Batch 9	Batch 10	Total	Average	Standard Deviation
C7	4854	4827	4859	4864	4762	4740	4788	4777	4781	4734	47986	4799*	49*
C7, C8	2143	2051	2065	2051	2091	2036	2070	2076	2044	2009	20636	2064*	36*
C7, C8, C9	545	508	554	506	541	529	534	559	538	503	5317	532*	20*
C7, C8, C9, C10	33	31	33	28	29	23	41	31	33	24	306	31*	5*
C7, C8, C9, C10, C12	0	1	1	1	0	0	0	1	0	1	5	1*	1*

Table 7 Test 3 results for the Static Control Variability test with Dynamic Control (Kwiatkowski 2017aa)

Table 5, Table 6 and Table 7 show the average test results from each type. These tables were used to calculate the overall results shown in Table 4.

Dynamic Control Results

Figure 31 and Figure 32 show the test results from the dynamic control tests (Test 3).

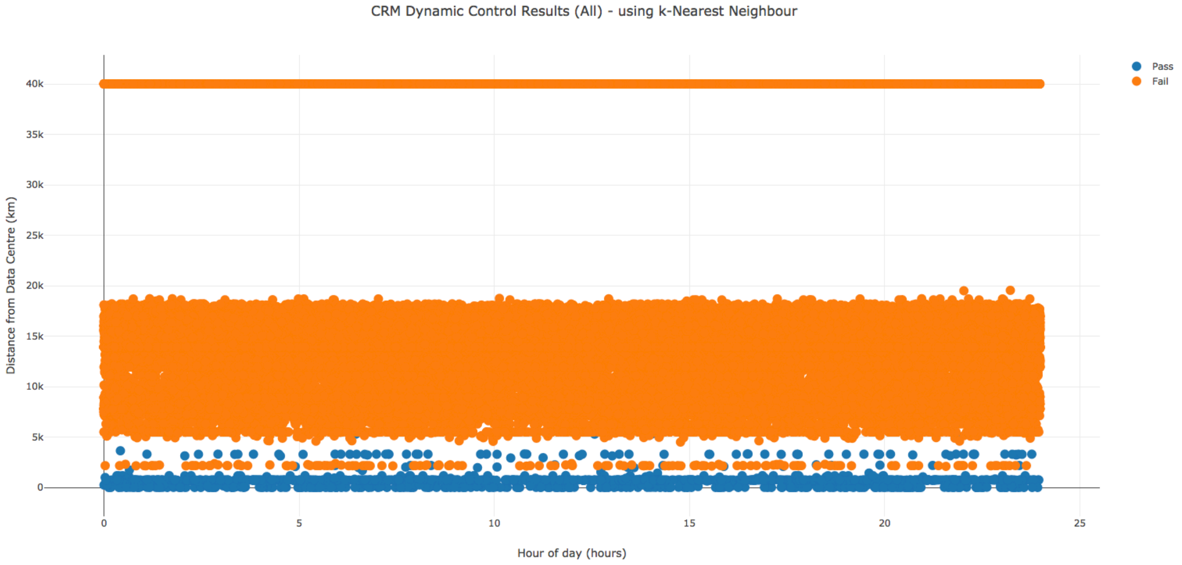


Figure 31 The dynamic control pass and fail requests for all batch tests. IP addresses that had no longitude and latitude were set to 40,000km to easily identify them (Kwiatkowski 2017ab)

