IFSA Guidance Note No. 22.00

IT Fraud and Security Guidelines

October 2007

Main features of this Guidance Note are:

- To provide a starting position to assist IFSA members in reviewing and assessing their Fraud and Security position relating to Information Technology ("IT Fraud and Security"), particularly as they impact both on consumers of financial products and on IFSA members.
- To encourage good practice in respect of IT Fraud and Security by identifing the key principles that can be used to address IT Fraud and Security concerns.

IFSA Guidance Note No. 22.00

Table of Contents

	Section	Page
Title	**1**	**3**
Guidance Note and Commentary	**2**	**3**
Date of Issue	**3**	**3**
Statement of Purpose	**4**	**3**
Scope	**5**	**3**
Glossary	**6**	**4**
IT Security and Fraud – Policy & Principles	**7**	**4**
IT Asset Management	**8**	**6**
Enhance Human Resources Security	**9**	**7**
Systems and Network Operations Management	**10**	**8**
Access Controls and Ongoing Compliance	**11**	**8**
Early Planning from System Acquisition and Development Through to Maintenance	**12**	**9**
IT Security / Fraud Incident Management	**13**	**10**
Consumer IT Security & Fraud Awareness	**14**	**11**
Legal Compliance	**15**	**11**

IFSA Guidance Note No. 22.00

1 TITLE

1.1 This Guidance Notes may be cited as IFSA Guidance Note No. 22.00 "IT Fraud and Security Guidelines" (the "Guidelines").

2 GUIDANCE NOTE AND COMMENTARY

2.1 The Guidelines provide a starting position to assist IFSA members to review and assess their Fraud and Security position relating to Information Technology ("IT Fraud and Security"), particularly as they impact both on consumers of financial products and on IFSA members.

2.2 The Guidelines are intended to encourage good practice in respect of IT Fraud and Security. To achieve this, the Guidelines identify the key principles that can be used to address IT Fraud and Security concerns. These principles are not exhaustive, they have been identified with reference to existing industry standards and other papers (see the References section of this Guidelines), using a risk based approach and have been subject to broad member consultation.

2.3 The Guidelines should not be read as representing the particular circumstances of individual organisations or group. Compliance with this the Guidelines is voluntary but encouraged.

3 DATE OF ISSUE

3.1 30th October 2007

4 STATEMENT OF PURPOSE

4.1 The wealth management industry (comprising funds management, superannuation/ pensions, life insurance and investment industries) is a growing industry and a cornerstone to the financial well-being of many Australians. It is also an industry that is profoundly and increasingly reliant on information technology for delivery of services to consumers of financial products.

4.2 For the reasons above, it is important that we develop and sustain a capability that effectively addresses the risks in the areas of IT Fraud and Security in order to preserve and enhance consumer confidence in our industry. The purpose of the Guidelines is to provide a framework to IFSA members for addressing the fraud and security risks associated with their IT infrastructure.

5 SCOPE

5.1 The Guidelines address one aspect of fraud and security that IFSA members should have active regard to. The matters excluded from consideration are either already addressed or is subject to a separate process. It is with this in mind that the following matters have been excluded from the scope of the Guidelines:

a. Non-IT related fraud and security concerns. Some of the principles set out, however, will have broad application.

b. IT Fraud and Security concerns relating to advisers, except to say that advisers should be made aware of some of the risks. See Section 14.

c. Matters relating to Anti-Money Laundering and terrorism financing. The focus of the Guidelines is on consumers and on IFSA members.

d. Security risks relating to business continuity. This is already addressed in IFSA Standard No. 5.00 "Operational Capability Standard".

6 GLOSSARY

6.1 In this Guidelines:

- *"IT Fraud"* is defined as a benefit unlawfully obtained by deception or other means via the interaction between human activities and IT infrastructure that impact on an organisation. IT fraud can be considered a subset of IT security, since the effectiveness of an organisation's IT security controls directly affect its potential exposure to fraud.

