2014

The application of an agile approach to it security risk management for SMES

Damien Hutchinson
Deakin University

Chris Armitt
Deakin University

Dean Edwards-Lear
Deakin University

DOI: 10.4225/75/57b66603343d7

12th Australian Information Security Management Conference. Held on the 1-3 December, 2014 at Edith Cowan University, Joondalup Campus, Perth, Western Australia.

THE APPLICATION OF AN AGILE APPROACH TO IT SECURITY RISK MANAGEMENT FOR SMES

Damien Hutchinson, Chris Armitt, Dean Edwards-Lear
School of Information Technology, Deakin University, Melbourne, Australia
Email: drh@deakin.edu.au

Abstract

This paper demonstrates the application of an agile risk management approach to perform asset-based risk analysis to meet the information security requirements of SMEs (Small and Medium-sized Enterprises). This approach is proposed as an alternative to traditional methods that are cumbersome, resource intensive and costly, often hindering their value and use by SMEs. The organisation being studied is an Aged Care Facility (ACF) with legal and ethical responsibilities. Within the business there is little knowledge regarding potential information technology threats that could impact on these responsibilities. The ACF maintains a system containing client personal and medical records, network communications, as well as financial and business information assets. Understanding the susceptibility of this data to unauthorised access and/or exploitation has become a key concern for the organisation. In order to analyse and communicate potential risks to current IT assets and propose suggestions to mitigate and minimise risk factors, an agile IT security risk assessment approach was developed in a collaborative research venture with ACF and their External IT Provider (EIP).

Keywords
SMEs, Information Security, Risk Analysis, Agile, Aged Care organisations

INTRODUCTION

There are a wide variety of risk assessment methods and tools that currently exist in the world of IT security. A majority of them are more adaptable for large companies with adequate financial and personnel resources to accurately assess their IT security as opposed to SMEs with fewer resources. This section presents an overview of the various methodologies, risk assessment frameworks and other tools that currently exist. Their potential benefits for SMEs are discussed using the Aged Care Facility (ACF) as the case study, as well as any reasons why they may not be suitable.

The problem was being able to determine and validate a suitable approach to perform the security risk assessment for Aged Care organisations that could then be justified as an agile model for SMEs. As part of the design process of this agile approach, workshops were conducted with an Aged Care organisation (refer to section Identification of Threats to Critical Assets). Based on conversation, observation and feedback during these workshops we determined that the suitable risk assessment approach for this ACF to undertake an independent risk analysis of their IT assets, needed to include the following criteria:

1. *Industry Sectors*: To facilitate ACF representation and operation across a range of industry sectors, the method needs to facilitate public, private and government organizations.
2. *Language*: The language of the method needs to be in English.
3. *Cost*: The associated cost of obtaining the method needs to be free.
4. *Scope*: The scope of the method must include usability by SMEs.
5. *Management Use Required*: The method needs to focus on the ability of ACF management to use, understand and apply the method.
6. *Required Training*: Maximum (2-3 days) training or guidance is required to skill an ACF to apply and use the method.
7. *Consultancy Support*: Consultancy support should not be required in order to apply the method.
8. *Regulatory Compliance*: The method needs to facilitate adaptability to changing regulatory compliance.
9. *Compliance to IT Standards*: The risk assessment method needs to have been designed and developed based on industry recognised and certified principles and processes to allow for future alignment and compliance of ACF security with an IT standard.

To both validate the relevance of this empirical criteria and understand the suitability of current approaches available for SMEs, a review of risk assessment methods was undertaken. The review set out to determine whether there is a current industry or government body framework available for comparing risk assessment methods. It was discovered that the European Union Agency for Network and Information Security (ENISA), a centre of expertise for Information Security in Europe, has generated an inventory of Risk Management / Risk Assessment methods (ENISA, 2014). Currently, the inventory consists of 13 methods. To both describe and enable comparison between the characteristics of the methods, ENISA devised 21 attributes and formulated them into a template (ENISA, 2005). To assist SMEs with the selection of the most appropriate method, the ENISA working group selected 11 of those attributes and tabled them with 8 of the 13 risk assessment and risk management methods characterised by their features and functions which were judged to be best suited for SMEs (ENISA, 2006). Six correlations from the 11 attributes that match and substantiate the empirical criteria for the ACF case study were identified. Table 1 shows the relationship between the 8 methods and the empirical criteria to demonstrate the comparison performed and determine a suitable security risk assessment approach for ACFs. The criteria highlighted in green indicates the correlation with 6 of the 11 ENISA SME attributes.

