INFOSEC RISK MITIGATION PROCESS –

RELIANCE ON DEMONSTRATED DILIGENCE

Joss Bernstein

Group Operational Risk, Investec

100 Grayston Drive, Sandown, Sandton, Johannesburg, South Africa +27 11 286 7941 (tel) 286 7946 (fax) PO Box 785700, Sandton, Johannesburg, South Africa 2146 jbernstein@investec.co.za

ABSTRACT

An organisation needs to protect the Confidentiality, Integrity and Availability (CIA) of its Information Assets against financial loss and ensure the reliability of its financial reporting

The Executive of an organisation has a *duty of care* to protect the CIA of Information Assets entrusted to its safekeeping in a *'reasonably diligent' manner*

Despite substantial investment in policies, technology, consulting and audit fees, the Executive of a large publicly traded organisation faces the *ongoing challenge* of discharging its duty of care in a manner that achieves an *acceptable level of risk* within resource constraints and satisfies Corporate Governance, Regulatory and Audit requirements

Reliance on *trust* is not enough to discharge its duty of care to internal and external stakeholders

This paper recommends that the Executive embed an InfoSec Risk Mitigation Process to enable its reliance on *demonstrated diligence* (supported by appropriate evidence of risk mitigation in place) in order to provide *positive assurance* that it protects the CIA of Information Assets entrusted to its safekeeping in a *'reasonably diligent' manner*, thereby discharging its duty of care

It is further recommended that InfoSec practitioners use the methodology outlined in this paper to develop and embed the InfoSec Risk Mitigation Process with the role players delegated by the Executive

The recommended methodology is an application of the principles of ISO/IEC 17799 in conjunction with BS 7799-2 to the needs of an organisation

The main benefits of using the recommended methodology are:

- embed operational management responsibility for mitigating InfoSec risks in a *'reasonably diligent' manner* and for reporting a *reliable risk profile* to the Executive
- enable the Executive to provide *positive assurance* that it protects the CIA of Information Assets entrusted to its safekeeping in a *'reasonably diligent' manner*

KEY WORDS

InfoSec (Information Security) Risk Mitigation Process, CIA (Confidentiality, Integrity, Availability), Information Assets, Executive, duty of care, ongoing challenge, acceptable level of risk, reliance on trust, InfoSec Risk Mitigation Process, reliance on demonstrated diligence, positive assurance, reasonably diligent manner, reliable risk profile, InfoSec practitioner, influence action

For a Glossary of Terms used in this paper – see section 11

INFOSEC RISK MITIGATION PROCESS – RELIANCE ON DEMONSTRATED DILIGENCE

1 TYPICAL CHALLENGES FACED BY INFOSEC PRACTITIONERS

InfoSec practitioners are mandated to *influence action* in their organizations. They should promote the concept that the governance of Information Security is about more than firewalls, intrusion detection and anti virus. Other 'baseline' controls also require effective governance - eg 'logical' and 'physical' access controls, configuration checking, patch update, incident response, user awareness, record retention

Best practice frameworks (eg ISO/IEC 17799[1]) are useful sources of knowledge to guide the InfoSec practitioner yet may be daunting to the InfoSec practitioner to consistently and effectively apply within a large publicly traded organization. Especially one that has autonomous Operating Divisions in various global jurisdictions, centralized and decentralized IT infrastructure, shared and unique business applications

To ensure sustainable governance that satisfies internal and external stakeholders, InfoSec practitioners should promote a practical and flexible methodology that applies the principles of ISO/IEC 17799 in conjunction with BS 7799-2[2] to the needs of an organisation

Steven J. Ross highlights the following observations regarding the application of ISO/IEC 17799 (inter alia, *emphasis* supplied):

- "ISO/IEC 17799 has become the international framework because it has been issued by an international standards body
- as a framework, it is providing the basic foundation for those who would develop their own policies and standards
- by itself, ISO/IEC 17799 makes nothing more secure, nor for that matter do standards written according to the framework it provides. It is the *application* of the framework and the standards that creates security"[3]

2 ENABLE EXECUTIVE RELIANCE ON DEMONSTRATED DILIGENCE

Demonstrated diligence provides the Executive with the means of providing *positive assurance* that it protects the CIA of Information Assets entrusted to its safekeeping in a 'reasonably diligent' manner

To enable its reliance on *demonstrated diligence,* the Executive should embed a sustainable InfoSec Risk Mitigation Process within the management structure of the organisation

