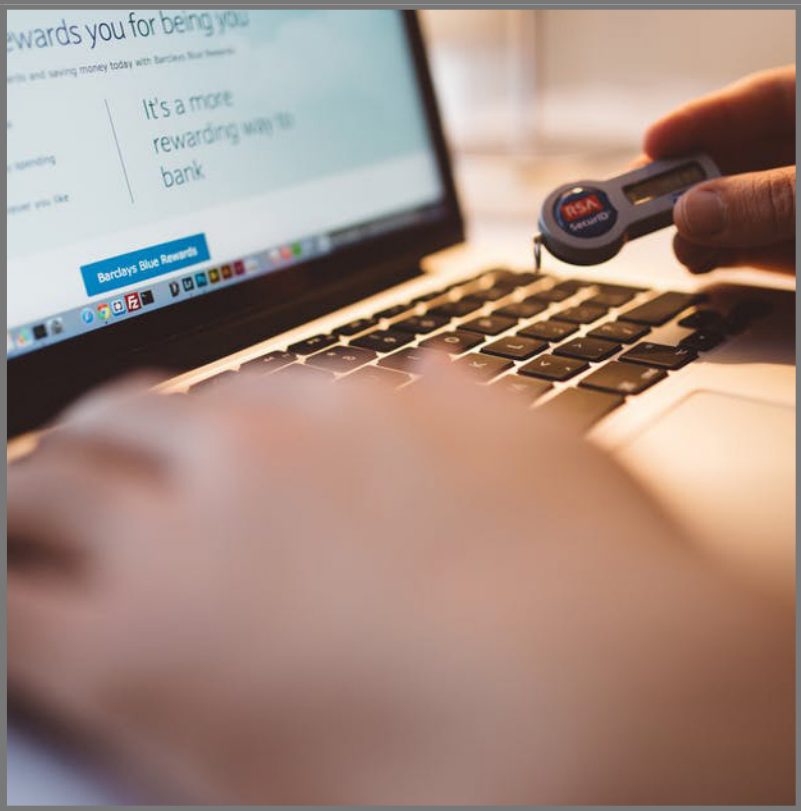
RISK MANAGEMENT



Risk Management

IL7 consultants will operate within a framework consistent with ISO 31000 principles, clauses and guidelines. Consultants will start by discovering the context of where they are operating first. The object is to understand the business, whether it be HMG or local government, a utility or service provider. Our consultancy will not just be about risk assessment and presenting an RMADS type document, but about risk management, including how system managers communicate security and risk awareness and how they monitor progress of controls – how they will keep the risk management progress alive and bring about continual improvement. In effect, our presence will build capability and competence.

