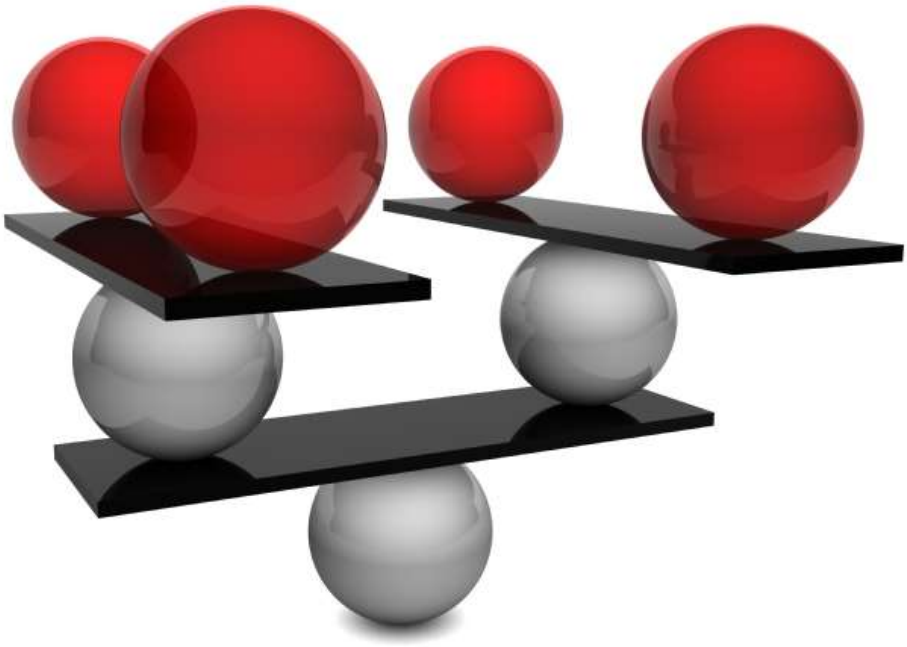
Exploring ISO/IEC 27001 Aligned Risk Methodologies



A White Paper from:

Peter Daniel,

Advent IM Security Consultant

TRANSFORMING BUSINESS THROUGH SECURITY

Introduction

Understanding how to approach risk management, both in the sense of its calculation and attempts to address remediation, is a mandatory requirement for ISO/IEC (International Organisation for Standardisation / International Electronic Commission) 27001 certification, and is becoming more and more of a recurring challenge facing today's business leaders. With best practice guidelines of those defined under ISO/IEC 27001, as well as from the NCSC (National Cyber Security Centre), taking an open-ended stance of stating to apply a strategy that aligns with business operations, this has left many with a sense of bewilderment over where to begin – let alone manage on a long-term basis. Whilst larger organisations have taken the initiative in developing their own bespoke risk assessment systems, this is not always possible for small- to medium-sized enterprises, as sourcing dedicated teams can be problematic.

Fortunately, there are those out there that are able to offer some respite and have developed risk assessment tools and guidelines that can be used by businesses to construct and maintain their own risk profile. Unfortunately, in spite of this, there are a plethora of methods on the market for businesses to choose from, which adds an extra element of confusion as to how to approach risk. As such, this whitepaper aims to provide a level of guidance surrounding the more commonly seen risk assessment tools (as identified by the NCSC), both in respects to pros and cons, and in addition to perceived intended audiences. Post each individual discussion, there will be an overarching comparison that will also give a personal reflection on own knowledge and experiences when choosing a risk methodology that will be fit-for-purpose.

Executive Summary

Many organisations struggle with implementing a risk management framework that is consistent with the demands of an ever-changing business. It is potentially highly resource and time intensive, both in respects to initial creation as well as ongoing maintenance. Choosing a risk methodology that is adaptable and can ensure consistency across the board is therefore integral to its overall strategy. With customer, suppliers, and partners ever increasingly requesting the certification of ISO/IEC 27001 for assurance of information security controls, and with robust risk assessment and risk treatment plans being a mandatory requirement as part of ISO/IEC 27001, the choice demands careful consideration.

