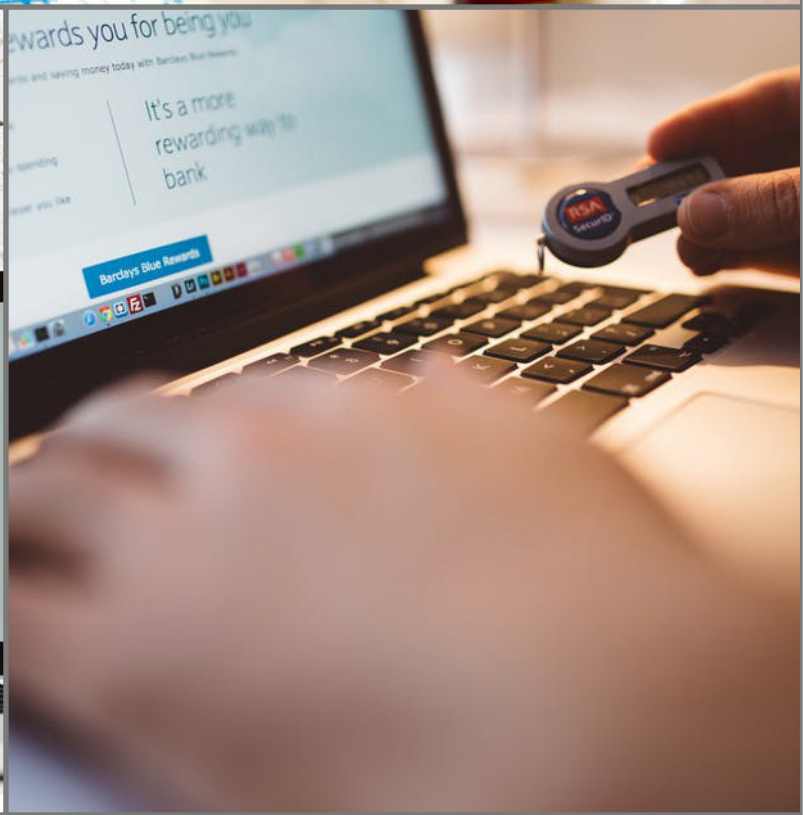
SUMMARY



Summary

Risk Assessments performed by IL7 will result in business outcomes based on contextualised risk and proportionate controls. They will address the importance of time in reaching their conclusions – context and time are vital to getting the right outcomes, producing the solutions that can then be monitored. They will understand the business reasoning – they will realise that risk evaluation is merely a cost benefit assessment and controls must show a return on investment. IL7 intend to improve the risk management delivered by IS1/2 by building on these standards within a framework that is relevant in other organisations and fits the ISO 31000 model.

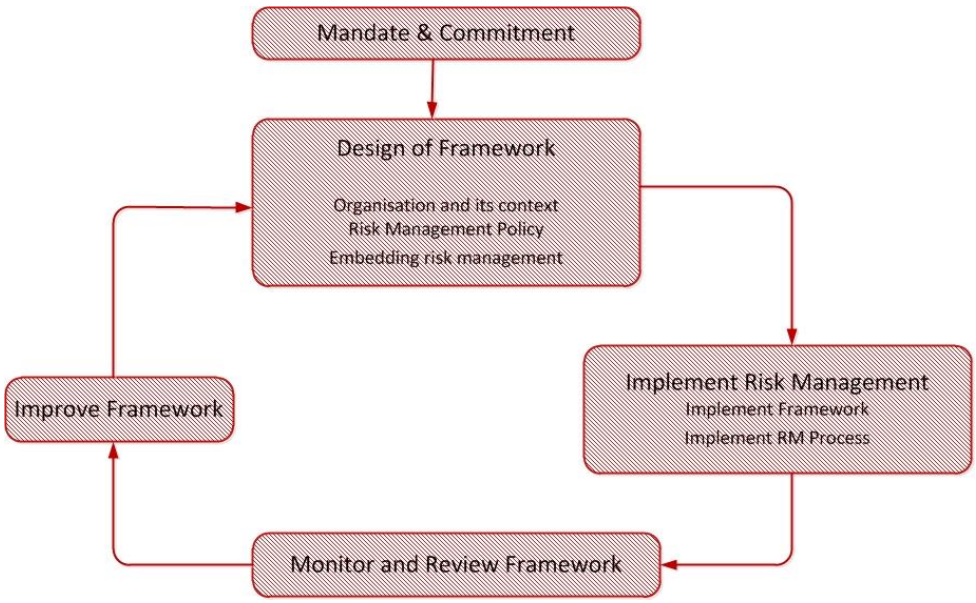


Figure 1 – Risk Management Framework

This is fully in line with the processes outlined in the IL7 Data Protection and Security Guidelines, a copy of which was sent to CESG in an earlier submission though designed exclusively to address the central government customer. IL7 will extend the framework into a cultural context where the framework itself is under review and subject to continuous improvement. We will mentor and consult with our customers so that we deliver this risk aware culture in a context that is relevant to them. In all, we will address the holistic risk picture, the risk of extant threats as well as the risk of embracing new technologies and exploring new markets. IL7's aim will facilitate opportunities in UK and embrace the NCSC mission

"to make the UK the safest place to live and do business online".

SOURCES

[1] National Audit Office report – Protecting Information Across Government. September 2016.
[2] ISO 31000:2009, Risk Management – Principles and Guidelines.
[3] BS 31100, Risk Management – Code of Practice and guidance for implementation of ISO 31000.
[4] ISO Guide 73, Risk Management – Vocabulary.
[5] ISO/IEC 27001, Information Technology – Security Techniques – Information Security Management Systems – Requirements.
[6] BS ISO/IEC 27005:2011 - Information Technology - Security techniques -Information Security Risk management.
[7] Cabinet Office Security Policy Framework (SPF) April 2014.
[8] HMG IA Standards Number 1 & 2, Information Risk Management, Issue 4.0, April 2012.
[9] HMG IA Standards Number 1 & 2, Supplement, Technical Risk Assessment and Risk Treatment, Issue 1.0, April 2012.
[10] HMG Government Security Classifications Annex Controls Framework April 2013.
[11] The Orange Book, HM Treasury, October 2004.
[12] Managing Risk the ISO 31000 Way – David Smith and Rob Politowski, bsi. 2013.
[13] Information Risk Management – A Practitioner's Guide – David Sutton, Bcs
[14] Fundamentals of Risk Management (3rd Ed) – Paul Hopkin, irm.
[15] Implementing Risk Management with ARM, Sword
[16] FAIR, ISO/IEC 27005 Cookbook, The Open Group, 2010
[17] Framework for Improving Cybersecurity, National Institute for Standards & Technology, 2014.
[18] A structured Approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000 (Airmic, Alarm, irm (download)).
[19] Overview of the General Data Protection Regulation (GDPR) Information Commissioner's Office, 2016.
[20] Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process, The Software Engineering Institute, May 2007.
[21] Vulnerability Management, on-line NCSC, September 2016.
[22] IL7 Data Protection and Security Guide, September 2016.
[23] Cisco – Cybersecurity as a Growth Advantage, 2016.
[24] NCSC – Common Cyber Attacks January 2016.
[25] NCSC 10 Steps to Cyber Security, updated 9 August 2016.
[26] CISSP Study Guide 4th Edition, October 2015.

NCSC Published

To date there are some 15 articles published in the NCSC risk management series.

https://www.ncsc.gov.uk/index/guidance?f[0]=field_topics%253Aname%3ARisk%20management