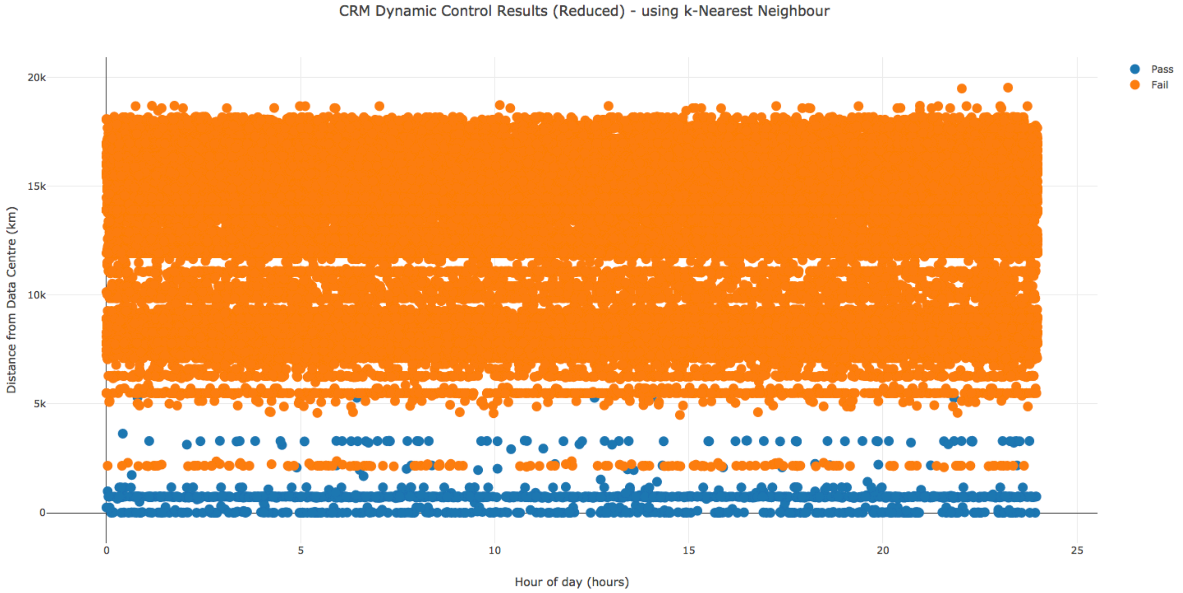


Figure 32 The dynamic control pass and fail requests for all batches, excluding IP addresses that had no longitude and latitude (Kwiatkowski 2017ac)

Allowed	Source Country	Hour of Access	Average Source Distance
66	Australia	20	528.4394
62	Australia	13	750.8226
58	Australia	2	750.9655
58	Australia	3	736.3276
58	Australia	7	788.6207
54	Australia	5	551.1852
52	Australia	8	730.3462
52	Australia	17	778.6538
51	Australia	6	886.9804
51	Australia	19	767.1373
51	Australia	21	744.0784
51	Australia	23	866.6275
50	Australia	14	612.4200
48	Australia	0	597.5625
46	Australia	15	722.9348
45	Australia	1	600.8667
45	Australia	4	630.9556
45	Australia	18	660.2222
45	Australia	22	770.2222
44	Australia	10	775.0227
43	Australia	9	726.2093
43	Australia	11	562.4186
43	Australia	12	775.4186
37	Australia	16	933.5405
2	Indonesia	0	4466.5000
2	New Zealand	7	2094.0000
2	New Zealand	18	2216.5000
1	Papua New Guinea	4	3115.0000
1	New Zealand	4	2076.0000
1	New Zealand	5	2174.0000
1	New Caledonia	6	1970.0000
1	Guam	6	5282.0000
1	Fiji	6	3218.0000
1	New Zealand	8	2173.0000
1	New Caledonia	9	1962.0000
1	New Zealand	10	2023.0000
1	Papua New Guinea	10	2921.0000
1	New Zealand	11	2240.0000
1	Fiji	11	2949.0000
1	Guam	12	5282.0000
1	New Caledonia	13	1962.0000
1	New Zealand	13	1995.0000
1	Indonesia	14	5313.0000
1	New Zealand	14	2173.0000

1	New Zealand	15	2083.0000
1	New Zealand	17	2084.0000
1	New Zealand	19	2212.0000
1	New Zealand	21	2179.0000
1	Guam	21	5279.0000
1	Fiji	23	3218.0000
1	New Zealand	23	2173.0000

Table 8 Number of allowed requests by Country and time (hours) (Kwiatkowski 2017 ad)

No requests from Australia were blocked. Table 8 shows all of the granted login requests, grouped by number of requests, country and time of the day. The maximum distance granted by the dynamic control was 5313km. Christmas Island was 5304km from the data centre location in the training data (see Table 2).

Table 9 shows the number of pass and fail results from the compliance layer for the dynamic control, grouped by count and country. This data is plotted in Figure 33 where the locations of a pass or fail result falls within a 6000km radius of the data centre (proposed CRM location).

Country	Count	Result	Average Distance
Brunei	5	Fail	5736.4000
Malaysia	61	Fail	5713.9180
Philippines	10	Fail	5643.1000
Northern Mariana Islands	1	Fail	5458.0000
Indonesia	608	Fail	5430.3454
Guam	3	Pass	5281.0000
Indonesia	3	Pass	4748.6667
Federated States of Micronesia	1	Fail	4574.0000
Fiji	3	Pass	3128.3333
Papua New Guinea	2	Pass	3018.0000
New Zealand	141	Fail	2173.5177
New Zealand	16	Pass	2137.8750
New Caledonia	3	Pass	1964.6667
Australia	1198	Pass	716.1319

Table 9 Countries allowed within the maximum allowed source IP address range of 5313km (Kwiatkowski 2017ae)