This choice will be dependent on the structure of the organisation, its level of experience with risk, as well as the intention of the risk methodology – particularly in instances whereby a framework is already in place. Smaller to medium organisations, in addition to those new to risk, may benefit from utilising entry-level toolkits such as OCTAVE Allegro or directly adapting guidance by ISO/IEC 27005 supported by COBIT 5. For medium to large tier companies, toolkits like ISF's IRAM2 and guidance by NIST SP 800-30 will produce a more detailed and structured output, despite this being marred by membership and localisation issues. Those that are experienced in the field of risk, or have a vast number and variety of assets to maintain, may be more inclined to approach the IAS 1&2 frameworks originally drafted by NCSC's predecessor, CESG. Despite being no longer supported, this toolkit is still widely used as it is the most comprehensive and thorough by comparison. Similarly, where finances allow, many consultancy firms will provide this as a service and will conduct the assessment on the business's behalf, saving the organisation from resource and experience requirements.

Table of Contents

Introduction ..... Page 1

Executive Summary ..... Page 1

Definitions and Usage ..... Page 2

CESG – IAS 1&2 ..... Page 3

ISO/IEC 27005 ..... Page 4

ISF – IRAM2 ..... Page 5

OCTAVE Allegro ..... Page 6

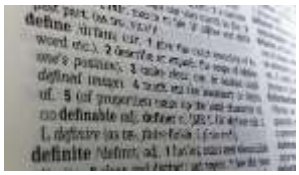
NIST – SP 800-30 ..... Page 7

ISACA – COBIT 5 ..... Page 8

Comparison ..... Page 9

Closing Statements ..... Page 10

Bibliography ..... Page 10



Definitions and Usage

Under ISO/IEC 27000, risk assessment is defined as "the overall process of risk identification, risk analysis, and risk evaluation". This, by nature alone, presents an organisation with three avenues to consider when developing their own risk management strategy. Each element is bound, formed, and interwoven with the others, so each must be acknowledged in turn in order to ensure effective operational use.

Risk identification involves the process of finding, recognising, and describing of risks – this may include their root cause, proceeding events, and potential consequences. Identification in itself can be made through reviewing historical data, performing theoretical analyses, researching expertise opinions, or in response to addressing stakeholder needs. Analysing each risk will provide the basis of comprehending the nature of the risk itself, and so in practical terms, assessing the likelihood of the risk occurring alongside the impact of such an occurrence to the business. Finally, risk evaluation involves a comparison of the results of the risk analysis against the controls currently in place to determine whether the risk is at acceptable levels or requires further treatment.

CESG – IAS 1&2

Background
CESG, prior to being absorbed into what is now known as the NCSC, produced their own suite of risk assessment and risk treatment toolsets called Information Assurance Standards IAS 1 & 2. This was a government-backed initiative to create a governance framework that could be adopted by all government functions, including the Ministry of Defence. Traditionally, these assessments would be fed into producing a weighty Risk Management and Accreditation Document Set (RMADS) that would be a mandatory document for such organisations to become accredited for storing and processing sensitive information. This was withdrawn as a requirement in January 2015 to allow for organisations to make their own decisions on which risk methodology to use, as well as to move towards more of an 'assurance-led' framework. Nevertheless, while IAS 1&2 has been archived and is no longer maintained by NCSC it is still available and remains popular across some departments of UK Government

Pros	Cons
• Highly detailed means of producing a technical risk assessment – it enforced the requirement for organisations to be properly assessed, for risks to be well communicated, and to adopt best practice • Factored in a toolset for the treatment of risks so that progress into remediation and acceptance could be tracked and managed • Standardisation of audit and accreditation of the RMADS gave strict guidelines to follow and be compliant with – this enabled replicability across the board to improve department-by-department and devise a baseline for external companies to follow	• Became a one-size fits all model that did not factor in the nuances of each individual government function • RMADS became a tick-box exercise, solely written for accreditation documents and not typically revised outside of audits • Complex and labour-intensive means of calculating risk – those new to the field may find it overly complicated for what they need, especially in the case of small to medium enterprises • Many governmental accreditors still stick to what they know and may specifically request using this method

Audience
Regardless of the move away from accreditation into now what is known as an assurance framework, this is still widely being used within government departments, despite being no longer supported. The mentality is still dependent on utilising what they know, but adapting the pre-existing standardised controls to suit on a more individualistic level. Due to the scale of what can be produced out of the IAS 1&2 toolsets, this would be more applicable to larger-scale organisations – those with a high number and variety of assets to manage and maintain, as well as to monitor on an ongoing basis.

