Money Advice Information Security Risk Management Policy

Version 1.1

Version **1.1**

Change History

VERSION NUMBER	AUTHOR	DATE	REASON FOR ISSUE	CHANGES
1.0	Sohail Farooqui	8/6/2011	1st Draft	
1.1	Satheesh Vattem	10/6/2015	Add templates to appendix	

Table of Contents

1. Introduction

The Money Advice Security Risk Management Policy presents a systematic approach for the process of analysing the security risks to the information computer systems and applications within the Money Advice organisation, and implementing steps to prevent these risks from occurring. At a high level, the risk management policy is the process of identifying risk, assessing risk and taking steps to reduce risk to an acceptable level.

The Money Advice Security Risk Management Policy can be broken down into 3 main sections

- Risk identification and assessment
- Risk mitigation
- On-going evaluation and assessment

Risk identification and assessment includes identification and evaluation of risks and risk impacts, and recommendation of risk-reducing measures. Risk mitigation refers to prioritising, implementing, and maintaining the appropriate risk-reducing measures recommended from the risk assessment process. The on-going evaluation and assessment process outlines the keys for implementing a successful risk management policy.

Risk management is a management responsibility but a successful risk management policy implementation requires all employees to buy into it. All Money Advice employees need to be aware of the security risks which have been identified, and the steps that need to be taken to prevent these risks from occurring

2. Risk Identification and Assessment

Before risk can be identified, it is necessary to carry out a full inventory of all security assets.

For the purpose of the Money Advice risk management policy, a security asset is defined as any piece of data, any device, or any other component of the environment that supports information-related activities.

The list of security assets should be entered in the Security Asset Register (see appendix). The Security Asset Register should record such information as the type of asset, its interconnections, who has responsibility for it and the criticality of the asset (how important is it to the organisation)

2.1 Identify Threats and vulnerabilities

To determine the likelihood of a future adverse event, threats to an IT system must be analysed in conjunction with the potential vulnerabilities and the controls in place for the IT system. A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability. A vulnerability is a weakness that can be accidentally triggered or intentionally exploited.

The Security Asset Register should be examined and any threats or vulnerabilities which are identified should be entered into the Security Risk Register (see appendix).

2.2 Impacts, Category and Prioritisation

When risks have been identified, the next step is to assign a risk rating to each risk. The risk rating is calculated by assessing the potential impact on the company if the risk was to be realised, and the probability of the risk occurring.

The adverse impact of a security risk occurring can be described in terms of loss or degradation of any, or a combination of any, of the following three security goals:

- Integrity
- Availability
- Confidentiality.

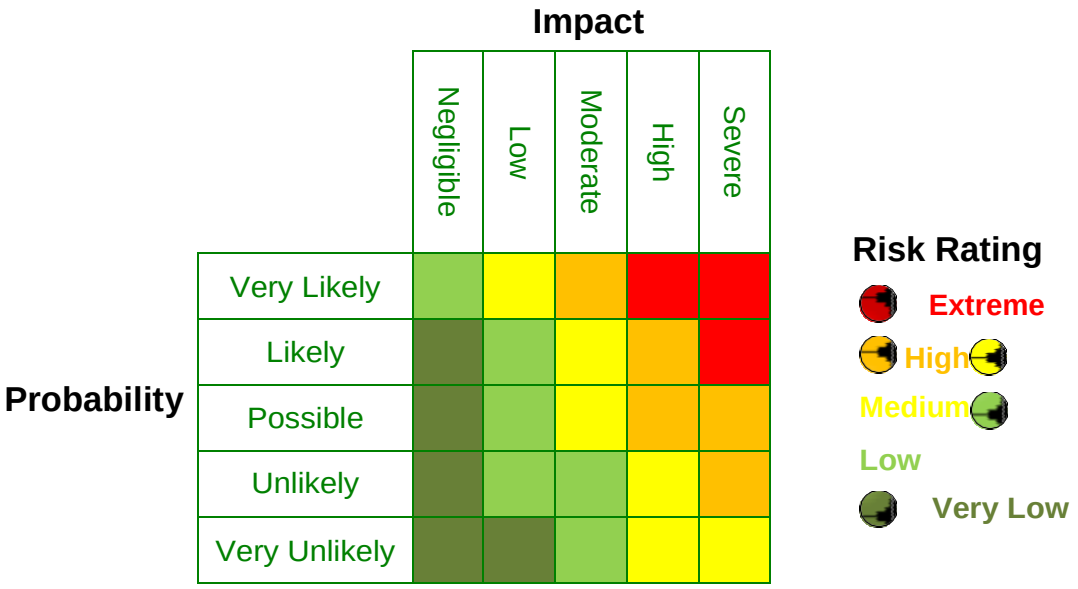
Loss of Integrity: System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorised changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the assurance of an IT system.

