

G41 RETURN ON SECURITY INVESTMENT (ROSI)

The specialised nature of information technology (IT) audit and assurance and the skills necessary to perform such audits require standards that apply specifically to IT audit and assurance. One of the goals of ISACA[®] is to advance globally applicable standards to meet its vision. The development and dissemination of the IT Audit and Assurance Standards is a cornerstone of the ISACA professional contribution to the audit and assurance community. There are multiple levels of guidance:

- **Standards** define mandatory requirements for IT audit and assurance. They inform:
 - IT audit and assurance professionals of the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics
 - Management and other interested parties of the profession's expectations concerning the work of practitioners
 - Holders of the Certified Information Systems Auditor™ (CISA[®]) designation of requirements. Failure to comply with these standards may result in an investigation into the CISA holder's conduct by the ISACA Board of Directors or appropriate ISACA committee and, ultimately, in disciplinary action.
- **Guidelines** provide guidance in applying IT Audit and Assurance Standards. The IT audit and assurance professional should consider them in determining how to achieve implementation of the standards, use professional judgement in their application and be prepared to justify any departure. The objective of the IT Audit and Assurance Guidelines is to provide further information on how to comply with the IT Audit and Assurance Standards.
- **Tools and Techniques** provide examples of procedures an IT audit and assurance professional might follow. The tools and techniques documents provide information on how to meet the standards when performing IT audit and assurance work, but do not set requirements. The objective of the IT Audit and Assurance Tools and Techniques is to provide further information on how to comply with the IT Audit and Assurance Standards.

COBIT[®] is an IT governance framework and supporting tool set that allows managers to bridge the gaps amongst control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout enterprises. It emphasises regulatory compliance, helps enterprises increase the value attained from IT, enables alignment and simplifies implementation of the COBIT framework's concepts. COBIT is intended for use by business and IT management as well as IT audit and assurance professionals; therefore, its usage enables the understanding of business objectives and communication of good practices and recommendations to be made around a commonly understood and well-respected framework. COBIT is available for download on the ISACA web site, www.isaca.org/cobit. As defined in the COBIT framework, each of the following related products and/or elements is organised by IT management process:

- **Control objectives**—Generic statements of minimum good control in relation to IT processes
- **Management guidelines**—Guidance on how to assess and improve IT process performance, using maturity models; Responsible, Accountable, Consulted and/or Informed (RACI) charts; goals; and metrics. They provide a management-oriented framework for continuous and proactive control self-assessment, specifically focused on:
 - Performance measurement
 - IT control profiling
 - Awareness
 - Benchmarking
- **COBIT Control Practices**—Risk and value statements and 'how to implement' guidance for the control objectives
- **IT Assurance Guide**—Guidance for each control area on how to obtain an understanding, evaluate each control, assess compliance and substantiate the risk of controls not being met

A **glossary** of terms can be found on the ISACA web site at www.isaca.org/glossary. The words audit and review are used interchangeably in the IT Audit and Assurance Standards, Guidelines, and Tools and Techniques.

Disclaimer: ISACA has designed this guidance as the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics. ISACA makes no claim that use of this product will assure a successful outcome. The publication should not be considered inclusive of all proper procedures and tests or exclusive of other procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific procedure or test, the controls professional should apply his/her own professional judgement to the specific control circumstances presented by the particular systems or IT environment.

The ISACA Professional Standards Committee is committed to wide consultation in the preparation of the IT Audit and Assurance Standards, Guidelines, and Tools and Techniques. Prior to issuing any documents, the Standards Board issues exposure drafts internationally for general public comment. The Professional Standards Committee also seeks out those with a special expertise or interest in the topic under consideration for consultation where necessary. The Standards Board has an ongoing development programme and welcomes the input of ISACA members and other interested parties to identify emerging issues requiring new standards. Any suggestions should be e-mailed (standards@isaca.org), faxed (+1.847. 253.1443) or mailed (address at the end of document) to ISACA International Headquarters, for the attention of the Val IT initiative manager. This material was issued on 1 March 2010.

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S10 IT Governance states the IT audit and assurance professional should review:

- And assess whether the IT function aligns with the enterprise's mission, vision, values, objectives and strategies
- Whether the IT function has a clear statement about the performance expected by the business (effectiveness and efficiency) and assess its achievement
- And assess the effectiveness of IT resources and performance management processes

1.2 Linkage to COBIT

1.2.1 Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's control objectives and associated management practices. To meet the return on security investment (ROSI) requirements of IT audit and assurance professionals, the processes in COBIT most likely to be relevant, selected and adapted are classified here as primary and secondary. The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

1.2.1 Primary IT processes are:

- PO1 *Define a strategic IT plan*
- PO3 *Determine technology direction*
- PO5 *Manage the IT investment*
- PO9 *Assess and manage IT risk*
- DS3 *Manage performance and capacity*
- DS6 *Identify and allocate costs*
- ME1 *Monitor and evaluate IT performance*
- ME4 *Provide IT governance*