ISO/IEC 27005

Background
ISO/IEC 27005 is the Information Security Risk Management framework subset of the ISO/IEC 27000 family of standards. As such, this is directly aligned with ISO/IEC 27001 for Information Security Management System Requirements, with components of one supporting understanding of those in another. Whilst ISO/IEC 27005's true intention is to provide more of a guideline document for information risk management, it does also offer a generic risk assessment process template within Chapter 8 and Annex E.

Pros	Cons
• Provides a solid basis for organisations to construct their own bespoke risk methodology framework • Acknowledges the flexibility and uniqueness required between organisations, as it allows for a tailor-minded approach to risk • Offers the choice of three simplified example risk matrix calculation methods • Built specifically with ISO/IEC 27001 in mind and is intended to align directly with its Annex A controls	• Not explicitly designed to be a risk assessment methodology, so templates presented are more high-level overviews of what should be included • Can be perceived as too open-ended – provides basic directions as to how to approach a risk assessment framework, but does not go into specifics • Potentially difficult to understand the approach if not familiar with ISO/IEC 27001 and its controls

Audience
Whilst ISO/IEC 27005 aligns directly with ISO/IEC 27001 for Information Security Management Systems, and provides a toolset which can be adopted around the controls specified, it is presented as a high-level guidance document that should be adapted to suit the business. With that in mind, this tool would be more applicable to those whom are familiar with ISO/IEC 27001, or those whom are in the process of becoming certified to that standard – this may be the result of a requirement from the company's clients, its partners, or as best practice governance.

ISF – IRAM2

Background
IRAM2 (Information Risk Assessment Methodology 2) is a commercially built tool devised by the ISF (Information Security Forum). Its purpose was to be a "complete end-to-end process that provides a robust and rigorous approach to enable risk practitioners and management to form a unified view on information risk across different areas of the business". The toolset is accessible exclusively to ISF members, with supplementary support documentation and consultancy being offered by ISF to assist with its use.

Pros	Cons
• Membership provides additional support services and training surrounding the use and maintenance of the IRAM2 tool, as well as having access to the ISF research library, their security health check tool, and various workshops • ISF can be outsourced to produce and maintain the risk assessment tool on the organisation's behalf, saving the company's own resource and efforts • The updated version accounts for the need to be business-focused, produce consistent results, and act as an end-to-end process	• Only offered and provided to members of the ISF whereby subscriptions may be expensive for small-scale organisations • Consultation on either having the risk assessment done on behalf of the business or as a training regime is excluded from the cost of the membership • Intricately designed which could be daunting to those new to risk methodologies – it has been created with a level of risk management and technical expertise in mind

Audience
The audience of this toolset is restricted to ISF membership where subscription costs being potentially too expensive for small-scale enterprises. Nevertheless, the options available for consultancy support and outsourced maintenance may appeal to medium- to large-sized organisations, and especially those operating within the private sector. Additionally, this may attract those whom are experienced with risk management techniques and are looking for a more comprehensive system.

OCTAVE Allegro

Background
The OCTAVE (Operational Critical Threat, Asset, and Vulnerability Evaluation) Allegro risk assessment methodology was first published by Carnegie Mellon University in the USA. Developed to be asset-focused, it places a particular importance on compiling a descriptive profile of assets, threats, and impacts, which are then scrutinised against real-world, working scenarios. An emphasis is placed on managing the risk assessment in more of a workshop style, utilising a small group of participants from a range of business operations to promote a collaborated message surrounding the organisation's approach to risk.

Pros	Cons
• Positioned as an entry-level framework for organisations who have little to no knowledge of conducting risk assessments • The framework itself is freely available for organisations to download and use, with additional e-learning training where needed being provided by Carnegie Mellon University for a small fee • Responsibility and ownership of risk management is divided between key stakeholders from across the business, enabling a consensus stance to its overall progression and maintenance	• Can present itself as being over-simplistic and as more of an introductory tool – attempts to delve into more granular detail could pose as a challenge • Highly resource intensive as it requires input from a multitude of different stakeholders from across the business • Possible conflicting opinions regarding the overarching strategy of risk management, as well as prioritisation of key areas of concern to address, could force unnecessary delays • Regular organisation of key stakeholders may cause complications to the risk management's continual maintenance

Audience
As an entry-level framework, this would mainly be directed at small-scale organisations or new start-ups that require an introduction to risk assessment techniques. Alternatively, this may also appeal to organisations that are seeking to return back to basics and attempt to devise their own bespoke system for risk management using this as a foundation. This may not suit larger or more experienced organisations – those with a high number of assets to assess and manage – as risk criteria and treatment will demand a more in-depth and meticulous examination.

