Risk Reviews

# Risk Reviews

Information and the supporting processes, systems and networks are important and valuable Ministry of Justice (MoJ) assets. They are central to enabling the MoJ to perform its functions and provide services to the public, the legal professions, and other government departments and organisations.

Confidentiality, integrity and availability of information is essential to maintain the MoJ's ability to provide efficient and effective services, maintain compliance with legal and regulatory requirements, and maintain its and the Government's reputation.

The MoJ and its information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, sabotage, vandalism, fire and flood. Sources of damage such as computer viruses, computer hacking and denial of service attacks have become more common, more ambitious and increasingly sophisticated.

The MoJ's dependence on its information systems and services means that there is always a possibility of technology-enabled security threats. Connections between the MoJ's computer networks and public and other private networks, and sharing of information resources, further increase the difficulty of achieving and maintaining control.

It is essential that the MoJ identify its information security requirements. There are three main sources of these requirements.

* The legal, statutory, regulatory and contractual requirements that the MoJ, its partners, contractors and service providers have to satisfy.
* The principles, objectives and requirements for information processing that the MoJ and Government have developed to support their operations, for example the protective marking system and government baseline security standards.
* Assessed risks to the MoJ. Through risk assessment, threats to assets are identified, the potential business impacts of these threats are estimated, and the vulnerability to and likelihood of occurrence of the threats are evaluated.

## Assessing information security risk

Security requirements are identified by a methodical assessment of security risks. Expenditure on security controls needs to be balanced against the business harm likely to result from security failures. Risk assessment is systematic consideration of:

* The business harm (the 'impact') which is likely to result from a security failure, taking into account the potential consequences of a loss of confidentiality, integrity or availability of the information and other assets.
* The realistic likelihood of such a failure occurring in the light of the threats to and vulnerabilities of the system, and the controls currently implemented.

## Managing information security risks

The results of the risk assessment are identified risks and risk severities. These help guide and determine the appropriate management action, and priorities for managing information security risks. Risks with a high severity level would justify the expenditure of more resources to control them than risks with a low severity level. Risk Management involves identification, selection and implementation of justified security and contingency 'countermeasures' to reduce risks to an acceptable level.

Countermeasures can act in different ways such as:

* Reducing the likelihood of attacks or incidents occurring.
* Reducing the system's vulnerability.
* Reducing the impact of an attack or incident should it occur.
* Detecting the occurrence of attacks or incidents.
* Facilitating recovery from an attack or incident.

Risk management requires a judgement about what is an acceptable level of risk. Although this is a business decision, it does require a thorough understanding of the nature of the risk and the effectiveness of the countermeasures implemented to manage the risk. For some systems or scenarios, specialist advice might be needed.

When taking risk management decisions, consideration must be given to the full implications of the decisions taken. Failure to implement some countermeasures might breach legal or regulatory requirements. This is unlikely to be an acceptable risk management decision. Failure to meet other countermeasures might breach Government information security standards; as a consequence it might not be possible to link the MoJ system with other systems. This might limit the usefulness of the MoJ system.

Consideration must also be given to what are tolerable financial losses, political sensitivities and adverse publicity. The cumulative effect of accepting high levels of risk should also be taken into account.

## Information security in projects

Information security controls are considerably cheaper and more effective if incorporated at the system requirements specification and design stage. Information risk assessments must be part of the project process.

## Ongoing information security risk management

Effective risk management does not end once a risk assessment has been done and the required countermeasures implemented. Checks need to be carried out to ensure that the countermeasures are being applied effectively. It is also important to carry out periodic reviews of security risks and implemented controls to:

* Take account of changes to business requirements and priorities.
* Consider new threats and vulnerabilities.
* Confirm that controls remain effective and appropriate.

## The role of security in risk assessment and risk management

The MoJ security team can provide help in all areas of security risk management for systems. Examples include:

* Advice on risk assessments.
* Help with carrying out risk assessments.
* Assist with the risk management decision process.
* Help with creating and managing documentation compliant with MoJ standards.
* Assisting with mandatory Government risk assessments.
* Advice on compliance checking.

## Contact details

For any further questions relating to security, contact: [security@digital.justice.gov.uk](mailto:security@digital.justice.gov.uk), or for security advice, contact the Cyber Assistance Team [CyberConsultancy@digital.justice.gov.uk](mailto:CyberConsultancy@digital.justice.gov.uk).

## Feedback

If you have any questions or comments about this guidance, such as suggestions for improvements, please contact: [itpolicycontent@digital.justice.gov.uk](mailto:itpolicycontent@digital.justice.gov.uk).