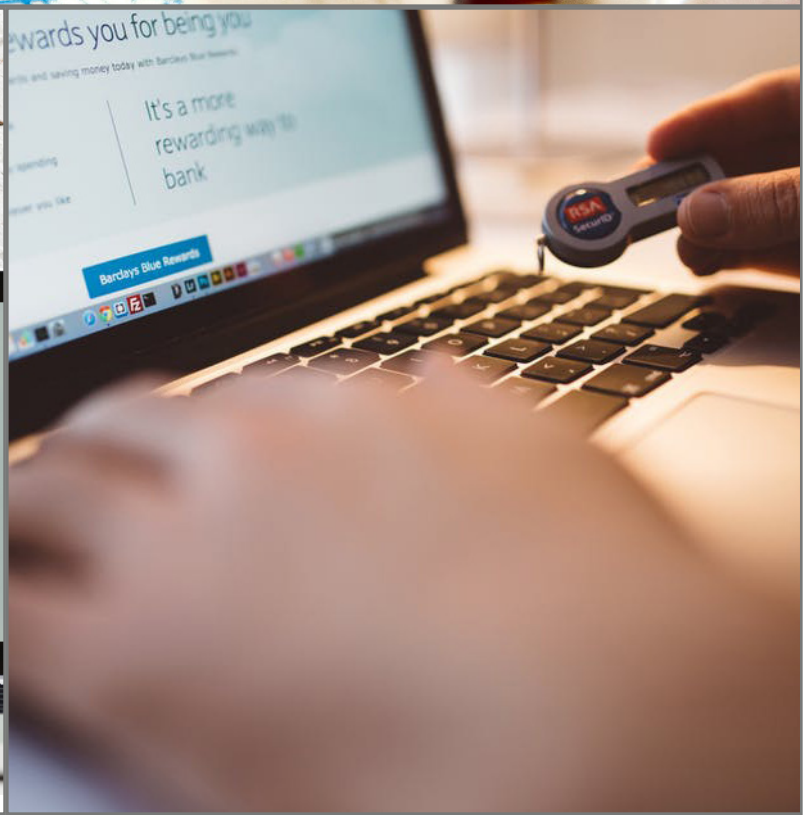
RISK CONTEXT



Setting Expectations – Recognising the Context

As documented in its earlier submission to CESG, Ref [22], IL7 will take its lead from initial customer engagement and is equipped to undertake assessments that could provide or develop:

- Enterprise Risk Management (ERM).
- Sectional (departmental) Information Risk Management.
- System or Network Information Risk Management.
- Project Information Risk Management.

Should IL7 be asked to set up the ERM framework it would be within the customer's corporate context and seek to have appropriate linkages with the business drivers of the customer organisation. Business risk drivers come from both inside and outside the organisation. They are not inherently information risks or aligned to IT. In figure 3 they are divided into financial, infrastructure, marketplace and reputational. Together they contribute to the risk attitude and policies, on which to implement risk management, and our framework will reflect this.

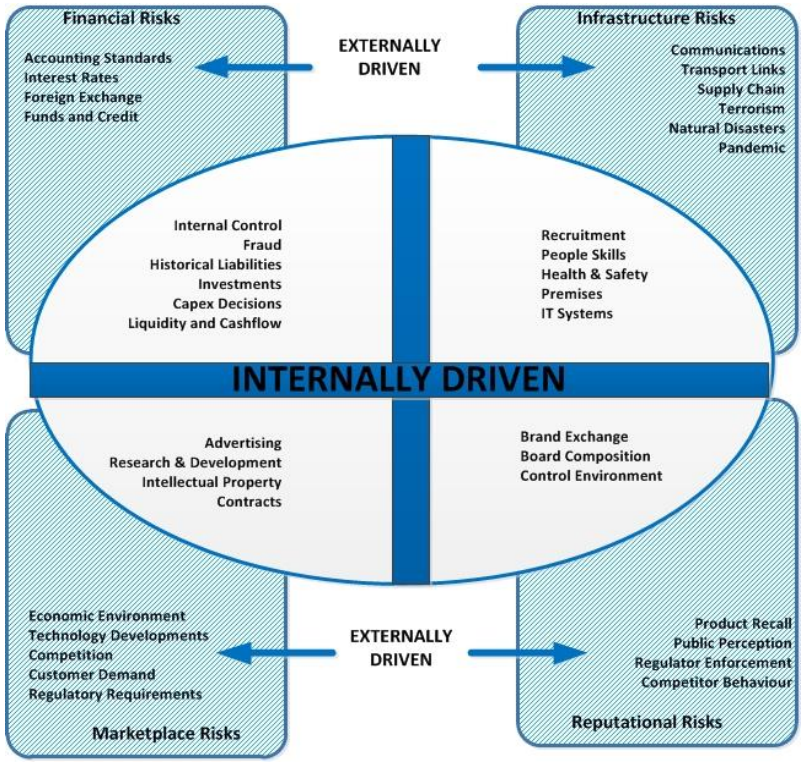


Figure 3 – Drivers of risk management (borrowed from the IRM)

Consultancy skills are honed to extract the risk attitude derived from the business drivers. During the first engagement with the customer IL7 will elicit the context and together with the customer, determine the way ahead. The customer engagement may not be with the highest stakeholder, the business risk owner, but the context can be learnt and the process ahead mapped out. This will depend on the customer, the ISMS, if already in place, whether there is a preferred methodology and what is to be risk assessed/managed.

