National Cyber Security Centre

Managing your information risk

Using technology to deliver business attracts risk. Applying the following principles will help your organisation understand how to approach, assess and manage information and technology risks.

1

Understand the business context

Provide a context in which risk management and assessment is to be conducted. This should outline what your organisation is trying to achieve, the business assets involved, legal and regulatory requirements and third party risk management/contractual considerations. This context must summarise the risks you're prepared (or not prepared) to take and the governance structure in place to support risk management decision taking.

2

Decide on the risk management approach

You must understand and communicate the risk management approach your business is going to take. This provides confidence that the technology and information used is secure. Risk assessment and management requires technical, security and business skills. Choosing the wrong approach can be costly in terms of resource and security compromise.

3

Understand key risk components

Risk assessments have inputs and outputs. Consider fundamental inputs of your risk assessment (e.g. threat, vulnerability and impact). Regardless of risk assessment methods used, the inputs and outputs should be understandable in the context of your organisation.

4

Understand what risks exist

The risk assessment method must be applied in the context of what your organisation is trying to accomplish. You should know which risk management decisions the assessment will inform, who's responsible for making them and the level of detail required. Prioritise the outputs from the assessments to make informed risk management decisions.

5

Communicate risk consistently

Irrespective of your approach to assessing risks, capture the outcome in a way that can be used to inform business decision making. Output from risk assessment and management activities may need to be communicated to interested third parties.

6

Make informed risk management decisions

Make objective decisions about what needs to be done to manage identified risks, informed by subject matter expertise, information and evidence.