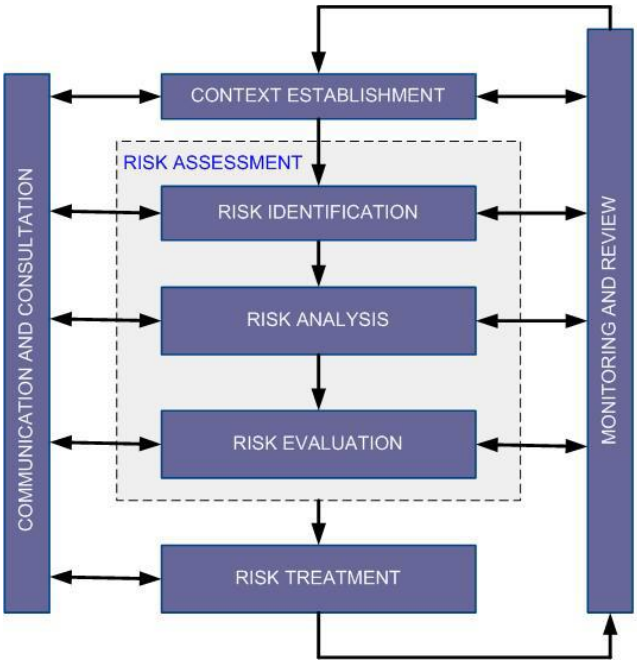


Figure 1 – ISO 31000 Risk Management Model

IL7 will also embrace ISO/IEC 27005, Risk Management Standard. We will seek to introduce a systematic approach to implementing an Information Security Management System (ISMS) based on the business context of risk. It will be a consistent approach based on the customers need. The ISMS will be aligned to overall risk management; it will be a cyclical and iterative process of consultation. It will reflect the organisations risk appetitive, its attitude to risk. The consultant(s) will analyse and evaluate risks accordingly, taking into account the calculated impacts and likelihood but this will be done through consultation and using intuition based on experience and expertise rather than cumbersome questionnaires and worksheets. If customers wanted a quantitative analysis with sterling values, if their compliance needs or adopted corporate strategies dictate, real values will be used. Risk needs to be quantified to be prioritised and to be dealt with as business need requires. Where figures are not available qualitative analysis will expose the order risks need to be addressed and expose in clear and precise terms the consequences and benefits of doing so. We would also keep away from the prescriptive conformity of compliance for the sake of it, preferring to examine and focus on context rather than a set of mandatory, prescriptive control rules. IL7 believe it is the quality of the consultancy which derives risk based measures. It is the quality of the consultancy that delivers a message that is accepted and the on-going processes for improvement are adopted.

