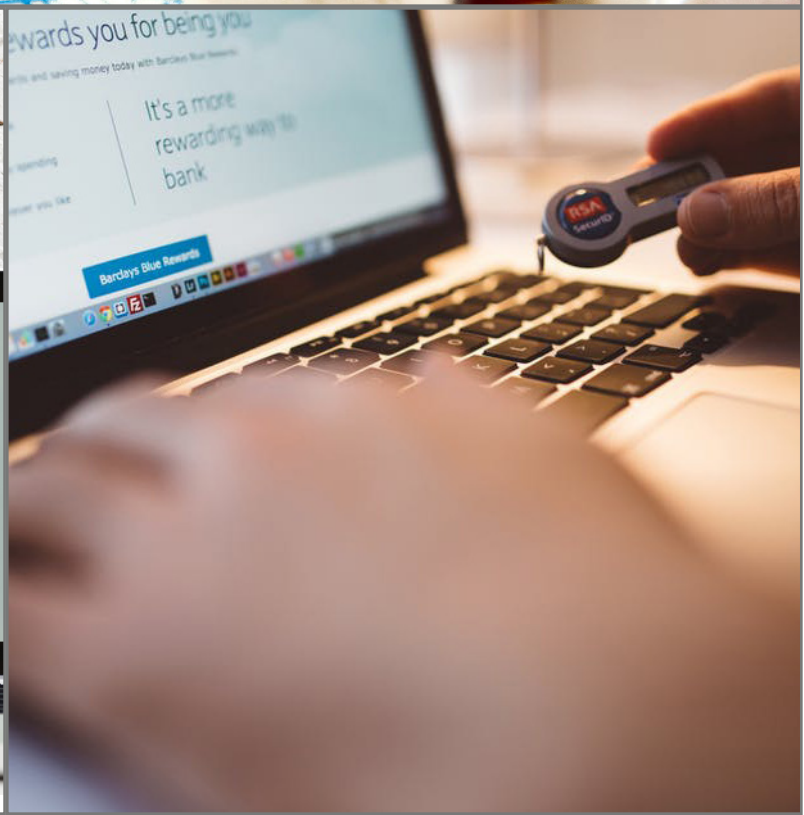
RISK METHODS



A further Review of Risk Methods

Il7 Consultants will work with customers to define which methodology they prefer. IL7 consultants will identify salient features and reasons for implementing a framework and discuss these with clients with some assurance.

The purpose of Risk Assessment (Identify, Analysis + Evaluation) is said to be recognition and ranking of risk. This is common to all methods. But each method associates different meanings with the words it uses. The difference between Analysis and Evaluation are clearly defined in ISO 73. In IS1/2 the calculated risk is set against the pre-defined risk appetite. If it is within this risk appetite it can be tolerated (accepted by an Accreditor) rather than escalated to the business risk owner (SIRO). In fact RMADS are rarely signed off by SIROs or IAO's, although individual risks might be escalated by means of a Risk Balance Case (RBC). IL7 will promote a framework and culture where all calculated (analysed) risks are evaluated within business context and where thought appropriate, promote the escalation of risk "sign off" to the business owner.

It is the implementation of IS1 and the culture within many organisations that denies the SIRO access to subject matter expert opinion on the risks that are taken on their behalf by the process of acceptance "if it is within pre-defined risk appetite". In this IS1/2 is very similar to the Orange Book even though its implementation has often excluded the SIRO. In fact IS 1/2 addresses risk appetite in the context of accepting and managing residual risks. It is not forthright about opportunity risk and how risk attitude can be a positive factor determining risk appetite. The Orange Book is more balanced on Risk Appetite. The concept *(of risk appetite)* may be looked at in different ways depending on whether the risk (the uncertainty) being considered is a threat or an opportunity. It says "In considering threats the concept of risk appetite embraces the level of exposure which is considered tolerable and justifiable should it be realised. In this sense it is about comparing the cost (financial or otherwise) of constraining the risk with the cost of the exposure should the exposure become a reality and finding an acceptable balance" This fits with IS ½ concept of accepting residual risk. But it also says "When considering opportunities the concept embraces consideration of how much one is prepared to actively put at risk in order to obtain the benefits of the opportunity. In this sense it is about comparing the value (financial or otherwise) of potential benefits with the losses which might be incurred (some losses may be incurred with or without realising the benefits). But it is unfair to think that IS1/2 ignores the benefits. IS1/2 says on page 17, that it is about balancing the benefits of risk. But it also states that the Management Board must clearly state 'and the SIRO must actively demonstrate the Management Boards endorsement of, and commitment to the information risk management statement by signing it on their behalf. It is then quoted in RMADS as the reason for accepting or treating risks. IS1/2 only ever mention opportunity when talking of threat actors 'opportunity' to attack, not in terms of projects benefiting from taking an 'opportunity risk'.