- *"IT security"* refers to the state of an organisation's IT infrastructure and its susceptibility to unauthorised access or attack from both internal and external sources.

- *"IT infrastructure"* can encompass hardware, software, confidential data and intellectual property. However, the Guidelines will focus primarily on IT Fraud and Security concerns that impact on consumers and on IFSA members.

- *"Malicious and Mobile Code"* means a programme running within a system or network that is not intended by the owner of the system or network, eg. a virus.

7 IT SECURITY AND FRAUD – POLICY & PRINCIPLES

7.1 The implementation of a given fraud and security management programme should start with an IT and Information Security Policy ("Policy"). This policy should be supported and implemented by senior management who have responsibility for adequately addressing the risks of IT Fraud and Security. The Policy also gives management direction on how to address these risks.

7.2 The Policy can be in one document or several documents or part of some larger document(s), the form of which is a matter of IFSA members, so long as the Policy meets the objective of being clearly documented. The IT and Information Security Policy should clearly set out:

a. Management commitment to information security as a key organisational priority.

b. The goals of the policy.

c. The key principles that the organisation will observe and adopt to ensure that IT Fraud and Security risks may be adequately addressed.

d. The controls that will be adopted to give effect to the principles.

7.3 The table below outlines the key principles that should form part of any IT and Information Security Policy in any IFSA member initiatives to prevent IT fraud and maintaining data security.

7.4 The remainder of this Guideline sets out the key considerations, including an overview of the risks involved, for determining the control requirements that would be necessary to give effect

to the principles.

7.5 Table 2 - IT Policy Fraud and Security Principles:

Principles	Guidelines	Sections Reference
IT assets management.	IFSA members should identify their IT and information assets, and implement appropriate protection over these assets based on their sensitivity and criticality classification.	8
Enhance human resources security.	IFSA members should ensure that sensitive responsibilities are carried out by well trained personnel with appropriate security clearance.	9
System and network operations management.	IFSA members should ensure the correct and secure operation of the network and systems that support business processes.	10
Access control and ongoing monitoring.	IFSA members should implement and document appropriate mechanisms for access controls, as well as detective controls to identify breaches of policy or practice. Access to critical and sensitive assets must be aligned with the roles and responsibilities of users	11
Early planning from system acquisition and development through to maintenance.	IFSA members should consider and implement appropriate levels of security when planning for and implementing new systems acquisitions and/or making changes to existing systems.	12
Adequate incident management.	IFSA members should ensure that information security events are identified and communicated in a manner that allows timely corrective actions to be taken, whilst complying with an over-arching Incident & Breach reporting guidelines and regulations.	13
Consumer awareness of IT security and fraud.	IFSA members should have adequate arrangements to ensure that customers, advisers, agents and relevant third parties are aware of the risks involved in electronic communication in the context of the business process that deals with their needs.	14

Principles	Guidelines	Sections Reference
Legal compliance.	IFSA members should understand and meet all relevant and applicable legal, statutory, regulatory and contractual IT security requirements.	15

7.6 In addition to implementing controls based around the principles above, organisations should also consider how they will periodically determine that the controls are designed appropriately and operating effectively. This 'assurance' approach to IT control management is consistent with the expectations from compliance regimes such as Sarbanes Oxley and PCI (see References section below).

7.7 Moreover, reliance on the Guidelines should not in any way derogate from the need for IFSA members to ensure they undertake appropriate identification, assessment, mitigation and monitoring of the risks in their organisation. The principles and guidelines above are not exhaustive.

8 IT ASSET MANAGEMENT

8.1 IFSA members should identify their IT and information assets, and implement appropriate protection over these assets based on their sensitivity and criticality classification.

8.2 Asset management covers physical assets (e.g. hardware) and logical assets (e.g. software stored on a computer). Controls should be implemented within the organisation to protect these assets to minimise any potential for fraud.