Risk Management Method	Origin	Industry Sectors	Language	Cost	Scope	Management Use	Required Training	Consultancy Support	Regulatory Compliance	Compliance to IT Standard(s)	Suitability for ACF
Au IT Security Handbook	Austria	×	×	✓	✓	✓	✓	✓	N/A	✓	×
A&K Analysis	The Netherlands	×	×	✓	✓	✓	✓	✓	×	✓	×
Ebios	France	✓	✓	✓	✓	✓	✓	×	×	✓	×
ISO/IEC IS 13335-2 (ISO/IEC IS 27005)	International standard	×	✓	×	✓	✓	✓	✓	N/A	✓	×
ISO/IEC IS 17799 (ISO/IEC IS 27002)	International standard	×	✓	×	✓	✓	✓	×	N/A	✓	✓
IT-Grundschutz	Germany	×	✓	✓	✓	✓	✓	×	×	✓	×
Mehari	France	✓	✓	✓	×	✓	✓	×	✓	✓	×
Octave	USA	×	✓	✓	✓	✓	✓	×	N/A	N/A	✓

Table 1 Suitability of risk assessment approach for ACF case study

The result of the review indicated that the Octave method and the ISO 27002 standard were the 2 most suitable methods that match the defined suitability criteria. The challenge was then to combine elements from both these methods to create and validate an agile risk management approach. The next sections provide further description and justification for the selection of these methods.

OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation)

The OCTAVE methodology was created by Carnegie Mellon University's Software Engineering Institute. OCTAVE is a popular, industry standard methodology that identifies a company's critical IT assets,

vulnerabilities and threats to those assets and develops a risk mitigation system to support the company's mission and priorities. Traditionally a self-directed approach, OCTAVE draws its strengths from members of the organisation itself, utilising their knowledge of organisational operations and giving them responsibility for applying the security strategy. OCTAVE is a very thorough method and allows a company to understand what potential risks, threats and vulnerabilities there are to its critical assets. The OCTAVE method is also quite flexible and can be tailored to meet the IT and business requirements of various types of companies. (Carnegie Mellon University, 2014a). This methodology is best suited for use by large companies with sufficient budgetary and people resources to undertake its development and implementation. It contains a lot of unnecessary testing and information regarding elements of a large business that a SME such as ACF does not have (Violino, 2011).

OCTAVE-s

OCTAVE-s is a variation of the OCTAVE approach to risk management specifically aimed at the requirements and constraints facing smaller organisations of approximately 100 employees or less. OCTAVE-s analyses can be led by small teams, typically 3-5 interdepartmental members with detailed knowledge of the inner workings of the organisation. These personnel will collect and analyse key asset, systems and information and produce protection strategies and risk mitigation plans based on the organisations' unique security risks. OCTAVE-s evaluations are performed more quickly and effectively when the team involved has a broad and detailed understanding of current business and security policies and procedures. All required tasks may then be completed internally and in a timely manner (Carnegie Mellon University, 2014b).

The OCTAVE-s methodology is a smaller and more concise version of the previously mentioned OCTAVE methodology. This version of the methodology is more suited to SMEs as it allows a smaller working group and takes into consideration the fact that smaller companies will have smaller and less hierarchies. This methodology simplifies and removes some sections from the original OCTAVE methodology, providing a more straightforward way to analyse a small business while still retaining the key assessment criteria of the original methodology.