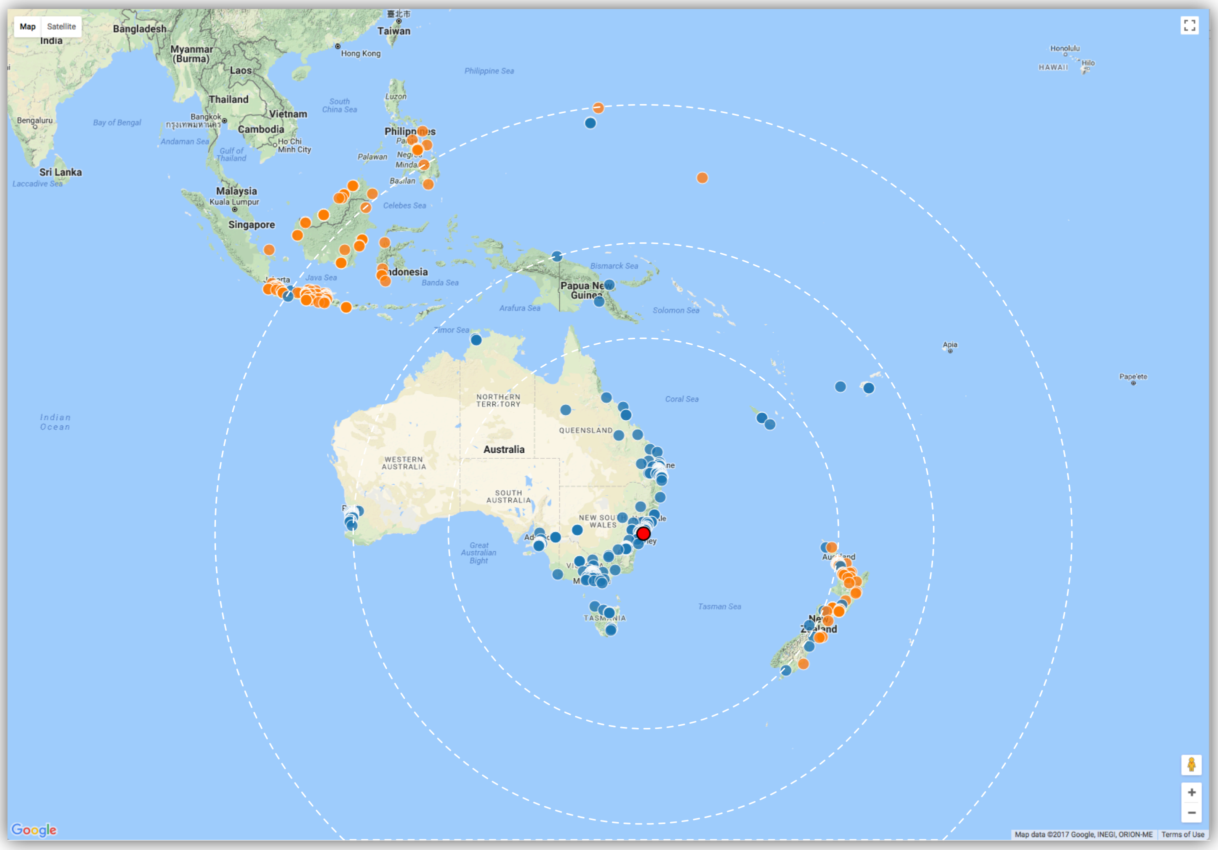


Figure 33 Results showing pass and fail results within 6000km from the data centre location (Kwiatkowski 2017af)

[Blue = Pass, Orange = Fail, Red = Data Centre. Mapping software courtesy: Google Maps]

Chapter 6. Discussion

The test plan evaluated the preventive and detective capabilities of the proposed risk assessment methodology in Figure 14. Whilst Donaldson et al. 2015 argue forensic and auditing controls are more affordable than preventative or detective controls, this may not be accurate when factoring in the cost of the privacy or security breach. For example, if a CRM contained 10,000 records and the main risk event occurred as per Figure 14, then the proposed CRM model could potentially save the organisation an average of USD$1,540,000. This figure was calculated as USD$154 per record, which contained sensitive or confidential information (Ponemon 2015).

The test plan evaluated the performance of the proposed risk assessment methodology. The path for “RC2 Remote Malicious User” was evaluated in Figure 14. The average number of requests allowed by the compliance layer decreased as the number of controls increased (see Table 4). This suggests that higher risk events will benefit from mitigation strategies that implement a greater number of controls. Collectively, the controls worked to together to mitigate a higher risk event, so that:

- Two controls reduced the risk by 27%;
- Three controls reduced the risk by a further 15%;
- Four controls reduced the risk by a further 5%; and
- Five controls reduced the risk by a further 0.3%.

The test types factored in the varying effectiveness of each control in different environments (risk situations). Whilst the compliance check required that all control pass for the request to pass, some controls would will not work effectively on their own in the real world. For example, the controls “C9. Valid Credentials” and “C10. Two-factor Authentication” are both considered primary, static controls. These controls are mandatory for a user to login to the system. The brute force attack could be considered a secondary control. This control would be largely in effective on its own when compared to C9 or C10. This is also true for the dynamic control.

The variability differences between test 2 and test 1 reduced the compliance checker’s performance by 5% to 7% (see Figure 29). This allowed an additional 601 requests to access potentially sensitive information. As ISO27001 is largely a manual process, organisations will need to assess the effectiveness of each control in their own environment.

Effectiveness of Single Controls

Figure 30 showed the most effective single control was the dynamic control. However, this control was reliant on other controls being active, as without controls such as “C9. Valid Credentials”, the dynamic control would be ineffective. Dynamic controls enhanced the effectiveness of the static controls, but were not be suitable in place of them.