Effective rollout should enable the Executive of each Operating Division to report a *reliable risk profile* to its stakeholders, supported by appropriate evidence of risk mitigation in place

Corporate Governance requirements place the onus of providing *positive assurance* on the Executive to report a *reliable risk profile* to those stakeholders to whom it owes a duty of care

3 CORPORATE GOVERNANCE, REGULATORY AND AUDIT REQUIREMENTS

Various Corporate Governance, Regulatory and Audit requirements make reference to Executive accountability for an organisation's effective risk mitigation (including Information Security)

The King Report on Corporate Governance for South Africa - "the Board is responsible for ensuring that an effective ongoing process is in place to identify and proactively manage risk"; "Directors have an obligation to demonstrate that they have dealt comprehensively with the issues of risk management and internal control"; "the Board should ensure that the company complies with all relevant laws, regulations and codes of best business practice"[4]

The (South African) Electronic Communications and Transactions Act 25 of 2002, inter alia, facilitates legal recognition of electronic transactions, protects the consumer by stipulating disclosure of minimum information on ECommerce websites and sets out requirements for asserting proper evidentiary weight of electronic records[5]

Financial Services Authority (FSA) Integrated prudential sourcebook, information security – "a firm should establish and maintain appropriate systems and controls for the management of its information security risks, including consideration of confidentiality, integrity, availability, authentication, non-repudiation and accountability" (abbreviated)[6]

A sustainable InfoSec Risk Mitigation Process provides Audit with the means to verify the reliability of *positive assurance* provided by the Executive and to express an independent opinion with regard to the *reported risk profile* (i.e. similar to verifying a 'financial' report)

4 EXECUTIVE MANDATE OF RESPONSIBLE PERSONS

The Executive should mandate a Group Co-ordinator, and a Local Co-ordinator for each Operating Division, to rollout and embed an InfoSec Risk Mitigation Process across the organization

The Group Co-ordinator should constitute a representative Group InfoSecForum, comprising the Local Co-ordinators of each Operating Division and any adhoc invitees

The Group InfoSecForum should *govern* issues of 'common interest' to all Operating Divisions (eg Strategy for risk mitigation, Methodology, Policies & Standards that provide specific management direction, Budget, progress milestones towards achieving the Strategy, adhoc issues)

The Local Co-ordinator of each Operating Division should constitute a representative Local InfoSecForum to *govern* its InfoSec Risk Mitigation Process, including the delegation of roles and responsibilities (as depicted in Figure 1 below)