These two factors, the promotion of the SIRO to signing the risk appetite statement, to be interpreted by others against individual risks, and the negativity of IS1/2 to risk being an opportunity means that IS1/2 does not fit in with, or does not seem to fit in with, business opportunities facing the digital world. HMG organisations want to benefit from the opportunities of COTS, BYOD and mobile working. The stepped approach and the risk tables coming out of the IS1/2 procedures might be seen to preclude this flexibility. IS 1/2 needs skilled consultants to achieve the balance necessary.

In practice where the calculations have achieved negative results the pragmatism, imagination and flexibility of the practitioner has achieved the solution, sometimes in spite of the methodology.

The Open Group suggest FAIR (Factor Analysis for Information Risk) as a methodology for providing a risk assessment in line with ISO/IEC 27005 and of course ISO/IEC 27001. FAIR focuses on identifying the factors that drive loss magnitude when events occur. Again, FAIR concentrates on loss rather than opportunity. An asset's loss potential stems from the value it represents and/or the liability it introduces to an organization. So, FAIR presents loss as a mathematical model of a range of likely monetary values. This follows the maxim "if you cannot measure something, how can you improve it?". CISSP teaches the mathematical formula based on the Annual Loss Expectancy (ALE). Whether the risk is presented in real currency values (Quantitative) or just a consistent comparative (Qualitative) value (high/medium/low) it is important that the business is presented with this in language understands. It is important too, that even qualitative descriptions should be accurate and as well defined as possible – be precise; the more the customer can feel the pain the greater the message. Consultants must quantify potential loss to the business owner but should keep this in the context of the opportunity benefits to be realised if risk can be cut to a manageable (acceptable level).

It is amazing how many definitions of risk there are and how the subjective contextualising of risk has both its good and bad points. While such individual interpretations are bad for consistency, they can be sometimes beneficial to business understanding. Most methodologies studied tend to be focused on different businesses. This is addressed by ISO's Guide 73 which gives definition to a lot of the terms used by analysts. IL7 will be versed in these definitions and it is important to note that Guide 73 itself is currently being revised. FAIR has its own definitions for impact, being the consequences from a loss of CIA – those being reputational, operational, financial and to compliance. More so FAIR separates losses into primary and secondary. Primary losses include productivity, cost of recovery and replacement. These are direct. Indirect, secondary losses include fines incurred, reputation and loss to ongoing business as well as competitive advantage. FAIR describes different landscapes such as the loss landscape and the vulnerability landscape. As well as coming to a measurement, the other most important outcome of risk assessment is that it makes the involved business community think about their contextual landscape.

Where it is appropriate IL7 will lift other tools from other methodologies such as Octave Allegro from the Software Engineering Institute (SEI). Allegro was a result of practitioners realising that earlier versions of Octave were too cumbersome and resource consuming, too complicated to generate a risk aware culture. Allegro focused on information assets as primary and other assets (people, paper and IT) as containers. Threat identification became streamlined and threat scenarios analysed in workgroups. Threats were closely analysed, vulnerabilities less so and greater emphasis on quantifying risks so as to prioritise them generated a more risk aware culture. The lessons communicated in the Allegro methodology are not just from methods themselves – IL7 do not favour worksheets, questionnaires or surveys over direct communication nor do we ignore vulnerabilities – but to simplify where possible and to streamline without missing a trick and to involve people in the process are all important. Brainstorming with relevant, interested parties can also be a faster, simpler way of exploring scenarios and gaining consensus on consequences and impact. The SWIFT (Structured What If Technique) is a systematic team-orientated method for