1.2.3 Secondary IT processes are:

- PO6 *Communicate management aims and direction*
- AI1 *Identify automated solutions*
- AI5 *Procure IT resources*
- ME3 *Ensure regulatory compliance*

1.2.4 The information criteria most relevant to ROSI are:

- Primary—Effectiveness, efficiency and availability
- Secondary—Confidentiality, integrity and reliability

1.3 Purpose of the Guideline

1.3.1 Enterprises are increasingly finding it challenging to make a case to invest in IT security. Clearly defining ROSI is critical for enterprises to attain business objectives. To obtain a reasonably accurate estimation of ROSI, the enterprise needs to determine its security requirements and the most appropriate measure of ROSI, and establish metrics to collect information to measure ROSI. Business operations today recognise the significance of security measures as well as the risks and consequences involved in ignoring the impact of security to business operations. Decision makers are required to quantify, review and modify security metrics periodically to ensure effectiveness of the security measure. Additionally, internal, external and regulatory compliance require maintaining continuous improvement of security goals.

1.3.2 Enterprises cannot afford to ignore the value propositions of security metrics to effectively achieve appropriate ROSI. It is important to define strategic security measures in quantifiable user needs, develop a road map that incorporates a consensus-driven approach to define effective measures and provide periodic assessments to establish continuous improvement of ROSI.

1.3.3 IT audit and assurance professionals must have a clear understanding of the value proposition for ROSI. It is in this context that there is a need for a guideline to provide guidance to IT audit and assurance professionals to review return on security investments while carrying out audit assignments.

1.4 Guideline Application

1.4.1 This guideline provides guidance in applying Standard S10 IT Governance.

1.4.2 The IT audit and assurance professional should consider this guideline in determining how to achieve implementation of the above standard, use professional judgement in its application and be prepared to justify any departure.

1.4.3 When applying this guideline, the IT audit and assurance professional should consider its guidance in relation to other relevant ISACA standards and guidelines.

1.5 Risk Management

1.5.1 There should be collaborative periodic risk assessment developed amongst those responsible for securing information assets and the responsible senior management, with the business owner(s) managing the information assets of the enterprise. Specifically, the enterprisewide and business process owner risk assessments, denoting layers of controls, should be considered in the evaluation by the IT audit and assurance professional in gaining an understanding of the control environment. For example, the risk assessment performed by the business process owner, which includes an evaluation of the adequacy of the preventive control of periodically revalidating access to critical information assets, should be considered.

1.5.2 There is an inherent risk that the subject matter may be highly complicated coupled with security engineers/administrators who may not adequately understand all of the risks to the enterprise and the necessary mitigating control processes. For example, security over information assets may require technical controls at various entry and exit points within the network transmission in addition to the server controls. Thus, a security specialist for network security may be required, in addition to a security administrator with primary knowledge over server access controls, to fully understand all of the security risks. Thus, inherent within this risk assessment is the subject matter risk that all risks have been adequately identified, quantified and mitigated to the extent possible by the enterprise. Accordingly, an independent assessment may be required from various specialists knowledgeable on end-to-end security controls within the entire IT area to potentially identify all of the risks and necessary mitigating controls.

1.5.3 There is inherent audit risk resulting from the auditor responsible for performing an independent assessment not adequately understanding and/or reviewing the necessary control processes commensurate with the level of risk. In addition, there is a likelihood that the auditor will not properly conclude on the adequacy and efficiency of controls by leveraging sampling and other limited methodologies based upon economy of scale factors that will not always result in complete coverage of the risk area. Thus, management should be alerted that audit will not guarantee that the auditor will completely identify, test and conclude on the adequacy of all controls. Accordingly, additional oversight and independent assessment of the auditor's evaluation may be warranted given the size, complexity and significance of the enterprise's information assets.

2. ROSI

2.1 Introduction

2.1.1 ROSI for an enterprise is an important measure in today's cyberworld, in which hackers, computer viruses and cyberterrorists are making headlines. Security has become a priority for business enterprises that leads to answering many questions such as:

- How does a business become secure?
- How much security is enough?
- How does a business know when its security level is reasonable?
- How should security investment be accounted for?
- What is the right monetary and time investment to put in security?
- Which system components or other aspects should be targeted first?

Specifically, the primary basis of ROSI is the comparison of costs (e.g., creating firewalls, cost of the breach, cost of backing storage and various system elements that are redundant) and the preventive and corrective benefits that reduce the likelihood of cybersecurity breaches and resulting losses.

2.1.2 Measurement of risk is predicated, as with all IT-related impacts, in system availability, data integrity and information confidentiality.

2.1.3 Executive decision makers want to understand the impact of security on the bottom line. To arrive at how much to spend on security they need to know:

- How much is the lack of security costing the business?