8.3 *What are the risk(s) being addressed?*

- A fundamental step in any risk management framework. There needs to be a rigorous process to enable an organisation to become aware of its IT assets' exposure and vulnerability to the risks of IT fraud and security, and to ensure appropriate ownership of these assets so that the risks can be effectively managed.

8.4 *Control Requirements:*

i. Formally defined information classification policy that allows management to classify the assets should include classification guidelines and the baseline controls over the storage, transmission, transportation and removal of assets within each classification level.

ii. An asset register should be kept detailing the hardware, software and data assets, and their information classification level.

iii. All assets deemed critical to the organisation should have an assigned owner. The owner should be a fulltime employee.

iv. The owner is responsible for decisions taken to protect the assets, including access within and outside the organisation and availability of the information, in order to fulfil IFSA members duties and obligations to consumers and other stakeholders.

v. The owner may delegate authority to other permanent members of staff within the organisation to fulfil the owner's responsibilities.

vi. Controls should be implemented to safeguard the asset commensurate with the value and classification of the asset with respect to the IFSA member and to consumers.

vii. Control processes should be in place to manage information media sent offsite (eg. Tapes, CD/DVD, USB flash drives, etc.).

viii. Where IT assets are to be disposed, consideration should be given to sensitive information contained within that are no longer needed to prevent inappropriate access. For example, destruction of hard drives when disposing of computers or other media to prevent external parties obtaining copies of private information about consumers.

ix. Requirements for the retention of organisational records (important records within the organisation that must be protected against loss, destruction and falsification) should be addressed by the organisation based on statutory and regulatory requirements. See section 15.

9 ENHANCE HUMAN RESOURCES SECURITY

9.1 IFSA members should ensure that sensitive responsibilities are carried out by well trained personnel with appropriate security vetting.

9.2 Human resources security relates to the hiring, induction and termination procedures for staff as well as the implementation of an information security awareness program.

9.3 *What are the risk(s) being addressed?*

- Theft, fraud and misuse of facilities are caused by humans, both within and external to an organisation.
- Measures should be in place to ensure good character, adequate level of competence, consciousness of IT Fraud and Security issues, and consequences of breaches.

9.4 *Control Requirements:*

i. Conduct appropriate security screening including personal and past employer reference checks to be completed prior to any recruitment offers to new staff. Give appropriate classifications to nominated sensitive positions that will require background and criminal checks.

ii. IFSA members should have published and make readily available to staff policies about acceptable computer use and information security.

iii. Ensure access to all IT infrastructure are revoked upon employment termination. For example, all keys and access devices to be returned and all access rights to computer systems revoked and signed off by appropriate authority.

iv. Ensure compliance with all fraud and security policies is a key term of employment for all staff.

v. Ensure all new staff are given induction training specifically on information security.

vi. Formally define security responsibility and agreement for employees, contractors and third party users that have access to the IT and information assets.

vii. A formal disciplinary process for employees who have committed a security breach. See section 13.

10 SYSTEMS AND NETWORK OPERATIONS MANAGEMENT

10.1 IFSA members should ensure the correct and secure operation of the network and systems that support business processes.

10.2 *What are the risk(s) being addressed?*

- There are certain vulnerabilities in any system and network operations where IT fraud and security can arise and should be addressed. They typically involve:
    - Points of human interactions;
    - Interactions with an organisation's IT infrastructure; and
    - Interactions with third party providers.

10.3 *Control Requirements:*

i. Operating procedures and responsibilities should be documented and kept up to date. They should address:
    - segregation of duties;
    - system start-ups and shutdown;
    - appropriate backup regimes – should be implemented and regularly tested to ensure that the integrity and availability of information is well protected.

ii. Information processing facility capacity and adequacy performance should be monitored to ensure that business requirements can be supported. Accordingly:
    - security controls should include appropriate protection measures to ensure that these facilities are protected from external threats. For example:
        - → Information exchange and communication protocols should protect information in transit; and
        - → Electronic commerce controls should be sufficiently robust to protect transactions and should be based on fraud and transaction risks;
    - controls should include protection against malicious and mobile code.

iii. Processing outsourced to third parties should be subject to similar controls as those performed in-house, including definition of service levels and monitoring.

iv. Implement monitoring procedures to identify and address system operation issues in a timely manner.