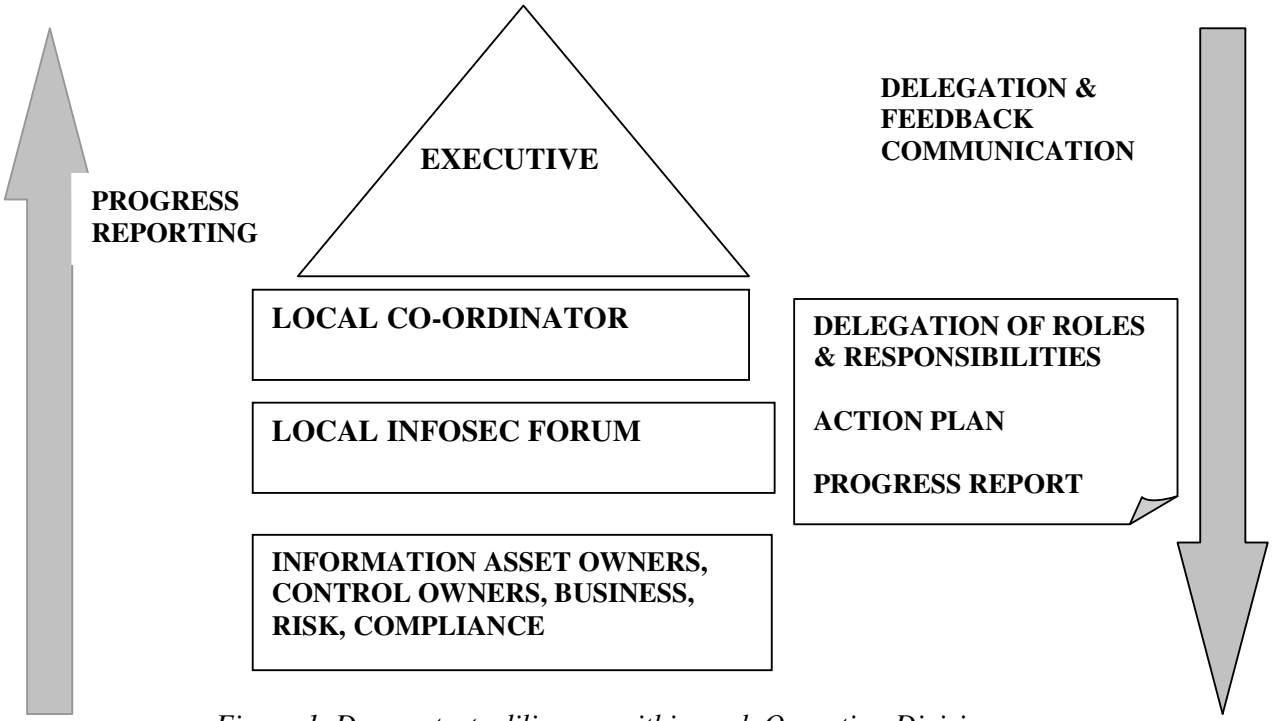

Figure 1. Demonstrate diligence within each Operating Division

5 GROUP CO-ORDINATOR AND LOCAL CO-ORDINATOR COMMUNICATION

All Local Co-ordinators should also supply their Progress Reports to the Group Co-ordinator, for the purpose of measuring progress milestones set by the Group InfoSecForum

Each Operating Division should implement its portion of the 'groupwide' Strategy by demonstrating diligence within its management structure (as depicted by Figure 1 above)

This is essential to achieve successful rollout across an organisation that has autonomous Operating Divisions in various global jurisdictions, centralised and decentralised IT infrastructure, shared and unique business applications

Embedding the Local Co-ordinator responsibility in each Operating Division ensures the protection of its Information Assets and Executive discharge of its duty of care to its stakeholders

The Group Co-ordinator is responsible for the detailed implementation and monitoring of Information Security across the Group and relies on the output of the Local Co-ordinator of each Operating Division (in most organisations, this involves 'dotted line' reporting)

6 APPLICATION OF ISO/IEC 17799 IN CONJUNCTION WITH BS 7799-2

The 'introduction' section of ISO/IEC 17799 sets out the definition of information security, why it is needed, how to establish security requirements, assessing security risks and selecting controls. As a Code of Practice for Information Security Management its ten sections "provide a common basis for *developing* organisational security standards and effective security management practice"[1]

The *detailed* recommendations of ISO/IEC 17799 should be applied in conjunction with the *management framework* of BS 7799-2 to establish elements of best practice most appropriate to the needs of an organisation

Paragraph 3 and Figure 1 of BS 7799-2 set out the following steps to identify and document the Specification for an Information Security Management System (ISMS) under the heading 'Establishing a management framework" (abbreviated, *emphasis* supplied):

- Define the Information Security Policy
- Define the Scope of the ISMS (the organisation, its location, assets and technology)
- Undertake a Risk Assessment (identify threats to assets, vulnerabilities and impact)
- Identify areas of risk to be managed
- Select appropriate Control Objectives and Controls to be implemented (*detailed* guidance is set out in ISO/IEC 17799 which adopted BS 7799-1)
- Prepare a Statement of Applicability (selected and excluded Control Objectives and Controls, with reasons)

Paragraph 3.6 of BS 7799-2 states (*emphasis* supplied) "Records, being *evidence* generated as a consequence of the operation of the ISMS, shall be maintained to *demonstrate compliance* with the requirements of this part of BS 7799 as appropriate to the system and the organisation"[2]

It is recommended that an organisation develop its InfoSec Risk Mitigation Process by applying the principles of ISO/IEC 17799 in conjunction with BS 7799-2 to its needs

7 RECOMMENDED METHODOLOGY FOR DEVELOPING AND EMBEDDING THE INFOSEC RISK MITIGATION PROCESS

InfoSec practitioners should promote use of the following methodology to develop and embed the InfoSec Risk Mitigation Process across the organisation:

A. 'Baseline' process driven by the Group Co-ordinator for the entire organization:

1) Maintain an inventory of Information Assets
2) Assess Risks that may breach the CIA of *all* Information Assets
3) Develop the *'baseline'* Control Objectives that will mitigate risk to an acceptable level