hazard assessment, which IL7 might use if considered appropriate. In this context a 'hazard' is any scenario with a potential for causing harm, so equal to the negative side of risk. IL7would invite participants to list 'hazards' then consider causes, consequences (including frequency) and possible safeguards needed. These would then be recorded as evidence. To combine SWIFT with 'Attack Tree' technique can give us a more granular cause and effect model. As seen later, where IL7 model the cyber threat with a customer IT expert, breaking down the stages of an attack from the attackers' exploration of the victim's vulnerabilities to the victims likely suffering can deliver an effective picture of the organisations threat landscape. It needs to be current and reflect today's cyber threats and the changes these represent.

The Institute of Risk Management (IRM) produced a standard in 2002 which presented externally and internally drivers of operational, financial, reputation and hazard risks. This separation is useful and consultants derive business context from these drivers and should explore them first before analysis and evaluation. The framework the IRM does not depart far from others and actually the procedure and use of tables is not dissimilar to IS ½. One point in favour is that IRM do identify opportunity risks. These can be treated similarly to negative risks. Communication – both internal and external are also addressed.

IRAM 2 is used by members of International Security Forum (ISF) and the Risk Manager tool can be purchased by non-members. Like other methodologies it provides a repeatable consistent framework involving spreadsheets to evaluate suppliers, create scenarios and model threats. It claims to provide a business centric view to develop a pragmatic risk treatment plan. As a commercial based method its major advantage would be the support of ISF membership.

ISO uses all 4 T's (Treat, Tolerate, Transfer and Terminate) as referring to Risk Treatment (Responding) within the context of the ISMS. IS1/2 identifies the controls and plans the treatment, the Risk treatment Plan or Risk Register. It does not deal with monitoring and communicating in its ten step model. It describes the operational controls that maintain assurance is in place. The author of the RMADS (the SyAc) may also be responsible for producing SyOPs but the SyAc is only sometimes part of the continuous improvement cycle.

ISO 31000 recognises the effect of time on risk. Assets, their containers (vulnerabilities) and the threats change over time. The RMADS state that if there is a fundamental change to the system the RMADS will change but it doesn't necessarily mean that the Risk Assessment will be re-done. It is not particularly agile. The SyAc should either instil the need for ownership and change management in the customer's people or remain as part of the process. ISO 27001 ISMS calls for continuous improvement and to do this when there is change to risk, there must be continuous assessment and analysis. Analysis brings about measurement and prioritisation and as we know "if you cannot measure something you can't improve it".

ISO 31000 describes the components of a risk management implementation framework. The initial action required is to get 'mandate and commitment' from the highest stakeholder followed by implementation:

- Design the framework.
- Implement Risk Management within the framework.

- Monitor and review framework, learn and report.
- Improve the framework.

ISO 31000 describes a framework for implementing risk management rather than a methodology for supporting risk management. Each organisation might have a different method, an architecture that supports risk management, the strategy and the protocols. This might include who is involved in meetings / reviews, the authority and frequency of these meetings and the means of communicating messages or decisions from these meetings. Risk strategy follows the organisations attitude regarding risk, its appetite and philosophy.

IS1/2 gives us a structured approach based on threats. It follows the Domain Based Security (DBSy)[1] which regarded people as the main threat (rather than hazards). Threat Actors could be users, administrators, suppliers, hackers or others. Other approaches can be focused on the organisations assets or the services it provides. It is important to combine all three but not just go over the same ground. The discipline required is to provide a list of all possible threats. IL7 will analyse them and concentrate on those that are real, with real potential impact and probability. However, one criticism is that IS1 produces a long list of risks that are repetitive and meaningless. An experienced practitioner would always consolidate and prioritise risks. In IL7 experience this meant the presentation of, at most, four or five consolidated prioritised risks. This was often overlooked by people familiar with the process but not the practice.

[1] See earlier footnote regarding DBSy's origins.