Dynamic Controls

The dynamic control did not deny a legitimate user from accessing the prototype CRM. The dynamic control was trained with supervised data, where pass requests originating in Australia, and on Christmas Island. The dynamic control allowed all requests that originated from Australia to pass. This was consistent with the test data in Figure 26 and Figure 33. No results from Christmas Island appeared in the test results. The dynamic control denied 60% of the user requests made within 6,000km from the data centre location (827 of 2055). The accuracy increased to 98.7% (1228 of 94784) for all IP addresses tested with a known longitude and latitude.

The dynamic control was partially ineffective outside of Australia. A small number of requests from New Zealand, Papua New Guinea, and Indonesia passed the dynamic control compliance check. Their geolocations were not present in the training data. However, the calculated distance of Indonesia was similar to Christmas Island. The dynamic control requires further evaluation to tune the effectiveness.

The training data only contained pass results for login requests made during business hours in Australia. The results showed the dynamic control allowed any user within Australia to login at any time of the day (0 – 23 hours inclusive). This supported the “work anywhere, anytime” requirement of a mobile workforce.

Overall, when used in combination with other controls, the dynamic control effectively reduced the uncertainty of risk. Additional validation of the dynamic control is required to determine how the control would operate outside of Australia. Countries which are not as remote as Australia, may have reduced accuracy.

ISO27001 and ISO31000 for CRMs

The proposed risk assessment methodology provided a way for organisations to manage risk within CRMs that would enable compliance with ISO27001 and ISO31000. There were no identified incompatibilities with ISO27001 and ISO31000 during testing. However, the depth of this finding will need to be broadened with further research. ISO27001 compliance requires that organisations perform periodic evaluations of the effectiveness of their ISMS. The proposed CRM model enabled a way for CRMs to become more actively compliant with an ISMS than existing CRM models. Future research could explore how the proposed CRM model and the proposed assessment methodology can better enable governance reporting and the documentation required to achieve ISO27001 compliance. This documentation is required by auditors and management, and would introduce the accountability aspect of CIAA. This would provide an opportunity for the organisation to validate their risk assumptions based on the actual risk data collected.

The resources required to implement automated compliance for many controls will need to be balanced against the expected cost of a data breach. With four controls active in the tests, 31 security breaches could have resulted (see Table 7). Each breach could have cost the organisation an average of USD$1,540,000. Adding a dynamic control to the existing controls could have saved the organisation on average USD$73,200,000. Whilst this saving appears large, Sony's recent security breach cost the company USD$35,000,000 for the disclosure 100 million records (Kassner 2015). Sony's management had previously stated they would not spend $10,000,000 on preventative security to avoid a possible (perceived) loss of USD$1,000,000 (Hacket 2015).

The effectiveness of static controls will change as new exploits and attack methods are developed to counter them. Without continually testing the effectiveness of an ISMS, an organisation could assume existing controls are effective, until the CIA of information is affected. The dynamic control reduced the uncertainty of risk more than any other static controls, including two factor authentications. Whilst the dynamic control still allowed 5 malicious requests in 100,000 to pass the compliance check, 31 breaches would have occurred without it.

Chapter 7. Conclusion

The literature review connected the broad areas of CRMs, security, privacy, and data mining in an attempt to improve the privacy and security postures of CRMs. The literature review identified a gap in current research relating to privacy and security assessment methodologies for CRMs, and highlighted a lack of visible privacy and security controls in existing CRM models.

Existing CRM models do not visibly and proactively manage privacy and security risks in a way that facilitates automated compliance with ISO27001. The research evaluated ISO27001 as a possible ISMS for CRMs, given that ISO27001 can be applied to any organisation, technology, and type of CRM.

The proposed CRM model adopts the ISO27001's PDAC principle as a way of achieving automated compliance with the standard. The proposed CRM model requires that information must be brokered through the compliance layer at each stage of the transaction(s). This keeps information secure and private.

The 2013 revision of ISO27001 requires organisations to also select their preferred risk management methodology. Currently, no CRM specific risk assessment methodology currently exists. The proposed risk assessment methodology addresses this gap and demonstrated that ISO27001 can be partially automated. Future research is required to determine how the proposed risk assessment methodology and proposed CRM model can generate the documentation (or dashboards) and data required to automate the ISO27001 auditing process.

A prototype CRM was built to test the effectiveness of the proposed risk management model. This code executed 10 batches of 10,000 individual web requests against the prototype CRM system, with each request simulating a user attempting to login to the system from different geographic locations. The test results found that average number of allowed requests decreased as the number of controls increased.

Collectively, the controls worked to together to mitigate a higher risk event, so that:

- Two controls reduced the risk by 27%;
- Three controls reduced the risk by a further 15%;
- Four controls reduced the risk by a further 5%; and
- Five controls (including one dynamic control) reduced the risk by a further 0.3%. The difference of 4.7% represented 30 security breaches.