ISMS family of standards – ISO27k

The ISMS family of standards is intended to assist organizations of all types and sizes to implement and operate an ISMS (Information Security Management System) to manage the security of their information assets, and currently consists of 15 International standards under the general title of information technology – Security techniques (ISO/IEC, 2014). A company certified to ISO27k means that it follows an established and verified information security framework, and is compliant with the ISO/IEC 27001 Information security management systems — Requirements standard as determined by an independent assessment of their ISMS applied to the protection of information (ISO/IEC, 2014). Due to current resource including time and cost constraints, it is not feasible for ACF to consider ISO27001 certification. This is consistent with the ENISA omission of ISO/IEC 27001 from their recommended methods best suited for SMEs. However Annex A of ISO/IEC 27001 includes a set of control objectives and controls directly derived from and aligned with those listed in ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security controls to be used as implementation guidance when selecting and implementing controls for achieving information security (ISO/IEC, 2014). As identified by the review and supported by ENISA, this guideline standard is suitable for use by SMEs and therefore provides ACF with a method on which to build an ISMS if they seek to become certified in the future.

Methodology choice and justification

Based on the results of the review, and in consultation with management of the ACF, it was discussed which method would best benefit the assessment current IT assets. It was clear that the OCTAVE methodology would be cumbersome requiring too many unnecessary tests regarding ACF IT systems. The OCTAVE-s methodology provided the best-fit as it retains most of the threat assessment that the OCTAVE methodology contains but is more tailored towards the smaller company being studied. The organisation has a staff population of less than 100 employees and a small but quickly growing information technology infrastructure. This is significant, as the full OCTAVE analysis requires a detailed technical review of IT infrastructure. Small organisations often outsource their IT services and therefore do not have the technical knowledge or analysis tools required to evaluate their security effectively. A major benefit of the OCTAVE-s methodology is it can be tailored to a small company who outsources their IT assistance (Carnegie Mellon University, 2014b), similar to the way the ACF does for the management of their IT infrastructure. OCTAVE-s also suits the goal established by ACF to focus review efforts on securing key information technology assets, as this is an asset-based risk profiling technique.

It was decided to use the OCTAVE-s method as the process to develop a report on the steps performed to define, assess and provide feedback for this ACFs' current security issues. As the only other method supported by the review, the ISO 27002 control objectives and controls could be applied as a compliance checklist to help build the threat based profiles and determine the severity of risks posed to ACFs' IT assets. The checklist covers 11 key aspects of IT security, including asset management, physical security, access controls, and legal compliance. The accompanying risk assessment matrix provided by the ISO27k forum (ISO27k, 2007) can be used to score and rank each of the identified threats to determine which posed the greatest risk to ACF.

THE AGILE RISK MANAGEMENT APPROACH

This section describes the development of the agile risk management approach.

Establishing an impact evaluation criteria

Although traditionally qualitative in nature, presenting risk impact categories to an organisation using values of high, medium, and low has some limitations. Within these categories, it becomes difficult to determine where the more significant risks exist. Supposing there are multiple risks all deemed to be high impact in nature, where should management first focus their attention? The aim became to integrate traditional OCTAVE layout and analysis approaches with a more concise and definitive impact criteria to supplement OCTAVE findings and provide more indication to ACF management of exactly which risks posed the greatest impact to business objectives.

It is also important to note which areas of impact ACF management believed to be of greatest concern. It was established that losses or compromises causing time loss or business reputation damage were to be the primary focus. The criteria utilised to evaluate the impact of risks to ACF IT assets were adapted from resources provided by the ISO27k forum detailed in table 2 (ISO27k forum, 2007, 2008, 2010).