NIST – SP 800-30

Background
NIST (National Institute of Standards and Technology) SP 800-30 is a US-based initiative produced primarily for US government agencies and is mandated as such. It is unique insofar that it features a step-by-step guide to explain the entire lifecycle of risk management: initially starting with pre-preparatory work towards the assessment, during its conduct, communicating the results to the wider business, to ensure its continual maintenance, and to then monitor its effectiveness. Their objective is to popularise the significance of acknowledging a risk assessment as a living document; one that is frequently reviewed and amended in line with changes to business operations, stakeholders, systems, and services.

Pros	Cons
• Created to be consistent with the ISO/IEC standards to allow for simple integration with pre-existing management systems • Freely accessible on NIST's website for organisations to download and use • Clear, concise, and regimented instructions which can enable it to be used alongside other risk assessment toolkits for a multi-faceted approach • Aimed at organisations of all sizes and across both the public and private sectors	• Through being a US-based initiative, most of the supplementary documentation is heavily focused on US legislation and regulation, and therefore, not necessarily applicable to non-US companies • Implementation support services through NIST are limited to US organisations, and so, sourcing appropriate, localised advice may prove difficult • Produced as a set of guidelines to follow – it is not a risk assessment framework in and of itself

Audience
Despite being a comprehensive system with procedural instructions as to how to adequately implement and manage the risk assessment on a long-term basis, its main audience is for US enterprises. However, for organisations that are adept with risk control methods and are in a state of complete understanding of their wider regulation and legislation stipulations, this would integrate with and potentially bolster risk management systems current in place.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

ISACA – COBIT 5

Background
ISACA's (Information Systems Audit and Control Association's) COBIT (Control Objectives for Information and Related Technologies) framework was created to provide a set of controls for the organisation of IT governance and best-practice management. COBIT's component #5 relates to information security risk management and has been written as an extension to the guidance defined under ISO/IEC 31000 (for general risk management), and more specifically, ISO/IEC 27005. The document itself can be bought on ISACA's website with additional guidance notes, case studies, and training available to purchase.

Pros	Cons
• Elaborates on the previous guidance and control objectives provided by ISO/IEC 27005 and 31000 • Built on taking a holistic approach to risk management that aims to support and improve processes from end-to-end • Flexible and adaptable enough to be embedded into any pre-existing risk management framework, which may simplify the process of aligning it to ISO/IEC 27001	• Is intended to be a supplementary guide to a company's pre-existing risk management framework – not be to utilised as a standalone document • In order to be fully effective, this needs to be bought and integrated alongside ISO/IEC 27005 for contextual understanding • Can be viewed as being overly theoretical and complex in its interpretations of the ISO/IEC standards

Audience
Through being an extension of the ISO/IEC 27005 and 31000 guidance documentation, this would more aptly suit companies that are aiming for ISO/IEC 27001 certification and require some additional context on how to more effectively approach the controls. Subsequently, this framework makes an assumption that a risk management system is in already in place, and should be paired as such. As a result, this would be more applicable to organisations that are familiar and comfortable with risk frameworks but are seeking to enhance their current system through expanding its scope.

Comparison

As has been explored on an individual basis, the risk methodologies span multiple audiences and have been created with different intentions in mind. Each comes with its own benefits and flaws with none being regarded as the ideal solution. Adopting any risk management approach has to align with the direction and operation of the organisation. It has to consider whether a simplified or more comprehensive outlook will be suitable for the nature of the business, as this will be based on the scope of assets to be evaluated, whether multiple locations or suppliers are to be included (especially on a cross-geographical basis), what legislation and regulatory standards need to be adhered to, the resources and time required to conduct the risk assessment, and who will ultimately be the responsible party for ensuring that the overarching system will be continually maintained.

