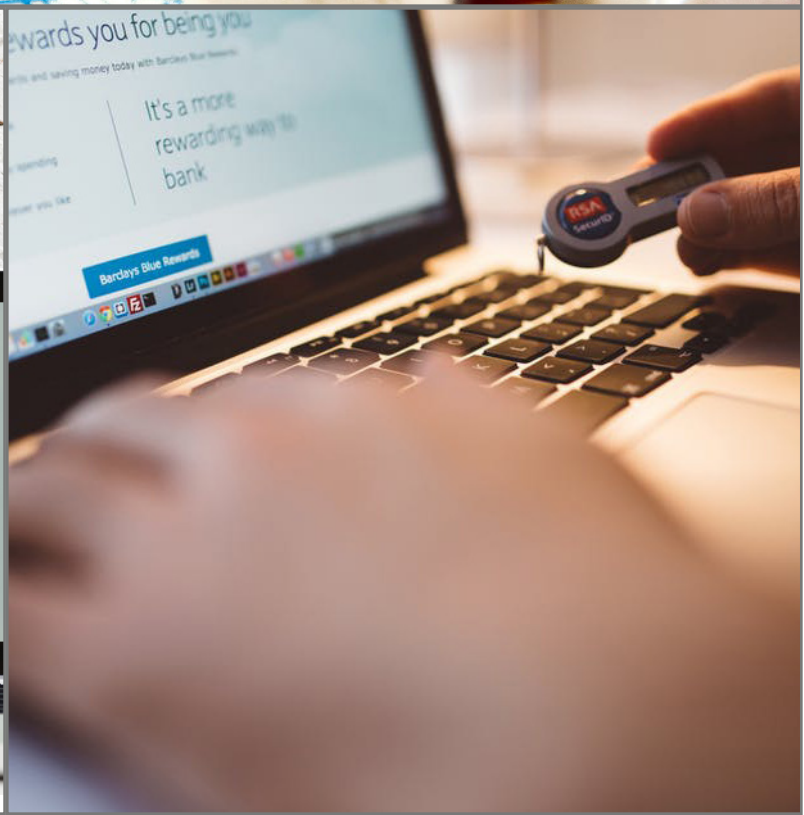
MONITORING & COMMUNICATIONS



Monitoring and Communications

The consultancy story does not need to stop after the assessment and recommendations. ISO 31000 has two further vital components. There needs to be ongoing communication with the stakeholders, the asset owners and IT delivery. There needs to be continuous monitoring of the outcome(s), the implementation of the recommendations. The system, the ISMS, in place must adhere to the principles laid down in the clauses of ISO 31000 (see Annex A) and monitor not only the effectiveness of controls but also those 'accepted and tolerate' residual risks to ensure any changes of circumstances warrant a change in the risk decision. For example the result of a risk assessment on a new system may be to allow it to go into operation with the caveat that a particular residual risk is too expensive to treat. This expense may be the cost of a hardware or software fix and as time goes by the cost may reduce. Monitoring the circumstances and context of a risk will allow effective management over time. Similarly, a low risk vulnerability of a legacy system exposed in an IT Health Check might become a high risk if a CERT notification shows a high probability of its exploitation. Such might warrant an upgrade, an advancement of patching or wholescale replacement. Additionally, new security systems or upgrades may come on the market which will allow effective defence for less resource (or more effective defence for the same resource etc.). Processes and expertise for such monitoring must be in place before the IL7 consultant leaves.

It is not always obvious that the IL7 consultant will be involved in the full life cycle. It may be the outcome is a plan for implementation and management of that implementation, an ISMS or integration into an existing management plan. The ISMS (or an integration/implementation plan) will be presented to the key business stakeholders and include processes for communication and monitoring as per ISO 31000, and in IS0 27001, Plan-Do-Check-Act process leading to continuous improvement. This would include the Risk Register, corrective or remedial action plans such as those following penetration tests, IT health checks, introducing new SEF and procedures.

The proposal for future activity will include terms of reference (and reporting structure/governance) for the Security Working Group for the system / project / delivery assessed. . IL7 will endeavour to take the best from each methodology to develop the picture of ongoing improvement. The consultants will utilise the clauses in ISO 31000 to build this into a risk management framework.