Probability	Explanation	Score
Negligible	Unlikely to occur	0
Very Low	2 – 3 times every 5 years	1
Low	Up to once per year	2
Medium	Up to twice per year	3
High	Up to once per month	4
Very High	More than once per month	5
Extreme	Several times per week	6

Impact Level	Explanation	Score
Insignificant	No impact	0
Minor	No extra effort required to repair	1
Significant	Tangible harm, extra effort required to repair	2
Damaging	Significant expenditure of resources required Damaging to reputation and confidence	3
Serious	Extended outage and/or loss of connectivity Compromise of large amounts of data or services	4
Grave	Permanent shutdown Complete compromise of data or services	5

Risk Detection	Likelihood of Detection	Score
Extremely High	Very obvious or easy to detect	1
High	Relatively easy to detect, quite noticeable	2
Medium	Can be detected, additional efforts	3

	are required	
Low	Difficult to detect, quite likely to remain hidden	4
Extremely Low	Exceedingly difficult (almost impossible) to detect. Almost certain to remain hidden	5

Table 2 Risk impact criteria

A Risk Probability Number (RPN) is determined by the product of probability, impact and risk detection: RPN equation: RPN = Probability x Impact x Risk Detection (ISO27k forum, 2012). The resulting value between 0 and 150 is used to determine the severity of the identified threat.

The significance of this equation is that converted risk levels may be reduced to zero if either impact or probability of the risk is scored at zero. Regardless of other variables in this calculation, if the threat is unlikely to ever occur or the impact to the business following this occurrence is negligible, there is no need for any action by business management to mitigate the risk.

Ordering risks by these values enables management to quickly and easily prioritise their resources, ensuring that risks with the greatest severity are addressed first. These values are subsequently converted into a qualitative range in accordance with the OCTAVE approach, providing directed focus of security issues surrounding critical assets. The qualitative conversion and result definitions present the agile risk management approach as outlined in table 3.

RPN Value	Converted Risk Level	Definitions
0	**Negligible / No Risk**	Negligible to no potential for impact on business objectives and/or reputation. No additional controls or procedural changes required unless a significant cost benefit exists in line with business objectives.
1 – 10	**Very Low Risk**	Limited potential for impact on business objectives and/or reputation. Additional controls or procedural changes only required if a cost benefit exists in line with business objectives.
10 – 20	**Low Risk**	Potential for minor impact on business objectives and/or reputation. Management to identify if a cost benefit exists in establishing improved controls or procedural changes.
20 – 40	**Medium Risk**	Potential for unfavourable or negative impact on business objectives and/or reputation. Management consideration recommended establishing viable risk controls or procedure changes in accordance with business objectives.
40 – 60	**High Risk**	Potential for unfavourable or noticeable negative impact on business objectives and/or reputation. Prompt consideration recommended to ensure risk is managed in accordance with business objectives.
60 +	**Very High Risk**	Potential for significant negative impact on business objectives and/or reputation. Immediate consideration is required to ensure risk is managed in accordance with business objectives.

Table 3 Agile risk management approach

APPLICATION OF AGILE RISK MANAGEMENT APPROACH

This section describes the application of the agile risk management approach to the ACF case study.

Selection of Critical Assets
Critical assets are those identified to be of highest important to ACF operations. The organisation will suffer significant adverse impacts in the following situations:

- A critical asset or its data is disclosed to unauthorised individuals;
- A critical asset or its data is modified without appropriate authorisation;
- A critical asset or its data is significantly damaged, lost or destroyed;
- Access to a critical asset or its data is impeded;

In consultation with ACF management it was decided that the analysis would centre on the following critical applications and systems:

- *Application A* – application controlling and storing key information surrounding the administration of medications and care requirements for clients.
- *Application B* – application controlling and storing personal information for clients, including care records, contact information and billing information.
- *Application C* – application used by management and payroll personnel to direct cash flow to and from debtors and creditors of the organisation.
- *Application D* – application used by management and payroll personnel to manage staff rosters and payments for work logged.
- *Application E* – application used by management and payroll personnel to create and dispatch billing information to clients.

The majority of assets selected by management of this ACF were key business applications. Downtime, loss of data or compromise of any of the applications listed or their data would hinder business function and therefore prove a risk.

Identification of Threats to Critical Assets
Security evaluations utilising the OCTAVE-s framework are typically completed internally by personnel who are intimately familiar with information technology security systems, infrastructure and policies. Identification of threats to critical assets involved conducting 2 workshops with ACF and EIP management. The focus of the first workshop was the identification of threats to critical assets following the OCTAVE-s approach. The second workshop concentrated on the evaluation of the threat probabilities. These workshops were facilitated by the researchers while the ACF staff responsible for the selected applications and systems were the decision makers.