B. 'Local' process driven by the Local Co-ordinator of each Operating Division:

4) Assess the 'risk mitigation' effectiveness of 'baseline' Controls in place
5) Document *additional* Controls that should protect 'critical' Information Assets
6) Adopt an ongoing Action Plan to mitigate risk to an acceptable level
7) Delegate Control Owners to implement the Action Plan and report progress
8) Submit Progress Report to the Executive
9) Executive to communicate its risk mitigation/acceptance decisions

8 DETAILED EXPLANATION OF EACH PROCESS STEP

A. 'Baseline' process driven by the Group Co-ordinator for the entire organization:

8.1 Maintain an inventory of Information Assets

Information Assets are the information systems and information that enable an organization to generate revenue and supply support services

The value of Information Assets relies on the protection of Confidentiality, Integrity and Availability (CIA) to ensure efficient and secure access to conduct business

Each Operating Division should develop and maintain its inventory of Information Assets

The Information Security Forum Standard of Good Practice for Information Security sets out categories of Information Assets that should be adopted groupwide to ensure complete inventories across the organisation – Computer Installations, Networks, Critical Business Applications and Systems Development[7]

Identify 'critical' Information Assets that may require *additional* risk mitigation

Maintaining an inventory of Information Assets in each Operating Division will assist the Group and Local Co-ordinators in their assessment of Information Security efforts and allocation of available resources across the Group

8.2 Assess Risks that may breach the CIA of *all* Information Assets

Identify a set of potential 'loss events' that may breach the CIA of *all* Information Assets and cause financial and/or reputation loss to the organisation

Group the types of potential 'loss events' into categories to arrive at a complete set that is 'generic' to *all* Information Assets across the Group (eg Physical, Logical, External, Internal)

Examples of 'generic' categories of potential 'loss events':

- group 'natural' and 'malicious' damage to IT Facilities under the Physical category
- group 'virus/worm' and 'denial of service' attacks under the External category

Assess the probability of occurrence and impact severity of all potential 'loss events', assuming no mitigating controls in place

Agree the complete set of 'potential loss events' (per category) at the Group InfoSecForum

8.3 Develop the 'baseline' Control Objectives that will mitigate risk to an acceptable level

Document a Loss Event/Mitigating Controls Matrix to develop a set of 'baseline' Control Objectives that will mitigate all potential 'loss events' to an acceptable level if implemented as designed

'Baseline' Control Objectives and their supporting 'baseline' controls are expected to be in place to protect *all* Information Assets across the organisation with a 'minimum' level of control

If a security breach occurs at an 'acceptable' level of risk (ie after assessing the effectiveness of 'risk mitigation' in place), it is *expected* to result in an acceptable level of financial loss

Table 1 overleaf sets out an example of how to develop a set of 'baseline' Control Objectives

For the purpose of explaining the methodology recommended in this paper, the Mitigating Controls identified in Table 1 have been listed as the 'baseline' Control Objectives in Table 2

Table 1. Matrix to develop a set of 'baseline' Control Objectives

Potential 'loss event' (eg)	**Outcome that may result in financial and/or reputation loss**	**Mitigating Control/s per potential 'loss event' (ISO/IEC 17799 examples)**
Natural damage to IT facilities	Business interruption	Equipment Security, Incident Response*, Backup*
Denial of service attacks	Business interruption	Protection against malicious software, Technical compliance checking, Incident Response*, Backup*
Theft of user identity	Fraud, Theft of confidential information and/or other assets	User password management*
Abuse of access granted	Fraud, Theft of confidential information and/or other assets	User password management*, Review of user access rights, Monitoring System Access and Use

The concept of the above Matrix was adapted from the Information Security Guideline for NSW Government[8] - it should be noted that a Mitigating Control such those marked * may mitigate *more than one* potential 'loss event'

Ensure the completeness of all the identified Mitigating Controls by assessing the design of the combined effect of risk mitigation per identified Potential Loss Event

Develop a set of 'baseline' Control Objectives by grouping all identified Mitigating Controls (eg group the 'detect, alert, respond and recover' Mitigating Controls under the Incident Response 'baseline' Control Objective)

Establish a comprehensive Strategy for directing all InfoSec Risk Mitigation efforts by ensuring the completeness of the 'baseline' Control Objectives

Allocate the set of 'baseline' Control Objectives into relevant ISO/IEC 17799 categories (eg Incident Response is listed under 'Personnel Security')