11 ACCESS CONTROLS AND ONGOING COMPLIANCE

11.1 IFSA members should consider and document appropriate mechanisms for access controls. Access controls involve exercising a directing or restraining influence over the behaviour, use, and content of a system. For instance, specifying what users can do, what resources they can

access, and what operations they can perform on an IT system. Good access control should be designed to ensure confidentiality, where required, and integrity of an organisation's information assets.

11.2 Members should also consider implementing activity tracking facilities for the use of key systems or transactions. Forensic information of this nature should be captured in a manner that makes it legally robust – i.e. confidential, not vulnerable to compromise, high levels of integrity and a retention period that matches corporate policy.

11.3 *What are the risk(s) being addressed?*

- Access controls is a simple and effective way of deterring fraud and security threats both internally and externally.
- Users affected by these controls can be both internal and external to an organisation, and can constitute staff, service providers and customers.

11.4 *Control Requirements:*

i. Ensure physical and logical access to systems, transactions and data is restricted and managed according to a user's role.

ii. Ensure IT staff access is managed particularly to powerful utilities and any production environments.

iii. Implement strong authentication controls and educate users on the need to keep these secured.

iv. Controls to allow the secure use of mobile computing and portable storage devices are in place and effective.

v. Ensure both user and administrative activity is recorded in a manner that can be used for investigations and forensics purposes.

vi. Maintain, protect and review audit trails on a regular basis for inappropriate access.

12 EARLY PLANNING FROM SYSTEM ACQUISITION AND DEVELOMENT THROUGH TO MAINTENANCE

12.1 IFSA members should consider and implement appropriate levels of security when planning for and implementing new systems acquisitions and/or making changes to existing systems.

12.2 *What are the risk(s) being addressed?*

- Embedding measures to prevent IT Fraud and Security early in the systems design and planning process ensures a proactive and preventative approach to risk management. This is more effective than a purely reactive one given the costs that could be incurred as a result of major fraud incidents and security breaches.

12.3 *Control Requirements:*

i. Identify all security requirements prior to system design or acquisition.

ii. Implement proper change control over the production environment.

iii. Strict access control over the system source code and design documentation to prevent unauthorised disclosure and changes.

iv. Identification, communication and implementation of secure development practices.

v. Appropriate controls included in information systems and applications to ensure the correct processing of information including validation of input data, internal processing and output data.

vi. Protection of sensitive information with appropriate cryptographic controls when required.

vii. Access control over system files and source code in segregated environments to prevent unauthorised changes. Data used for development and testing should be appropriately sanitised.

viii. Ensure separation of production and development environments. That is, developers should not have business operation roles and should be restricted from the production environment.

ix. Formal asset acquisition and removal procedures.

13 IT SECURITY / FRAUD INCIDENT MANAGEMENT

13.1 IFSA members should ensure that incidents involving IT security failures and fraud are communicated in a manner that allows timely corrective actions to be taken, whilst complying with over-arching incident and breach reporting regulations and guidelines.

13.2 *What are the risk(s) being addressed?*

- Incident management is an good way of measuring the effectiveness of any IT Fraud and Security risk management system.
- It can point to systemic weaknesses that should be removed.
- Effective incident management can also be crucial for maintaining the confidence of consumers.