Dynamic controls were the most effective individual control and did not deny a legitimate user from accessing the prototype CRM. The accuracy of the dynamic control decreased to 60% accuracy within a radius of 6,000km to the information location. This accuracy increased to 98.7% globally. At this time, dynamic controls are best suited for supporting existing static controls, due to their unpredictability.

Future research is required to validate the findings of this thesis with live data, and explore the operation of the proposed CRM model and proposed risk assessment methodology in different CRM environments.

Chapter 8. Recommendations and Future Research

1. The proposed CRM model bridged the gap between the lack of privacy and security controls in existing CRM models and provided a compliance layer to ensure requests were compliant with controls:
    a. This is the first step required to achieve ISO27001 automation within a CRM.
2. When using the proposed risk assessment methodology, the adoption of more controls helped prevent higher risk events from occurring.
3. Future research is required to determine how the proposed risk assessment methodology and proposed CRM model can generate the documentation (or dashboards) and data required to automate ISO27001.
4. When using the proposed risk assessment methodology, dynamic controls were more effective than static controls, however dynamic controls were found to be only effective with static controls.
5. The proposed risk assessment methodology should be re-validated with live data to assess how the model performs in the real world.
6. The proposed risk assessment methodology could incorporate a risk scoring system that better adapts to the uncertainty in risky situations.
7. The performance of the forensic and detective controls within the proposed risk assessment methodology could be explored.
8. Privacy of personal information cannot exist without security controls.
9. As ISO27001 is an organisational wide ISMS, the proposed risk assessment methodology may not be able to handle all aspects of ISO27001 compliance for the organisation.
10. Some organisations are likely to have unique risks and controls, and the proposed CRM model and proposed risk assessment methodology may not be suitable for them.
11. Privacy preserving data mining techniques could be further explored with dynamic controls.
12. The dynamic control could be re-tested with different machine learning algorithms to evaluate performance.

13. The dynamic control could be re-tested with:
    a. Countries that have closer boundaries to known threats;
    b. Workers that travel between many countries.
14. The United States of America appeared more times in the results, presumably because they had more IP addresses in the GeoIP database. The effect on the dynamic control performance should be explored.
15. The layers and functions of the proposed CRM model could be further evaluated to determine how successful the CRM will operate compared to the existing models.

References

Al-Shawi, A 2011, ‘Data mining techniques for information security applications’, *Wires Computational Statistics*, vol. 3, no. 3, pp. 221–229.

Boss, R 2000 "Information Technology Standards" Library Technology Reports, vol. 36, no. 4, p. 1. Expanded Academic ASAP.

Buttle, F & Maklan S 2015, *Customer Relationship Management*, 3rd edn, Butterworth-Heinemann, Oxon, UK.

Caron, X, Bosua, R, Maynard, SB & Ahmad, A 2016, ‘The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective’, *Computer Law Security Review*, vol. 32, no. 1, pp. 4–15.

Choon, SLK 2004, ‘An integrated evaluation system based on the continuous improvement model of IS performance’, *Industrial Management & Data Systems*, vol. 104, no. 2, pp. 115–128.

Cranor, L. (2012) *P3P is dead, long live P3P!*, viewed 3 February 2017, <http://lorrie.cranor.org/blog/2012/12/03/p3p-is-dead-long-live-p3p/>.

de Montjoye, Y-A, Radaelli, L, Singh, VK & Pentland, AS 2015, ‘Unique in the Shopping Mall: On the reidentifiability of credit card metadata’, *Science*, vol. 347, no. 6221, pp. 536–539.

Donaldson, S, Siegel S, Williams, C, & Aslam, A 2015, *Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats*, Apress, New York.

Flaus, J 2013, Risk Analysis, John Wiley & Sons, Incorporated, Somerset. Available from: ProQuest Ebook Central. [27 March 2017].

Gasiorowski-Denis, E. n.d. *How to measure the effectiveness of information security*, viewed 4 February 2017, <http://www.iso.org/iso/es/home/standards/management-standards/iso27001.htm>.

Gmbh, 2017, ‘Downloads – Here you find the current installation package of MAMP & MAMP PRO’, viewed 10 July 2017, <https://www.mamp.info/en/downloads/>.

Hacket, R 2015, ‘How much do data breaches cost big companies? Shockingly little’, accessed 26th October 2017, <http://fortune.com/2015/03/27/how-much-do-data-breaches-actually-cost-big-companies-shockingly-little/>.

Igoshev, D 2017, ‘Captcha integration for the Laravel 5, viewed 10 July 2017, <https://github.com/igoshev/laravel-captcha>.

ISO/IEC 27001, *Information technology – Security techniques – Information security management systems – Requirements*, viewed 2 February 2017, <http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534>.

ISO/IEC 31000, *Risk Management – Principles and guidelines*, viewed 2 August 2017, < https://www.iso.org/standard/43170.html>.