Loss of Availability: If a mission-critical IT system is unavailable to its end users, the organisation's mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users' performance of their functions in supporting the organisation's mission.

Loss of Confidentiality: System and data confidentiality refers to the protection of information from unauthorised disclosure. The impact of unauthorised disclosure of confidential information can range from the jeopardising of national security to the disclosure of Privacy Act data. Unauthorised, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organisation.

Using the Risk Matrix, one of these 5 ratings should then be assigned to each risk in the register:

- Extreme
- High
- Medium
- Low
- Very Low



The identified risks should be prioritised based on their risk rating. Any risk which is identified as **Extreme** should be given immediate attention

2.3 Safeguard Recommendations

Once the risk rating is determined for each threat/vulnerability, safeguards should be identified for the medium to extreme level risks.

When a recommended safeguard is implemented, the risk should then be re-evaluated to determine the remaining risk, or residual risk rating.

The safeguard recommendations which are identified will in turn be evaluated, prioritised, and implemented as part of the risk mitigation process. It should be noted that not all possible recommended controls can be implemented to reduce loss. In addition, the operational impact (e.g., effect on system performance) and feasibility (e.g., technical requirements, user acceptance) of introducing the recommended option should be evaluated carefully during the risk mitigation phase.

3. Risk Mitigation

The risk mitigation phase involves prioritising, evaluating, and implementing the appropriate risk-reducing safeguards recommended from the risk identification and assessment phase.

Risk mitigation can be achieved through any of the following risk mitigation options:
• **Risk Assumption.** To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level
• **Risk Avoidance.** To avoid the risk by eliminating the risk cause and/or consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified)
• **Risk Limitation.** To limit the risk by implementing controls that minimise the adverse impact of a threat's exercising a vulnerability (e.g., use of supporting, preventive, detective controls)
• **Risk Planning.** To manage risk by developing a risk mitigation plan that prioritises, implements, and maintains controls
• **Research and Acknowledgment.** To lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability
• **Risk Transference.** To transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

3.1 Security controls

In implementing recommended safeguards or controls to mitigate risk, you should consider technical, management, and operational security controls, or a combination of such controls, to maximise the effectiveness of controls for IT systems within Money Advice. Security controls, when used appropriately, can prevent, limit, or deter threat-source damage to a company's reputation

The control recommendation process will involve choosing among a combination of

- technical
- management
- and operational

controls for improving the company's security position.

3.1.1 Technical

The technical controls can be sub divided into the following categories:

1) Support
2) Prevent
3) Detect and Recover

Supporting Technical Controls

- Identification. This control provides the ability to uniquely identify users, processes and information resources.
- Cryptographic Key Management. Cryptographic keys must be securely managed when cryptographic functions are implemented in various other controls. Cryptographic key management includes key generation, distribution, storage, and maintenance.
- Security Administration. The security features of an IT system must be configured (e.g., enabled or disabled) to meet the needs of a specific installation and to account for changes

in the operational environment. System security can be built into operating system security or the application.

- System Protections. Underlying a system's various security functional capabilities is a base of confidence in the technical implementation. This represents the quality of the implementation from the perspective both of the design processes used and of the manner in which the implementation was accomplished. Some examples of system protections are residual information protection (also known as object reuse), least privilege (or "need to know"), process separation, modularity, layering, and minimisation of what needs to be trusted.

Preventive Technical Controls

These controls, which can inhibit attempts to violate security policy, include the following:

- **Authentication.** The authentication control provides the means of verifying the identity of a subject to ensure that a claimed identity is valid. Authentication mechanisms include passwords, personal identification numbers, or PINs, and emerging authentication technology that provides strong authentication
- **Authorisation**. The authorisation control enables specification and subsequent management of the allowed actions for a given system (e.g., the information owner or the database administrator determines who can update a shared file accessed by a group of online users).
- **Access Control Enforcement.** Data integrity and confidentiality are enforced by access controls. When the subject requesting access has been authorised to access particular processes, it is necessary to enforce the defined security policy. These policy-based controls are enforced via access control mechanisms distributed throughout the system. The effectiveness and the strength of access control depend on the correctness of the access control decisions (e.g., how the security rules are configured) and the strength of access control enforcement (e.g., the design of software or hardware security).
- **Nonrepudiation**. System accountability depends on the ability to ensure that senders cannot deny sending information and that receivers cannot deny receiving it. Nonrepudiation spans both prevention and detection. It has been placed in the prevention category in this guide because the mechanisms implemented prevent the successful repudiation of an action (e.g., the digital certificate that contains the owner's private key is known only to the owner). As a result, this control is typically applied at the point of transmission or reception.
- **Protected Communications**. In a distributed system, the ability to accomplish security objectives is highly dependent on trustworthy communications. The protected communications control ensures the integrity, availability, and confidentiality of sensitive and critical information while it is in transit. Protected communications use data encryption methods (e.g., virtual private network, Internet
- **Protocol Security** [IPSEC] Protocol), and deployment of cryptographic technologies to minimise network threats such as replay, interception, packet sniffing, wiretapping, or eavesdropping.