In order to identify potential threats to the selected assets, each asset was cross-referenced with each control of the ISO 27002 security compliance checklist. A threat was found to be applicable where ACF did not have a control in place to protect the asset, and subsequently added to the worksheet of identified threats. Upon examining the compliance checklist once for each of the critical assets, the potential threats were identified and organised by asset for quantifiable evaluation. The next step in applying the agile risk management approach was calculating the RPN values using the risk impact criteria calculation for each identified threat. Utilising the equation RPN = Probability x Impact x Risk Detection, the researchers ranked the identified threats in order of importance based on subjective understanding of the potential risk to each of the ACF assets. In this way they could be presented to ACF management and EIP representatives for evaluation of their probability, impact and risk of non-detection.

Evaluation of Threat Probabilities
During the second workshop, the probability scores were reviewed and amended based on input from ACF and EIP management regarding their perspective on the severity of each threat to the IT assets. This collaboration provided valuable insight for ACF by revealing and sharing the detailed knowledge of organisational policies, procedures and infrastructure possessed by these individuals.

The existing security measures implemented by this ACF which affected the selected critical assets were considered and evaluated when finalising the probability scores. The ACF had a variety of protection measures including acceptable use policies, password policies and various types of protection for its IT systems. Some applications had additional security measures in place while general security practices and protocols were in place for all users of the ACF information technology infrastructure. This information was then used to prioritise the identified risks for ACF. The second workshop concluded with the successful review of threat probabilities with both ACF and EIP agreeing on what the most significant risks were to the IT assets. To

complete the process of the OCTAVE-s methodology, a protection strategy and mitigation plan for each of these risks could now be recommended.

PROTECTION STRATEGY AND MITIGATION PLANS

At this point in the analysis process, scenarios which posed significant risk to critical ACF assets due to the potential for loss of integrity, availability or confidentiality of data had been established and ranked in order of significance. Recommendations were proposed to ACF management and EIP personnel. Recommendations were aimed at improving the security of each asset in one of three fields; probability of occurrence, impact on the organisations functions and chance of non-detection. A reduction in any of these fields would reduce the overall risk outcome and the chance of damage to the organisation through compromise of that asset.

An example of recommendations included in the report to ACF to improve security for a key critical asset based on applying the agile approach is provided in table 4. A detailed risk analysis of all recommendations made in relation to this asset and policy was provided to the ACF and EIP management.

Observations	Several issues have been identified regarding the way in which medical and patient care applications are accessed: • terminals are located in easily accessible areas and several are in public and unobstructed locations; • terminals are often unmonitored by staff or surveillance equipment; • staff members are known to share and/or physically record access passwords; • complexity of passwords encourages recording of passwords by staff members; • terminals are often left logged on due to complexity of passwords and time taken for login process to be completed; • no timeout feature exists. Screen saver is displayed after 5 minutes of inactivity, preventing sensitive information from being displayed, however this will not prevent access to the information if someone attempts to access the terminal. No automated logout feature currently exists.
Potential Threat	With terminals often left vacant by staff in easily accessible locations, accessing *Application B* without authorisation would be a relatively simple task. Obtaining login credentials is also a possibility while staff members continue to freely record and share login details. Access could compromise resident confidentiality and allow unauthorised theft, alteration or deletion of key medical and personal information.
Recommendations	Short term – Revised computer use and password protection policies emphasising immediate logout from *Application B* terminals and prohibiting password sharing and physical recording. Introduction of automated logouts after periods of inactivity will ensure no information can be obtained by unauthorised personnel in the event that a staff member fails to log off. Re-education of staff to ensure proper password procedures are known and adhered to. Mandatory password complexity and regular password changes required of all authorised personnel. Long term – Introduction of RFID or equivalent login cards for all medical personnel to access *Application B* workstations. This removes the need for staff to remember passwords and can introduce an immediate logoff procedure following the completion of staff access, as logging in again becomes a simple task of swiping a unique staff identification card. This alternative would improve application security significantly more than policy change/amendment, though due to its cost, establishment time and maintenance requirements, it is proposed as a long-term possible solution.