Distribute a template of 'baseline' Control Objectives and their supporting Controls to the Local Co-ordinators of each Operating Division, for detailed assessment

B. 'Local' process driven by the Local Co-ordinator of each Operating Division:

8.4 Assess the 'risk mitigation' effectiveness of 'baseline' Controls in place

Controls Assessment and Action Plan activities should be integrated into a single *living* document, to enable ongoing and effective risk mitigation

This enables the Local Co-ordinator to delegate ownership for each assessed control

Assess the effectiveness of 'baseline' Controls in place and maintain an ongoing Action Plan

Update the Controls Assessment and Action Plan at appropriate frequency

Table 2 overleaf set out an example of a Controls Assessment and Action Plan

For the purpose of explaining the methodology recommended in this paper, the Mitigating Controls identified in Table 1 have been listed as the 'baseline' Control Objectives in Table 2

Table 2. Controls Assessment and Action Plan

'Baseline' Control Objectives (per ISO/IEC 17799 category) **- eg**	**Supporting 'Baseline' Controls to achieve each Control Objective - eg**	**In place? (Y/N)**	**Comment (if Y), Action Plan (if N)**	**Control Owner, Milestone Date** **(frequency if Y, implementation if N)**
Personnel Security				
Incident Response	Detect, alert, respond, recover			
Physical and Environmental Security				
Equipment Security	Power, temperature, lightning, water drainage, fire suppression			
Communications and Operations Management				
Protection against malicious software	Patch & AntiVirus update			
Backup	Frequency, offsite storage, retention			
Access Control				
Review of user access rights	Segregation of duties, authorisation of changes, frequent review & signoff			
User password management	User awareness, policy management, complexity checking			
Monitoring System Access and Use	Tolerance parameters, alert system owners, response procedures			
Compliance				
Technical compliance checking	Compliance checking with technical standards (eg firewall, router, server)			

Refer to ISO/IEC 17799 for detailed controls under *other* categories (eg Security Policy, Organisational Security, Asset Classification and Control, Systems Development and Maintenance)

8.5 Document additional Controls that should protect 'critical' Information Assets

'Baseline' Controls are designed to mitigate risks that may breach CIA of *all* Information Assets

Document *additional* Controls in the Controls Assessment and Action Plan that should achieve effective risk mitigation for 'critical' Information Assets (eg Application, Network)

Additional controls are required where 'minimum, baseline' controls are not expected to achieve effective risk mitigation (eg 'two factor' authentication may be preferred to 'password')

8.6 Adopt an ongoing Action Plan to mitigate risk to an acceptable level

The Local Co-ordinator's Action Plan enables *ongoing* achievement of two goals:

Maintain the effectiveness of Controls in place ('operational' *frequency* check)

Implement the required Controls not yet in place ('project' *milestone* check)

All Controls ('baseline' and 'additional') should be documented in the Action Plan and updated on an appropriately frequent basis

8.7 Delegate Control Owners to implement the Action Plan and report progress

Delegate the implementation of Action Plan tasks to Control Owners (including personnel that report outside the Operating Division eg Central IT)

Control Owners are responsible for implementing, monitoring and retaining evidence of demonstrated diligence and progress reporting to the Local Co-Ordinator for all delegated Controls

The Local Co-ordinator is responsible for monitoring the performance of all delegated Control Owners and collating their Progress Reports

8.8 Submit Progress Report to the Executive

Table a Progress Report for the Operating Division at its Local InfoSecForum

Submit a Progress Report to the Executive at appropriate frequency, highlighting:

- strong and weak 'baseline' Control Objectives (progress achieved and priority actions)
- key Control Performance Indicators
- key obstacles encountered
- any Loss Events since the last Progress Report
- current status of 'additional' Controls that protect 'critical' Information Assets
- residual risk exposures requiring Executive risk mitigation/acceptance decisions

8.9 Executive to communicate its risk mitigation/acceptance decisions

Executive feedback is critical to the sustainability of the InfoSec Risk Mitigation Process and the commitment of all role players

This feedback should be directed to relevant *management* aspects to sustain the overall Process such as adequate resources to achieve an *acceptable level of risk*, support to address key obstacles and enquiry to understand the impact of the reported residual risk exposures in order to establish and communicate appropriate risk acceptance/mitigation decisions