Detection and Recovery Technical controls

- **Audit.** The auditing of security-relevant events and the monitoring and tracking of system abnormalities are key elements in the after-the-fact detection of, and recovery from, security breaches.
- **Intrusion Detection and Containment.** It is essential to detect security breaches so that a response can occur in a timely manner. It is also of little use to detect a security breach if no

effective response can be initiated. The intrusion detection and containment control provides these two capabilities.

- **Proof of Wholeness.** The proof-of-wholeness control (e.g., system integrity tool) analyses system integrity and irregularities and identifies exposures and potential threats. This control does not prevent violations of security policy but detects violations and helps determine the type of corrective action needed.
- **Virus Detection and Eradication.** Virus detection and eradication software installed on servers and user workstations detects, identifies, and removes software viruses to ensure system and data integrity.

3.1.2 Management

The management controls can be sub divided into the following categories:

1) Preventative
2) Detection
3) Recovery

Preventive Management Security Controls

These controls include the following:

- Assign security responsibility to ensure that adequate security is provided for the mission-critical IT systems
- Develop and maintain system security plans to document current controls and address planned controls for IT systems in support of the company's policy
- Implement personnel security controls, including separation of duties, least privilege, and user computer access registration and termination
- Conduct security awareness and technical training to ensure that end users and system users are aware of the rules of behaviour and their responsibilities in protecting the company's reputation

Detection Management Security Controls

- Implement personnel security controls, including personnel clearance, background investigations, rotation of duties
- Conduct periodic review of security controls to ensure that the controls are effective
- Perform periodic system audits
- Conduct on-going risk management to assess and mitigate risk
- Authorise IT systems to address and accept residual risk.

Recovery Management Security Controls

- Provide continuity of support and develop, test, and maintain the continuity of operations plan to provide for business resumption and ensure continuity of operations during emergencies or disasters
- Establish an incident response capability to prepare for, recognise, report, and respond to the incident and return the IT system to operational status.

3.1.3 Operational

The operational controls can be sub divided into the following categories:

1) Preventative

2) Detection

Preventive Operational Security Controls
These controls include the following:

- Control data media access and disposal (e.g., physical access control, etc)
- Limit external data distribution (e.g., use of labelling)
- Control software viruses
- Safeguard physical facility (company offices)
- Provide backup capability
- Establish off-site storage procedures and security
- Protect laptops, PCs and workstations
- Protect IT assets from fire damage
- Provide emergency power source
- Control the humidity and temperature of the computing facility

Detection Operational Security Controls

- Provide physical security as appropriate (e.g., use of motion detectors, closed-circuit television monitoring, sensors and alarms)
- Ensure environmental security (e.g., use of smoke and fire detectors, sensors and alarms).

4. On-Going Evaluation and Assessment

In Money Advice, the environment is often amended or updated, through software upgrades etc. In addition, personnel changes will occur and security policies are likely to change over time.

These changes mean that new risks will surface and risks previously mitigated may again become a concern. Thus, the risk management process should be on-going and always evolving. Therefore it is essential that Money Advice operate an on-going risk evaluation and assessment strategy

4.1 Frequency

A full company wide security risk assessment should take place every 12-18 months.

Periodic assessments should take place whenever there is a change in the network configuration, when new hardware is being implemented, when new software releases take place or whenever the Information Security Manager (ISM) sees fit.

4.2 Responsibility

The person responsible for the implementation of the information security risk management policy in Money Advice is the ISM. At this current time the ISM is Sohail Farooqui

5. Appendix

5.1 Security Asset Register

Name	Type	Make/Model	Interconnections	Person Responsible	Criticality Level

5.2 Information Security Risk Register

Security Asset	Risk Description	Potential Impact	Risk Rating Before Mitigation	Person Responsible	Mitigation Description (if applicable)	Risk Rating After Mitigation