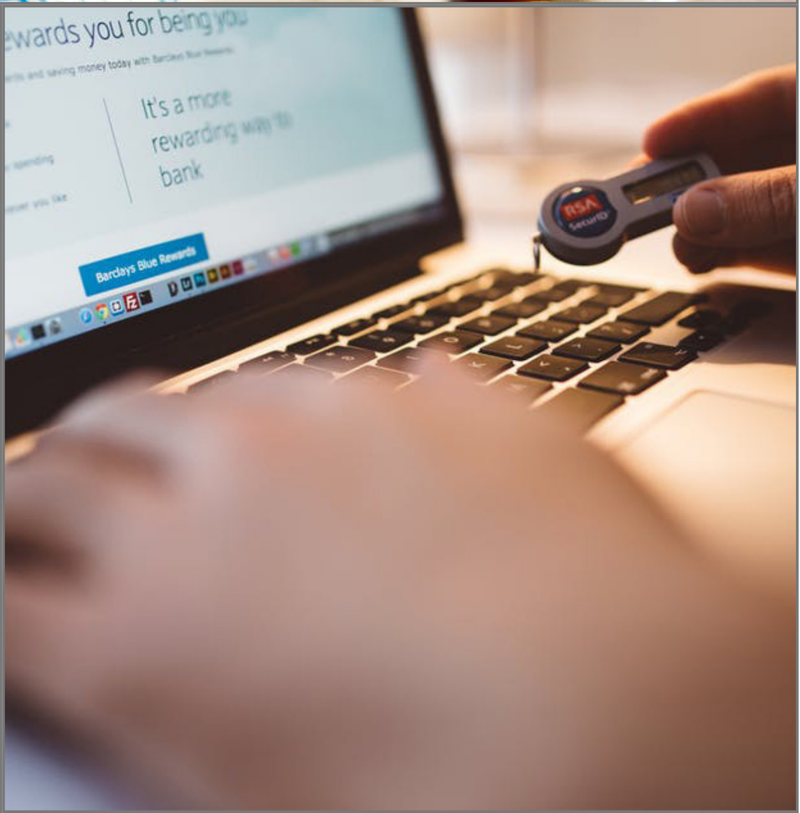
EVALUATION AND RISK



Evaluation and Risk Treatment

The purpose of the evaluation is to come up with risk treatment recommendations. These will be applicable and proportionate and be designed to eliminate or mitigate the risk. This might be to facilitate an endeavour (to exploit an opportunity) or to counter a revealed threat. Whatever methodology used to conduct the analysis the controls recommended will fall into the divisions of Procedural, Physical Personnel or Technical (P3T) or if required for easier understanding the Orange Book. Ref [11] can be used (Preventative, Corrective, Directive or Detective). Normally the controls will be taken from a list such as ISO/IEC 27002 and put into a business context. IL7 will continue to seek guidance from the NCSC documentation, new and legacy, and where applicable in the context of the customer, apply guidance from the Good Practice Guides.

IL7 consultants will keep up to date on new cyber threats and new solutions available to them where they can find technologies. Should technical controls, Security Enforcing Functionality (SEF) such as Firewalls or IPS be recommended, truly independent advice will be put forward with estimates of cost and through life value of investment. IL7 regularly review Common Criteria[1] products. While no longer confined to EAL certificated products and able to buy COTS, IL7 commonly review Gartner assessments (Magic quadrant etc.) and NSS Labs to advice customers on capability. In competitive tender exercises, technical specifications can be mapped onto operational requirements for SEF, taking care to include those features and capacities that mitigate the analysed and evaluated risks and not unnecessary extras. IL7 takes account of practical views such as the NCSC advice on SIEM not being a panacea and should protective monitoring and correlation be required it is just as important to have trained and qualified staff too.

When presenting findings of the assessment, the evaluated risks, the recommended treatments, experience demands that the consultant keeps things simple. IL7 use the simple equation – threats x vulnerabilities = risk. If either of the factors, vulnerabilities or threats, given the business and technical context, is zero, risk equals zero; there are no recommendations. The presentation will be honest, straightforward and talk in business terms of loss, consequence, and loss of opportunity. The consultant will present a security based, business case for taking action, for delivering the outcome. Where real costs exist comparisons can be made. IL7 will be able to discuss and analyse in the context of the 7R's and 4T's of risk management and evaluate and present findings in terms of:

- Recognition / identification.
- Ranking / evaluation.
- Responding:
    - Tolerate.
    - Treat.
    - Transfer.
    - Terminate.
- Resource controls.
- Reaction planning.
- Report and monitor.
- Review the risk management framework.

[1] https://www.commoncriteriaportal.org/

The decision taker will be made aware in real terms of costs for and against. They can make the final decision on whether to:

- Avoid or terminate the risk.
- Insure against or transfer the risk (this might be some sort of outsourcing or SaaS).
- Mitigation or reduction treatment of the risk.
- Acceptance or tolerance of the risk.

The last two bullets are often combined. The Risk Owner might tolerate a reduced or mitigated risk and may do so under the caveat that the mitigation circumstances are monitored and improved upon when possible. It is important to look at these residual risks. Some risks can be tolerated because they are reduced or managed. For example Anti-Virus might be seen as a control on the probability of being vulnerable to attack but there is always a threat of a Day-Zero attack, a remaining or residual risk. This may be mitigated in that the impact of such an attack is reduced through back up or disaster recovery plans. The caveat on acceptance may be that if a better or additional solution to AV becomes available (affordable) such as IPS, this is re-considered. The decision is largely one of cost or resource of various complimentary or alternative probability reducing controls (and the confidence in impact-mitigating factors) and the calculated risk.

Whatever the decision of the risk owner it is important that a record is kept. With most methodologies and standards this forms a Risk Register. Documentation will record why, how and by whom the decision was made and the evidence supporting this. The Register will include all proposed actions resultant on the decision and the owners of those actions.

It is important that time for resultant action is also logged as this will allow measurement and monitoring of effectiveness and escalation if not acceptable. IL7 contends that the IS1/2 RMADS in format demanded by both IS1/2 and JSP440, and when well written, provided the Risk Management story and although its author often did not become involved with the monitoring and assessment of the continuous process, provided an effective audit trail of why decisions were made. Along with the Risk Register it provided strong input into the following processes. IL7 will use its experience in producing RMADS to meet future customers' evidential and audit requirements.

It is important that the outcome is not one for options. If all the processes of the ISO 31000 framework have been properly worked through the conclusion will be corporately acceptable – the outcome is the result of a number of clear business decisions based on contextual evidence. The Risk Assessment process, the identification, the analysis and evaluation becomes a solution leading to an agreed resolution.