ISO/IEC 27002, *Information technology – Security techniques – Code of practice for information security controls – Requirements*, viewed 2 February 2017, <https://www.iso.org/standard/54533.html>.

ISO 2014, Economic benefits of standards [ebook] Switzerland. Available at: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/ebs_case_studies_factsheets.pdf <Accessed 13 Aug. 2017>.

Jalan, P 2017, ‘GeoIP’, viewed 10 July 2017, <https://github.com/pulkitjalan/geoip>.

Jaschen, M 2017, ‘phpgeo – A Simple Geo Library for PHP’, viewed 20 July 2017, <https://github.com/mjaschen/phpgeo>.

Ji, Z & Elkan, C 2013, ‘Differential privacy based on importance weighting’, *Machine Learning*, vol. 93, no. 1, pp. 163–183.

Kassner M, 2015, ‘Data breaches may cost less than the security to prevent them’, viewed 26 October 2017, <https://www.techrepublic.com/article/data-breaches-may-cost-less-than-the-security-to-prevent-them/>.

Kim, S 2010, ‘Assessment on Security Risks of Customer Relationship Management Systems’, *International Journal of Software Engineering and Knowledge Engineering*, vol. 20, no. 1, pp. 103–109.

Kobsa, A 2001, ‘Tailoring Privacy to Users’ Needs 1’, in M Bauer, PJ Gmytrasiewicz & J Vassileva (eds), *User Modeling 2001: 8th International Conference, UM 2001 Sonthofen, Germany, July 13–17, 2001 Proceedings*, Springer, Berlin Heidelberg, pp. 301–313.

Kondas, A 2017, ‘PHP-ML – Machine Learning library for PHP’, viewed 10 July 2017, <https://php-ml.readthedocs.io/en/latest/>.

Kosutic, D 2015, ‘Becoming ISO 27001 certified – How to prepare for certification audit’, viewed 10 July 2017, <https://advisera.com/27001academy/knowledgebase/becoming-iso-27001-certified-how-to-prepare-for-certification-audit/>.

Kuligowski, C 2009, ‘Comparison of IT Security Standards’, viewed 28 January 2017, <http://www.federalcybersecurity.org/CourseFiles/WhitePapers/ISOvNIST.pdf>.

Kwiatkowski, A 2016, ‘Initial model’, Master of IT, Flinders University, Adelaide, SA.

Kwiatkowski, A 2017a, ‘Class diagram for prototype CRM, demonstrating how the compliance check is triggered by a user action or risk scenario’, Master of IT, Flinders University, Adelaide, SA.

Kwiatkowski, A 2017b, ‘Technology stack for the Prototype CRM’, Master of IT, Flinders University, Adelaide, SA.

Kwiatkowski, A 2017c, ‘Use case diagram showing different actors accessing the prototype CRM’, Master of IT, Flinders University, Adelaide, SA.

Kwiatkowski, A 2017d, ‘Workflow diagram demonstrating how a user triggers a compliance check on each interaction with the system’, Master of IT, Flinders University, Adelaide, SA.

Kwiatkowski, A 2017e, ‘Workflow diagram for when a client accesses the Prototype CRM’, Master of IT, Flinders University, Adelaide, SA.

Kwiatkowski, A 2017f, ‘Proposed CRM Model’, Master of IT, Flinders University, Adelaide, SA.

Kwiatkowski, A 2017g, ‘Proposed Risk Assessment Methodology (adapted from the Bow Tie method)’, Master of IT, Flinders University, Adelaide, SA.

Kwiatkowski, A 2017h, ‘Prototype CRM (left) linked to the Proposed CRM Model (middle) linked to the Proposed Assessment Methodology (right)’, Master of IT, Flinders University, Adelaide, SA.

Kwiatkowski, A 2017i, ‘Test Plan code for Prototype CRM’, Master of IT, Flinders University, Adelaide, SA.

Kwiatkowski, A 2017j, ‘Proposed Assessment Methodology legend and sequence’, Master of IT, Flinders University, Adelaide, SA.

Kwiatkowski, A 2017k, ‘The methodology used to determine the effectiveness of multiple controls working together, to collectively block the risk event from occurring. If any control fails then the request will be denied’, Master of IT, Flinders University, Adelaide, SA.

Kwiatkowski, A 2017l, ‘The compliance layer within the Proposed Assessment Methodology that validates a series of controls. All controls must be successful for the user action to be successful’, Master of IT, Flinders University, Adelaide, SA.

Kwiatkowski, A 2017m, ‘Test Plan strategy overview’, Master of IT, Flinders University, Adelaide, SA.

Kwiatkowski, A 2017n, ‘The compliance check process is triggered when a user makes a request against the Prototype CRM’, Master of IT, Flinders University, Adelaide, SA.

Kwiatkowski, A 2017o, ‘Testing the dynamic CRM compliance model. The login screen controller contains the controls designed to limit the likelihood of the main risk event’, Master of IT, Flinders University, Adelaide, SA.

