13

Policies

This chapter forms part of Stage 1 - Foundations in the Toolkit Route map.

Every organisation requires a top level policy for information security which must define clear lines of responsibility for delivery and risk ownership. The policy and associated responsibility should be developed as a result of the governance arrangements in place within the organisation (see Chapter 2, Information security governance), and in particular the policy must be approved by the highest body in the organisation's governance framework.

Managing information security risks should be part of an organisation's overall risk management strategy, and the formulation of information security policy should form part of that strategy. In organisations with a low maturity in terms of risk management, a governance structure may need to be developed specifically for the purpose of writing the information security policy and the use of a RACI matrix (Responsible, Accountable, Consulted, and Informed) may help to establish it.

The supplementary volume to this publication which, at the time of writing, is still in production, builds on the third edition of UCISA's Information Security Toolkit published in 2007 (the predecessor of this publication) and will include revised policies to comply with ISO 27001:2013.

Summary

- The information security policy should not stand alone; it should be part of an organisation's risk management strategy and must be approved by the highest governance body in the organisation
- The organisation's policy for information security defines responsibility for delivery and risk ownership

Resources

Template for a generic policy

Reading list

No items.