13.3 *Control Requirements:*

i. Monitoring controls should be implemented to detect unauthorised information processing activities.

ii. IFSA members should establish Incident Reporting guidelines that set out formal escalation procedures that cater for the different types of incidents based on criticality and sensitivity. That is, consider alerting Directors / Responsible Officers within a specified time. It is very important that critical incidents are escalated in a timely manner.

iii. Containment of sensitive documents and file notes internally – restrict access to key personnel / case manager.

iv. Tracking and reporting of the status of all reported incidents through until resolution.

v. Obtain client permission at the earliest opportunity to release information to Law Enforcement authorities ie. thus negating the need for a subpoena.

vi. Establish line of dialogue between case manager and client, to establish a sense of cooperation on the investigation.

vii. Subsequent enquiry communications should be couriered, to avoid further mail interception in the case of identity theft / fraud

viii. Where evidence is to be collected for potential legal action, the investigation and collection of evidence should be performed in a manner that preserves the admissibility of the evidence in a court of law.

ix. Amendment to General Terms & Conditions in PDS documents to permit information-sharing between parties in the event of fraudulent activity.

14 CONSUMER IT SECURITY & FRAUD AWARENESS

14.1 IFSA members should have adequate arrangements to ensure that customers, advisers, agents and relevant third parties are aware of the risks involved in electronic communication in the context of the business process that deals with their needs.

14.2 *What are the risk(s) being addressed?*

- One of the main barriers to effective deployment of technology to deliver effective services to customers remain the varying degree of IT literacy among customers.
- While technology including the internet and e-mails are powerful tools for communication and service delivery, there are inherent risks associated with these tools that could just as easily undermine their effectiveness and the credibility of industry.

14.3 *Control Requirements:*

i. Establish formal methods of communicating with consumers about relevant and appropriate risks.

ii. Ensure that business process owners are aware of the risks to customers of electronic communication in the context of the services that are provided.

iii. Ensure that advisers and agents understand their roles & responsibilities for managing information security.

iv. Establish a formal contact & incident management process for handling fraud and identity theft claims from external parties. See section 13.

15 LEGAL COMPLIANCE

15.1 IFSA members should understand and meet all relevant and applicable legal, statutory, regulatory and contractual IT security requirements.

15.2 *What are the risk(s) being addressed?*

- Regulatory and compliance risk is a significant risk for IFSA members. Compliance failure could often mean significant reputational damage as well as civil and criminal consequences.

15.3 *Control Requirements:*

i. Identification of all applicable legal, statutory, regulatory and/or contractual IT security requirements.
ii. Define responsibilities to maintain compliance to the identified IT security requirements.
iii. Implement monitoring processes to measure the level of compliance.

REFERENCES

- ISO/IEC 27001: 2005 or "Information technology - Security techniques -Information security management systems" by International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC).
  http://www.iso.org/iso/en/ISOOnline.frontpage

- Sarbanes-Oxley Act 2002 (US), SOX Section 404, Pub L. No.107-204, 116 Stat. 745.

- "Control Objectives for Information and related Technology" Fourth Edition or COBIT Version 4.1, released in December 2005 by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI).

- Privacy Act (Cth) 1988, National Privacy Principles (NNP)

- Payment Card Industry (PCI) Security Standards Council, The Payment Card Industry Standard Data Security Standard.

- "An Agreement to a National Identity Security Strategy" between The Commonwealth of Australia, the States of New South Wales, Victoria, Queensland, Western Australia, South Australia, and Tasmania, the Australian Capital Territory and the Northern Territory, April 2007. See Intergovernmental Agreement to the COAG meeting of 13 April 2007.
  (http://www.coag.gov.au/meetings/130407/docs/national_identity_security_strategy.pdf)

- "Report for the Council of Australian Governments on a Gold Standard Enrolment Framework – An Element of the National Identity Security Strategy" by the National Identity Security Coordination Group, see Related Reports to the COAG meeting of 13 April 2007.
  (http://www.coag.gov.au/meetings/130407/index.htm)

- IFSA Standard No. 5, 1999, "Operational Capability Standard", Section 10.1 Business Continuity and Disaster Planning, Sydney. (http://www.ifsa.com.au/index.aspx)