Kwiatkowski, A 2017p, ‘Compliance layer code’, Master of IT, Flinders University, Adelaide, SA.

Kwiatkowski, A 2017q, 'The login form validation results, shown when the user submits the login form. A compliance error is displayed to the user for each validation check that failed', Master of IT, Flinders University, Adelaide, SA.

Kwiatkowski, A 2017r, 'Sample training data used by Dynamic Control, which were classified as a pass', Master of IT, Flinders University, Adelaide, SA.

Kwiatkowski, A 2017s, 'Sample training data used by the Dynamic Control, which were classified as a fail', Master of IT, Flinders University, Adelaide, SA.

Kwiatkowski, A 2017t, 'Dynamic Control training data visualisation, with majority of pass results in Australia and Christmas Island', Master of IT, Flinders University, Adelaide, SA.

Kwiatkowski, A 2017u, 'The average number of requests that were allowed by the compliance layer across the ten batches of tests for test number', Master of IT, Flinders University, Adelaide, SA.

Kwiatkowski, A 2017v, 'Comparison between the three different testing strategies', Master of IT, Flinders University, Adelaide, SA.

Kwiatkowski, A 2017w, 'Average number of login requests allowed to the Prototype CRM from all testing strategies', Master of IT, Flinders University, Adelaide, SA.

Kwiatkowski, A 2017x, 'Number of requests allowed to Prototype CRM when only a single control was used', Master of IT, Flinders University, Adelaide, SA.

Kwiatkowski, A 2017y, 'Test 1 results for the Static Control baseline test', Master of IT, Flinders University, Adelaide, SA.

Kwiatkowski, A 2017z, 'Test 2 results for the Static Control variability test', Master of IT, Flinders University, Adelaide, SA.

Kwiatkowski, A 2017aa, 'Test 3 results for the Static Control variability test with Dynamic Control', Master of IT, Flinders University, Adelaide, SA.

Kwiatkowski, A 2017ab, 'The Dynamic Control pass and fail requests for all batch tests. IP addresses that had no longitude and latitude were set to 40,000km to easily identify them', Master of IT, Flinders University, Adelaide, SA.

Kwiatkowski, A 2017ac, ‘The Dynamic Control pass and fail requests for all batches, excluding IP addresses that had no longitude and latitude’, Master of IT, Flinders University, Adelaide, SA.

Kwiatkowski, A 2017ad, ‘Number of allowed requests by Country and time (hour)’, Master of IT, Flinders University, Adelaide, SA.

Kwiatkowski, A 2017ae, ‘Countries allowed within the maximum allowed source IP address range of 5313km’, Master of IT, Flinders University, Adelaide, SA.

Kwiatkowski, A 2017af, ‘Results showing pass and fail results within 6000km from the data centre location’, Master of IT, Flinders University, Adelaide, SA.

Kwiatkowski, A 2017ag, ‘Map of training data’, Master of IT, Flinders University, Adelaide, SA.

Lark J, 2015, *ISO 31000 Risk management – A practical guide for SME*, viewed 28 March 2017, <https://www.iso.org/publication/PUB100367.html>.

Longhorn, M & Hughes, S 2015, ‘Modern replication of Eratosthenes’ measurement of the circumference of Earth’, *Physics Education*, vol. 50, no. 2, IOP Publishing, pp. 175–178.

Malthouse, EC, Haenlein, M, Skiera, B, Wege, E & Zhang, M 2013, ‘Managing Customer Relationships in the Social Media Era: Introducing the Social CRM House’, *Social Media and Marketing*, vol. 27, no. 4, pp. 270–280.

Maoz, M, & Manusama, B 2016, *Gartner reprint*, viewed 3 February 2017, <https://www.gartner.com/doc/reprints?id=1-32AEZIA&ct=160331&st=sb>.

Microsoft 2017, *P3P is no longer supported*, viewed 27 January 2017, <https://msdn.microsoft.com/en-us/library/mt146424(v=vs.85).aspx>.

Mitchell, S.L. 2007, "GRC360: A framework to help organisations drive principled performance", *International Journal of Disclosure and Governance,* vol. 4, no. 4, pp. 279-296.

Network Advertising Initiative 2017, *Understanding Online Advertising*, viewed 20 February 2017, <https://www.networkadvertising.org/faq>.

Nicholson, L, & Puranikmath, S 2015, *Can I have the same access to my information as law enforcement agencies?*, viewed 4 February 2017, <https://www.holdingredlich.com/privacy-data-protection/can-i-have-the-same-access-to-my-information-as-law-enforcement-agencies>.

NIST 2014, *Framework for Improving Critical Infrastructure Cybersecurity*, viewed 1 February 2017, <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>.

NIST 2016, *Framework for Improving Critical Infrastructure Cybersecurity*, viewed 12 February 2017, <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf >.

OAIC 2014, *Privacy Fact Sheet 17: Australian Privacy Principles*, viewed 15 December 2016, <https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles>.