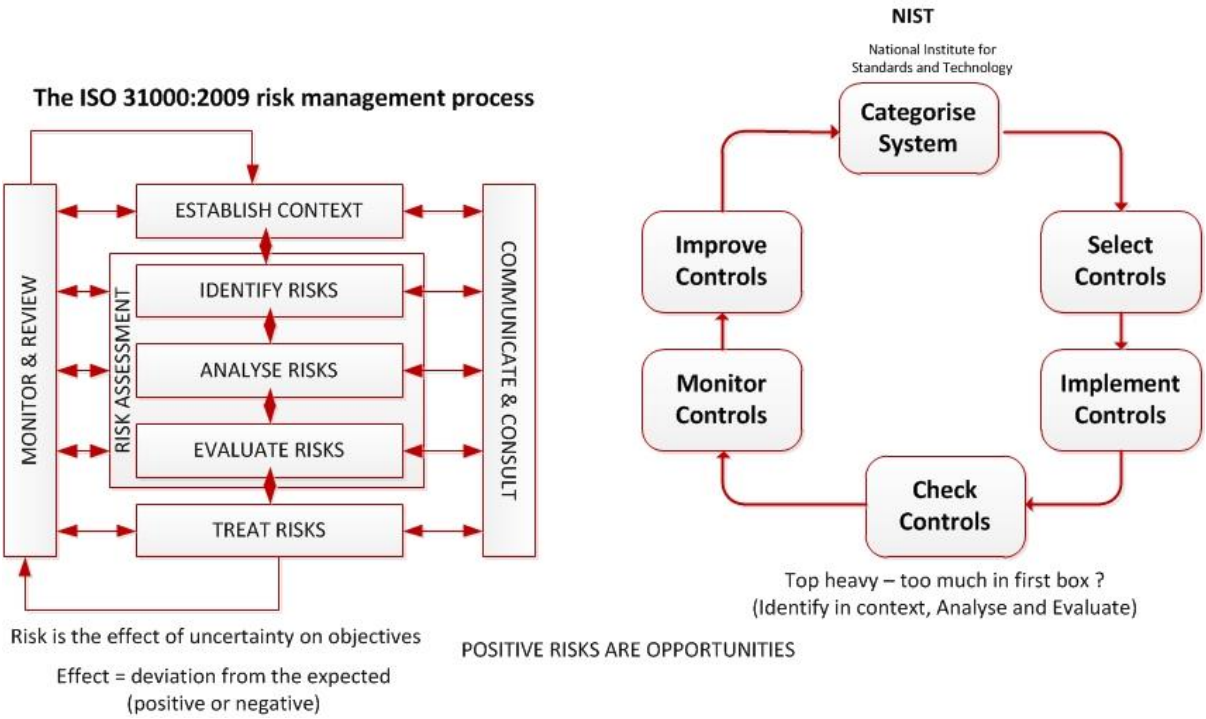


Figure 2 – Assessment and Prescription

These above alternatives are not fundamentally different approaches, though the National Institute for Standards and Technology (NIST), mandatory across US government is a prescriptive set of controls up front. IL7 believe risks have to be identified and prioritised to get business buy in for their treatment. In order to prioritise they need to be calculated, measured. As Lord Kelvin said, "If you can't measure something you can't improve it". ISO/IEC 27005 provides guidance on using qualitative and quantitative approaches. The standard is not prescriptive about which should be used but does say that an assessment must include, and account for, threats, vulnerabilities, and impacts which must be contextualised to the business, then fed into the risk evaluation process. If a customer has a chosen risk methodology IL7 will work with them. If not a method will be developed to use as a structured, repeatable process to measure the risk, assessing the impact in customer terms and analysing the probability. This latter can be based on empirical customer evidence and based on considered threat capability and motivation.

IL7 consultants will also assess opportunity risk; they will be facilitators of risk taking for business benefit. Risk Assessments, the RMADS, in HMG mainly address manageable, controllable risks. Paul Hopkin, Ref [14] identifies three types of risk, hazard, control and opportunity. Hazard risks are avoided by having Disaster Recovery and a Business Continuity Plan rather than actually assessing the risk. Manageable risks are treated by prioritisation and through adopting proportionate and appropriate controls. Risk assessments also address 'opportunity' risks in new projects, new delivery programmes, and entering new markets, supplying new products and services – all opportunities for business and delivery, though not without risk. On 3rd August 2016 (Managing Information Risk) CESG defined risk as "Risk is the potential for something harmful to happen". And they are not alone. I've heard risk be simply called "the likelihood of loss". But ISO 31000 says risk is the "effect of uncertainty on objectives" and the effect can be positive as well as negative. The effect of a negative event could cause a loss. But what business thrived on not taking a risk? A business manager for

the Home Office once accused our security group of being gatekeepers, refusing to allow good things to happen. Taking my experience into account, I was able to offer solutions to his problems. I had learnt my role as security consultant in MOD and later with HSBC - I was to enable new ideas to be adopted by providing mitigation to any risk and allowing considered decisions to be made to adopt those risks. A NCSC example of such an enabler is the 'End User Device' (EUD) configuration guides which make safe intuitively or inherently unsafe devices. IL7 will encourage its consultants to use their knowledge of security technology and procedures to be facilitators of risk. We will enable businesses to embrace new technologies yet stay secure in the face of increasingly aggressive, industrialised cyber-crime. A recent paper from Cisco claims that inadequate Cybersecurity stifles innovation and taking the opportunity to provide new services.[1]

Opportunities are often represented as new projects yet in some environments they just seem to evolve. Therefore, they are not subjected to project management risk assessment. Examples of outsourcing, off shoring and even insourcing have been witnessed where the only control on the business opportunity is the deference to the security group's authority. Such opportunities should be supported with risk assessment that delivers business outcomes, protective measures that allow the benefits to be realised in safety. IL7 will work with and within projects to enable this.