9 LINK BETWEEN THE RECOMMENDED METHODOLOGY AND BS 7799-2

The following table shows a clear link between the steps of the recommended Methodology and the steps outlined in the BS 7799-2 ISMS (Information Security Management System):

Table 3. Link between the Recommended Methodology and BS 7799-2 ISMS steps

BS 7799-2 ISMS steps	Recommended Methodology steps	Comment
Define the Policy	Not specifically addressed in Methodology	InfoSecForum mandate
Define the Scope of the ISMS	Maintain inventory of Information Assets*	Clear link to ISMS
Undertake a Risk Assessment	Assess risks that may breach CIA of *all* Information Assets	Clear link to ISMS
Identify areas of risk to be managed	Protect all Computer Installations, Networks, Critical Business Applications, Systems Development	Adequate link to ISMS
Select appropriate Control Objectives and Controls to be implemented	Develop 'baseline' Control Objectives for *all* Information Assets and 'additional' Controls for 'critical' Information Assets	Clear link to ISMS
Prepare a Statement of Applicability	Adopt ongoing Action Plan and Progress Report; Executive risk management decision	Methodology shows a practical application of ISMS

The methodology recommended in this paper is an application of the detailed ISO/IEC 17799 recommendations in conjunction with the management framework set out in BS 7799-2 ISMS

10 CONCLUSION

Demonstrated diligence provides the Executive with the means of providing *positive assurance* that it protects the CIA of Information Assets entrusted to its safekeeping in a 'reasonably diligent' manner

To enable its reliance on demonstrated diligence, the Executive should embed a sustainable InfoSec Risk Mitigation Process within the management structure of the organisation

InfoSec practitioners are mandated to *influence action* in their organisations and should promote this Process to assist the Executive in the discharge of its duty of care

It is recommended that InfoSec practitioners use the methodology outlined in this paper to develop and embed the InfoSec Risk Mitigation Process with the role players delegated by the Executive

The recommended methodology applies the principles of ISO/IEC 17799 in conjunction with BS7799-2 to the needs of an organisation

Embedding the Local Co-ordinator responsibility in each Operating Division ensures the protection of its Information Assets and Executive discharge of its duty of care to its stakeholders

The Group Co-ordinator is responsible for the detailed implementation and monitoring of Information Security across the Group and relies on the output of the Local Co-ordinator of each Operating Division (in most organisations, this involves 'dotted line' reporting)

Commitment of the Executive is critical to the sustainability of the InfoSec Risk Mitigation Process and should focus on supporting the *management and resourcing* aspects to achieve an acceptable level of risk

The main benefits of using the recommended methodology are:

- embed operational management responsibility for mitigating InfoSec risks in a *'reasonably diligent' manner* and for reporting a *reliable risk profile* to the Executive
- enable the Executive to provide *positive assurance* that it protects the CIA of Information Assets entrusted to its safekeeping in a *'reasonably diligent' manner*

The remainder of this paper sets out the Glossary of Terms, End Notes and References

11 GLOSSARY OF TERMS USED IN THIS PAPER

Glossary of terms provided by the author, set out in the order in which they first appear in this paper:

- CIA - Confidentiality, Integrity, Availability
    - Confidentiality – information is restricted to those authorised to have access
    - Integrity – information processing is complete and accurate
    - Availability – information is available to authorised persons when required
- Information Assets – information and systems used to generate revenue and supply support services
- Executive – grouping of persons mandated by the stakeholders of an organisation with the primary duty of care to protect the best interests of an organisation
- duty of care – obligation to stakeholders of an organisation to protect its best interests
- ongoing challenge – ongoing challenge to demonstrate a 'reasonable' level of diligence
- acceptable level of risk – if a breach occurs at this level of risk (ie after assessing the effectiveness of 'risk mitigation' in place), it is *expected* to result in an acceptable level of financial loss
- reliance on trust – reliance on the trust of mandated persons to practice diligence:
    - *sole* reliance on 'trust' (which is necessary to sustain the mandated role) does not require the 'demonstration' of diligence
- InfoSec (Information Security) Risk Mitigation Process – ongoing process of demonstrated diligence
- reliance on demonstrated diligence – reliance on the management representation of delegated role players, which is warranted on the basis of appropriate and retained evidence of diligence
- InfoSec practitioner – mandated to influence action and assist the delegated role players
- influence action – proactive promotion of action to anticipate and achieve effective risk mitigation in a reasonably diligent manner that protects the best interests of an organisation
- sustainable governance – the ongoing demonstration of diligence by delegated role players
- positive assurance – management representation of the effectiveness of risk mitigation in place
- reasonably diligent – doing the best expected of a mandated role player, with available resources:
    - although a security breach may still occur *after* demonstrating 'reasonable' diligence, the mandated role player should be able to show a responsible discharge of the mandated role
    - effective incident review should result in enhanced effectiveness of risk mitigation in place
    - the same principle of 'hindsight learning' applies to a 'weak' audit report
- reliable risk profile – reporting the effectiveness of risk mitigation in place on the basis of warranted reliance on demonstrated diligence (supported by appropriate evidence of risk mitigation in place)
- 'Baseline' process – this process is driven by the Group Co-ordinator to co-develop the 'baseline' controls that are designed to mitigate the risks of security breach that threaten *all* Information Assets across the organisation
- 'Baseline' Control Objectives – these Control Objectives (and their supporting 'baseline' controls) are expected to be in place to protect *all* Information Assets across the organisation
    - 'baseline' Control Objectives apply a 'minimum' level of control that is appropriate to protect each class of Information Asset across the organisation (eg Computer Installations, Networks, Applications in Production and those undergoing System Development)
- 'Local' process – this process is driven by the Local Co-ordinator of each Operating Division to achieve the following goals:
    - implement and monitor 'baseline' Control Objectives that are delegated to Control Owners
    - implement and monitor any *additional* controls required to protect 'critical' Information Assets belonging to the Operating Division

12 END NOTES

Unless otherwise quoted, the views expressed in this Paper are based on the author's research of best practice and experience in co-developing the Investec Information Security Risk Assessment Framework, and do not necessarily represent the Investec Group of Companies or any other organisation

13 REFERENCES

[1] International Standards Organisation (2000). *ISO/IEC 17799:2000 (E), Information Technology – Code of Practice for Information Security Management.* Available for purchase at SABS Standards Direct website as at April 15, 2005 from the Internet: URL http://www.standardsdirect.org/iso17799.htm

[2] British Standards Institute (1999). *BS 7799-2: 1999, Information Security Management – Part 2: Specification for information security management systems.* Available for purchase at SABS Standards Direct website as at April 15, 2005 from the Internet: URL http://www.standardsdirect.org/iso17799.htm

[3] Ross, S. (2004). IS Security Matters, *Frameworkers of the World, Unite.* Information Systems Control Journal, 6: pp. 9-10.

[4] Institute of Directors (2002). *King Report on Corporate Governance for South Africa*: pp. 46 & 74. Available for purchase at Institute of Directors website as at April 15, 2005 from the Internet: URL http://www.iodsa.co.za/corporate.htm

[5] South African Government (2002). *Electronic Communications and Transactions Act 25 of 2002*. Retrieved April 15, 2005 from the Internet: URL http://www.internet.org.za/ect_act.html

[6] Financial Services Authority (2003). *Integrated prudential sourcebook, Near-final text on prudential risks systems and controls.* Information Security SYSC 3A.5.10G and SYSC 3A.5.11: pp. 6. Current version available from FSA website sitemap as at April 15, 2005 http://www.fsa.gov.uk/pages/sitemap/index.shtml

[7] Information Security Forum (2003). *The Standard of Good Practice for Information Security.* Retrieved April 15, 2005 from the Internet: URL http://www.isfsecuritystandard.com/index_ie.htm

[8] New South Wales Government (2003). Department of Commerce, Office of Information and Communications Technology, *Information Security Guideline for NSW Government.* Retrieved April 14, 2005 from the Internet: URL http://www.oict.nsw.gov.au/guidelines/4.3.18.b.security.asp

14 ADDITIONAL READING

Chapin, D, Akridge, S. (2005). *How can Security be Measured?* Information Systems Control Journal, 2: pp. 43-47.

IT Governance Institute. (2004). *COBIT Security Baseline – An Information Security Survival Toolkit.* Available for download at ITGI website as at April 15, 2005 from the Internet: URL www.itgi.org

Mears, L, von Solms, R. (2004). Department of Information Technology, Port Elizabeth Technikon, South Africa, *Corporate Information Security Governance – A Holistic Approac*h.

Pironti, J. (2005). *Key Elements of an Information Security Program.* Information Systems Control Journal, 1: pp. 23-28.