The Assurance Framework is a good tool to work through, even in the first or second engagement. IL7 consultants will communicate and consult with initial customer representatives to discover the nature

of controls, already in place. Not enough emphasis was made in IS1/2 of consulting with customers about the different environments where assurance could come from. Emphasising the difference between intrinsic controls, where assurance can be derived from best practice in the supply chain and implantation or operation, where the onus is placed on the customer, is best done with the customer, perhaps in a workshop, not in a closed office by a lone practitioner.

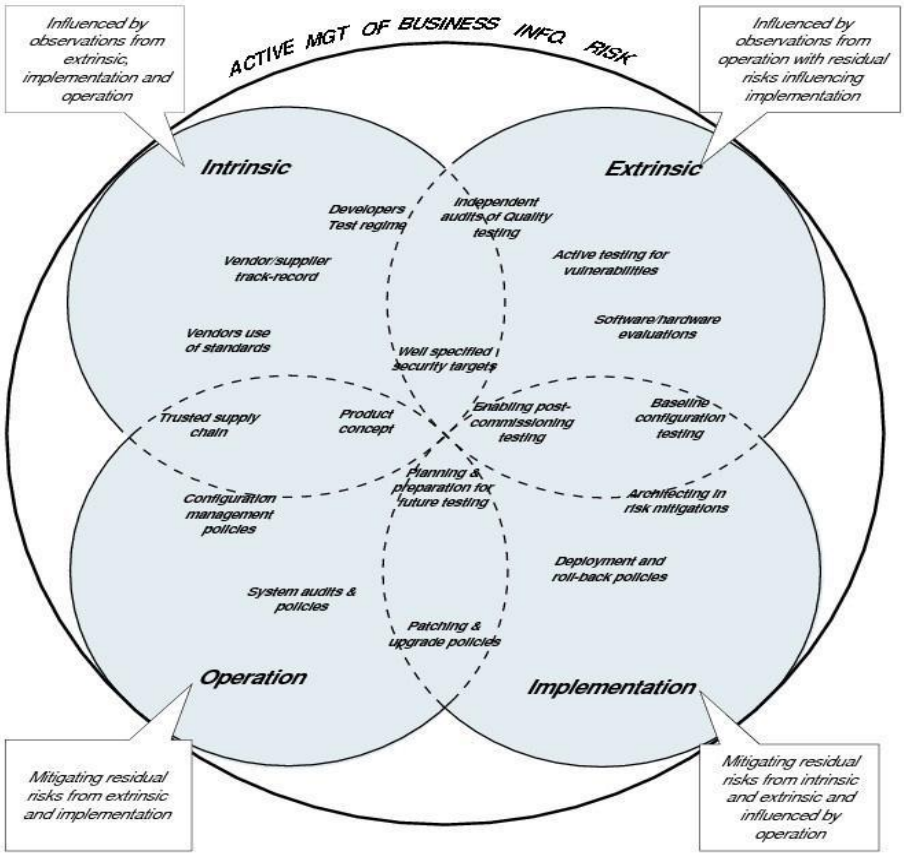


Figure 4 - The Assurance Framework

As per IL7 processes already submitted, for HMG customers previously, the consultant would produce an Accreditation Plan. For non-HMG customers this might be termed as Assurance Plan. Its purpose will be to give the customer a clear picture of to expect from IL7 in terms of approach and consultancy, as well as what will be required from the customer in terms of input. It will be a roadmap giving them and their organisation the assurance that risks can be identified, prioritised and managed in terms of Intrinsic, extrinsic, implementation and operation relevance. This will in turn demonstrate who in the organisation the consultant needs to talk to.

Whatever the customer methodology, the Assurance Plan will follow a consistent framework to meet ISO 31000. It will set out the key stages of identification, analysis, evaluation and treatment. If there is no preferred methodology for analysis (for quantifying and prioritising risk) this will be developed in the consultancy stages where the business drivers will be discovered. If there is no ISMS in place, the consultant will propose a management plan for monitoring controls put in place and making iterative improvements. For example, a project specific Security Working Group (SWG) with regular focus on the Risk Register. The Assurance Plan will include a communications strategy as set out below

for consulting, communicating and responding. IL7 would produce a document which would include sections on:

a) Governance – risk management and internal control objectives.
b) Strategy – a statement of the corporate attitude to risk and its management.
c) Awareness – a statement on corporate cultural and control environment.
d) Appetite – the level and nature of risk that is acceptable.
e) Architecture – risk management organisation, authority and communications.
f) Assessment – procedures for identification, analysis and evaluation.
g) Protocols – the means of communication, documents and reports.
h) Response / Treatment – mitigation and control mechanisms for implementation.
i) Responsibilities – Allocation of Roles and Responsibilities in context of above.
j) Training – mandatory training topics and priorities for awareness.
k) Monitoring – tasks, goals, benchmarking of risks.
l) Resources – appropriate and proportionate allocation.
m) Ongoing – Future activities to recognise and manage risk in next 12 months.

Where the ISMS is in place the Assurance Plan will provide linkages to it. The plan will be agreed before we move forward.