In IL7 experience in HMG, the consequences of not working within the bounds of safety were defined by the IS1 impact levels to Confidentiality, Integrity and Availability (CIA). CLAS consultants drew on the 'what ifs' and weighted CIA on the severity of the possible consequences. But these were 'business of government' consequences. Possibly they were too narrow. No government has gone out of business because of a realised cyber risk. Expanding the realms of risk management beyond central government into local government, utilities, facilities and commerce, we discover the actual consequences, beyond CIA. These risks realise consequences that are to operational capability and effectiveness, loss of intellectual property, directly financial, reputational or to compliance. And the last of these has particular relevance in the coming years, the European General Data Protection Regulation (GDPR), Ref [19]. (According to a Symantec poll last month 96% of businesses still don't understand the implications[2] – while central HMG might, how many local authorities are actively pursuing their readiness for this?) Some of the changes GDPR will usher in will have wide ranging benefits for data controllers and organisations but there will also be penalties to avoid. Compliance Risk, the risk of being non-compliant, drives forward measures that in themselves mitigate the other risks, operational, financial and reputational. Compliance with ISO/IEC 27001, Ref [5], generates the controls and promotes the all-important 'management system (the ISMS). This in turn establishes processes for monitoring and communications, a corporate culture in line with risk attitude, in line with ISO 31000, including Corrective Actions/Preventative Actions (CAPA) internal audit and management review. The GDPR compliance requirement is about 60% legal and 40% technical and we will advise clients to seek legal advice while IL7 itself will partner with law practices. Like the UK DPA, organisations as well as complying with the eight principles for protection (need to have, process etc.), must demonstrate they have the measures in force to protect personal data when it is being

[1] Cybersecurity As a Growth Advantage – Cisco Study 2016

[2] http://www.computerweekly.com/news/450401190/UK-firms-could-face-122bn-in-data-breach-fines-in-2018

processed or stored, and destroyed when it is no longer needed. What better way to demonstrate this than to comply with ISO/IEC 27001? Indeed many smaller government organisations are already abandoning analysis based risk assessment for compliance, and while IL7 do not support this, it is a business choice. Of course, compliance with ISO/IEC 27001 is also an opportunity risk – organisations who adopt it gain business benefits, seek out new opportunities and gain a real commercial advantage. In recognition of this IL7 has sought out partners in its CCP community for certified ISO/IEC 27001 practitioners and auditors. IL7 will engage these practitioners and auditors to alleviate the Compliance Risk. Similarly we will advise smaller customers (SME's etc.) of the advisability of adopting 'Cyber Essentials' and following the '10 steps to Cyber Security', Ref [25]. It makes common sense and lends commercial advantage. In turn other members of IL7 will concentrate on the business risks to operations, finance and reputation. Some organisations might not be able to afford ISO/IEC 27001 or want to go the whole journey. IL7 will still ensure a risk managed approach to security, including compliance with the GDPR.

As said, IL7 will adopt the methodology chosen by the customer, or if the customer wishes to move away from a legacy methodology, IL7 will use its knowledge of existing methodologies to find or develop one that suits. The principles of risk management have not changed over the years, even if the demands for outcomes have increased, as have the fluidity and the bombardment of risks themselves. Our experience is derived well before the Orange Book of 2001, updated in 2004, Ref [11], but it is worth noting that this provides an excellent grounding. There are a number of features relevant to IL7 consultancy. There is a hierarchy of risk, from corporate or enterprise risk, down to the programme then the project or system level. Additionally, the Orange Book emphasise the interaction between risks and these need to be clearly communicated. There are two distinct activities, the initial identification of risk and the need for continuous identification of new risks and the monitoring of controls. IL7 will develop from this and using the principles set out in ISO 31000, which reflect the need, not just for analysis and remediation but continuous monitoring. ISO 31000 enables understanding and grasping the importance of the inter-relationships between risk assessment, treatment, monitoring and communication. This is vital in improving the culture and the foundation on which we base any methodology. In ISO / IEC 27005 Risk Management is put into the context of ISO /IEC 27001 Security calling for the establishment of an ISMS. This is the primary vehicle for establishing the principles of and implanting the risk management framework called for in ISO 31000. So important are these principles, the ISO 31000 clauses, they are included at Annex A and have been incorporated into IL7 guidance, Ref [22].