OAIC 2015a, *Privacy Act*, viewed 15 December 2016, <https://www.oaic.gov.au/privacy-law/privacy-act/>.

OAIC 2015b, 'Chapter 8: APP 8 – Cross border disclosure of personal information, viewed 16 December 2016, <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information>

Otwell, T n.d., 'Introduction', viewed 23 October 2017, <https://laravel.com/docs/4.2/introduction>.

Otwell, T 2017, 'Release Notes', viewed 23 October 2017, <https://laravel.com/docs/5.5/releases#laravel-5.5>.

Pathak, M & Raj, B 2010, 'Large Margin Multiclass Guassian Classification with Differential Privacy', in Dimitrakakis, C et al. (eds.), *Privacy and Security Issues in Data Mining and Machine Learning*, Springer, Berlin Heidelberg, pp 99-112.

Pearson, S & Allison, D 2009, ‘A Model-Based Privacy Compliance Checker’, *International Journal of E-Business Research*, vol. 5, no. 3, pp. 63–83.

PHP, n.d., ‘What can PHP do?’, viewed 1 July 2017, <http://php.net/manual/en/intro-whatcando.php>.

Pierazzi, F, Casolari, S, Colajanni, M & Marchetti, M 2016, ‘Exploratory security analytics for anomaly detection’, *Computers & Security*, vol. 56, pp. 28-49.

Privacy Act 1988 (Cth).

Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4.

Ponemon Institute 2015, *2015 Cost of Data Breach Study: Global Analysis*, Arizona, viewed 22 February 2017, <https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF>.

Reagle, J & Wenning, R 2000, *Privacy P3P FAQ*, viewed 1 February 2017, <https://www.w3.org/P3P/P3FAQ.html>.

Romano, NC Jr & Fjermestad, J 2007, ‘Privacy and Security in the Age of Electronic Customer Relationship Management’, *International Journal of Information Security and Privacy,* vol. 1, no. 1, pp. 65-86.

Rountree, D & Castrillo, I 2014, *The Basics of Cloud Computing: Understanding the Fundamentals of Cloud Computing in Theory and Practice*, Syngress, Boston.

Santos-Olmo, A, Sánchez, L, Rosado, D, Fernández-Medina, E & Piattini, M 2016, ‘Applying the Action Research Method to Develop a Methodology to Reduce the Installation and Maintenance Times of Information Security Management Systems’, *Future Internet*, vol. 8, no. 3, Multidisciplinary Digital Publishing Institute, p. 36.

Seify M. 2006, ‘New Method for Risk Management in CRM Security Management’, *Third International Conference on Information Technology: New Generations (ITNG'06)*, Las Vegas, pp. 440-445.

Seitz, K 2006, ‘*Taking Steps To Ensure CRM Data Security’*, *Customer Interaction Solutions,* vol. 24, no. 11, pp. 62-66.

Standards Australia 2013, *Risk management guidelines – Companion to AS/ZS ISO 31000:2009*, Standards New Zealand, Wellington.

Starostenko, O, Cruz-Perez, C, Uceda-Ponga, F & Alarcon-Aquino, V 2015, 'Breaking text-based CAPTCHAs with variable word and character orientation', *Pattern Recognition*, vol. 48, no. 4, Pergamon, pp. 1101–1112.

Sutton, I 2015, *Process Risk and Reliability Management*, 2nd edn, Elsevier, Oxford, GB.

Tan, P, Steinbach, M, & Kumar, V 2006, *Introduction to Data Mining*, Pearson Addison Wesley, Boston.

Thomson, I 2017, 'After years of warnings, mobile network hackers exploit SS7 flaws to drain bank accounts', viewed 17 October 2017, <https://www.theregister.co.uk/2017/05/03/hackers_fire_up_ss7_flaw/>.

Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (Cth).

Wheeler, E 2011, *In Security Risk Management*, Syngress, Boston.

W3Techs, 2016, 'Usage of server-side programming languages for websites', viewed 23 October 2017, <https://w3techs.com/technologies/overview/programming_language/all>.

Xu, L, Jiang, C, Wang, J & Ren, Y 2014, 'Information Security in Big Data: Privacy and Data Mining', in *IEEE Access*, vol. 2, no., pp. 1149-1176.

Yang, Q, & Wu, X 2006, '10 Challenging problems in data mining research', *International Journal of Information Technology & Decision Making*, vol. 5, no. 4. Pp. 597-604.

Appendix 1. ISO27001 Process summarised from ISO Standard

has been removed due to copyright restrictions

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	
[redacted]	[redacted]
[redacted]	
[redacted]	[redacted]
[redacted]	
[redacted]	[redacted]
[redacted]	
[redacted]	[redacted]
[redacted]	
[redacted]	[redacted]
[redacted]	
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted] [redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	
[redacted]	
[redacted]	
[redacted]	
[redacted]	
[redacted]	
[redacted]	
[redacted]	
[redacted]	
[redacted]	
[redacted]	[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]