Table 4 Application B – Unauthorised access and / or authentication – Risk Level: Very High

CONCLUSION

What has been developed and presented in this paper is not just an assessment of the ACF IT infrastructure and security practices in relation to key critical assets, but a streamlined process, the results of which can be utilised

by ACF to prioritise their IT security direction. The agile risk management approach can be applied to future IT infrastructure developments within this ACF and other SMEs.

ACF management can reapply the matrix used during this analysis to track improvements in their security infrastructure and gain an understanding of what improvements may be required in the future as their IT infrastructure (and the organisation) continues to expand.

The combination of ISO27k threat assessment categories combined with the condensed assessment framework of the OCTAVE-s risk assessment framework to analyse a specific asset creates a unique, versatile and reusable methodology with quantifiable results for future assessments.
There are potentially some improvements to be made to further streamline the assessment process. The number of ISO27k threat categories can be reduced for future assessments, as certain categories are not, and will not in the future, be applicable to IT assets. This would reduce the time required to properly perform the analysis, although care must be taken as threat categories may be overlooked.
The RPN value scale on which assets are ranked from very low to very high threat may also need to be refined. Currently, any threat from 60-150 (theoretical maximum value) represents a very high risk of compromise to the critical asset. With the addition of future data from other organisations or other critical assets, these RPN values could be normalised to form a bell-shape curve, where only the top 5% of threats (for example) represent a very high risk.

Ideally, framework templates may also be established for common asset categories, such as applications, databases, and common infrastructure components. This refers back to ISO27k categories which would or would not be appropriate to specific asset types. Having templates in place with these categories already selected would enable the analysis process to proceed much faster for each asset, as the ISO27k compliance checklist would not need to be analysed in its entirety each time an asset is to be evaluated.

The agile approach developed for the ACF utilised internationally recognised security methods and provides them with a solid foundation upon which to base analyses for potential future security risks. By addressing the threats we have outlined, the ACF will have moved closer to ISO certification if it were to become a future IT development goal for the organisation, and considerably reduced much of the time, effort and uncertainty associated with future assessments.

REFERENCES

Carnegie Mellon University (2014a) OCTAVE Method. Retrieved from https://www.cert.org/octave/

Carnegie Mellon University (2014b) OCTAVE-S Method. Retrieved from https://www.cert.org/octave/octaves.html

ENISA (2005) Template of Risk Management - Risk Assessment Methods. Retrieved from https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-ra-methods/template

ENISA (2006) Risk Assessment and Risk Management Methods: Information Packages for Small and Medium Sized Enterprises (SMEs). Retrieved from https://www.enisa.europa.eu/activities/risk-management/files/deliverables/information-packages-for-small-and-medium-sized-enterprises-smes

ENISA (2014) Inventory of Risk Management / Risk Assessment methods. Retrieved from https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-ra-methods

ISO/IEC (2014) ISO/IEC 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary. Retrieved from http://standards.iso.org/ittf/licence.html

ISO27k Forum (2007) Information security risk assessment version 2. No longer available. Originally retrieved from http://www.iso27001security.com/html/iso27k_toolkit.htmlISO

ISO27k Forum (2008) FMEA risk analysis spreadsheet. Retrieved from http://www.iso27001security.com/html/iso27k_toolkit.htmlISO

ISO27k Forum (2010) Information security risk assessment version 3. Retrieved from www.iso27001security.com/ISO27k_RA_spreadsheet_v3.xlsx

ISO27k Forum (2012) Risk register template version 2. Retrieved from http://www.iso27001security.com/html/iso27k_toolkit.htmlISO

Violino, B. (2011) IT risk assessment frameworks: real-world experience – OCTAVE. Retrieved from http://www.csoonline.com/article/592525/it-risk-assessment-frameworks-real-world-experience?page=1