Whereby an organisation is seeking to improve on pre-existing risk management frameworks (either those using dedicated toolkits or those who have devised their own in-house system), then the likes of ISO/IEC 27005, NIST SP 800-30, or COBIT 5 would prove the most suitable. Whilst NIST SP 800-30, when compared to the other two, would enforce a level of direction when conducting the risk assessment, it is heavily tailored to US institutions and may take a lot of tweaking for localisation. COBIT 5 would also provide a level of direction for businesses attempting to construct a more linear and streamlined process, but would be most effective when paired with ISO/IEC 27005 for a collaborative approach. As standalone guidance, ISO/IEC 27005 should gain the most appeal as this has been designed for the sole purpose of aligning with ISO/IEC 27001 and could provide a level of assurance to those self-assessing their own risk management framework in accordance with the ISO/IEC 27001 controls.

If an organisation is looking to build a risk management framework from scratch (either for the purposes of redefining their risk approach and direction or due to it being a new operational requirement), then toolkits such as NCSC/ CESG's IAS 1&2, ISF's IRAM2, or OCTAVE Allegro would be most appropriate. In the rationale of having a lack of experience within risk, then an entry-level system like OCTAVE Allegro would feature prominently as an option. Concurrently, this toolkit would suit smaller enterprises; those with limited amounts of assets and varieties. For businesses that have a dedicated risk management function with experienced personnel, then either NCSC/CESG's IAS 1&2 or ISF's IRAM2 may be favoured. The former of the two is far more complex and sophisticated but demands a higher amount of resource effort and attention because of it. Assistance and further guidance to the toolkits are offered by all three vendors, however, only in the cases of IAS 1&2 or IRAM2 are options available for a consultant to conduct the risk assessment on the organisation's behalf. This may be attractive to larger companies with the finances available, but not necessarily the level of experience needed to conduct the assessment by themselves.

Closing Statements

Whilst ISO/IEC 27001 mandates that a risk assessment must be completed and evidenced, with associated risk treatment plans in place, what is important to note is that adaptability and a need to be concurrent with the intricacies of the true business operations is imperative. Each organisation must demonstrate that the risk management framework used (in whatever form that takes) is reflective of top managerial direction, while being replicable throughout the business. Simultaneously, it must be kept up-to-date with changes in operations, systems, suppliers, partners, and legislation and regulatory controls in order to maintain integrity.

The assessment of risk methodologies throughout this whitepaper is to serve as an introductory guide to what is available to organisations on the market today, and as identified by the NCSC. Note that this is not an exhaustive list, but is intended to set the scene for organisations to conduct their own preparatory evaluations before deciding on a risk management framework to adopt. In essence, it does not matter which risk methodology is selected provided the organisation has a business justification for its use and it can be proven to be fit-for-purpose, especially in relation to ISO/IEC 27001 stipulations.

Bibliography

CESG IAS 1&2 (2015) *Information Risk Management: HMG IA Standard Numbers 1 & 2*. Retrieved from https://www.ncsc.gov.uk/guidance/information-risk-management-hmg-ia-standard-numbers-1-2

ISACA COBIT 5 (n.d.) *What is COBIT 5?* Retrieved from http://www.isaca.org/COBIT/Pages/COBIT-5.aspx

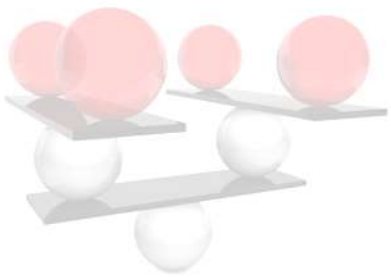
ISF IRAM2 (n.d.) *Information Risk Assessment Methodology 2.* Retrieved from https://www.securityforum.org/tool/information-risk-assessment-methodology-iram2/

ISO/IEC 27005 (n.d.) *ISO/IEC 27005:2018 Information Technology – Security Techniques – Information Security Risk Management*. Retrieved from https://www.iso.org/standard/75281.html

NCSC (2016) *Summary of risk methods and frameworks*. Retrieved from https://www.ncsc.gov.uk/guidance/summary-risk-methods-and-frameworks

NIST SP 800-30 (2012) *Guide for Conducting Risk Assessments*. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

OCTAVE Allegro (2007) *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process.* Retrieved from https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=8419



advent-im.co.uk

0121 559 6699

0207 100 1124

@Advent_IM

bestpractice@advent-im.co.uk