- What impact is the lack of security having on productivity?
- What impact would a catastrophic security breach have?
- What are the cost-effective solutions?
- What impact will solutions have on productivity?
- Is the exposure being reduced?

2.1.4 ROSI is a key performance indicator that helps measure efficiency and effectiveness of spending on IT security. The metric is a top-down measure correlating IT security expense and its productivity into a concise, comparative metric for current performance assessment and planning.

2.1.5 By identifying ROSI, a business has a meaningful planning tool that allows it to determine both the appropriate level of IT security expense and the appropriate level of security required to protect the business.

2.1.6 By properly planning, managers should distinguish between operating costs benefiting the enterprise for a single time period or a capital investment extending beyond this single time period horizon in cybersecurity activities.

2.2 Determining ROSI

2.2.1 Identification and allocation of costs are essential to deploying the ROSI principle. Direct costs can be specifically linked to the particular cybersecurity breach, whereas indirect costs (e.g., an intrusion detection system that provides abundant controls for numerous types of breaches) cannot be linked with any certainty to a specific breach.

2.2.2 Another delineation is between explicit and implicit cost. Explicit cost can be measured, for example, in developing and maintaining firewalls, whereas implicit cost may be termed 'lost opportunities', such as loss in reputation, an ambiguous estimate. Regardless of ease of estimation, explicit and implicit costs should be included in the cost-benefit analysis in some quantifiable way.

2.2.3 To determine return on investment (ROI), a widely used equation is:

$$\text{ROI} = \frac{\text{Expected returns} - \text{Cost of investment}}{\text{Cost of investment}}$$

2.2.4 There are several quantifiable methods to employ for ROSI. For example, there is net present value (NPV), which compares anticipated benefits and costs over different time periods. In addition, there is a variant of the NPV called internal rate of return (IRR), which sets the discount rate to make the NPV of the investment equal to zero. Both these methods provide a decision rule for accepting or rejecting incremental cybersecurity activities.

2.2.5 Calculation of ROSI in tabular form, without consideration of the time value of money, predicated upon the cost of prevention, is shown in **figure 1**.

2.2.6 Risk exposure is calculated by multiplying the projected cost of a single loss exposure (SLE) with its expected annual rate of occurrence (ARO). Risk exposure = SLE * ARO

The methods of estimating SLE and ARO are based upon metrics internally generated from past experience or drawn from external resources. Actuarial tables are created from insurance claim data, academic research and independent surveys.

2.2.7 Research from Idaho University (USA) defines ROSI based upon cost of recovery after the event as:

$$\text{ROSI} = \text{R} - \text{annual loss expectancy (ALE)}, \text{ where } \text{ALE} = (\text{R} - \text{E}) + \text{T}, \text{ i.e., } \text{ROSI} = \text{E} - \text{T}$$

'R' is the annual cost to recover from any number of intrusions, 'E' is the monetary savings resulting from use of the security tool, and 'T' is the cost of the intrusion detection tool.

Figure 1—ROSI Calculation					
(without consideration of the time value of money, predicated upon the cost of prevention)					
#	Numbers should be in the 000s	Options			
		A	B	C	D
i	Financial investment level	0	650.00	1,300.00	1,950.00
ii	Total potential loss from cybersecurity breach without investment	10,000.00	10,000.00	10,000.00	10,000.00
iii	Probability of loss at each financial investment level denoted in i	.75	.50	.40	.33
iv	Expected loss at each investment level (iv) = (ii) X (iii)	7,500.00	5,000.00	4,000.00	3,300.00

Figure 1—ROSI Calculation (without consideration of the time value of money, predicated upon the cost of prevention)					
#	Numbers should be in the 000s	Options			
		A	B	C	D
v	Total expected cypersecurity costs equals investment costs plus expected loss from breaches (v) = (i) + (iv)	7,500.00	5,650.00	5,300.00	5,250.00
vi	Incremental benefits from increase in investment level, reduction in expected loss, i.e., reduction in (iv) values with additional investment	N/A	2,500.00	1,000.00	700.00
vii	Incremental level of investment increase in investment levels, i.e., increase in row i values	N/A	650.00	650.00	650.00
viii	Incremental net benefit of increase in investment level (viii) = (vi) – (vii)	N/A	1,850.00	350.00	50.00

A simplified equation for **figure 1** is:

$$\text{ROSI} = \frac{(\text{Risk exposure} * \% \text{ risk mitigated}) - \text{Cost of security investment}}{\text{Cost of security investment}}$$

2.2.8 In this approach ROSI must be greater than or equal to the difference between R and ALE. See appendix for example.

2.2.9 Two important components are insurance that analyses risks mitigated by proposed security investments and a component that assesses the productivity contribution of the investments. Insurance does not reduce the likelihood of a breach, but rather reduces the severity of losses if a breach occurs. The insurance component requires the comprehensive analysis of vulnerabilities, threats, and value of existing information assets and safeguards that are currently in place to quantify ALE. Security investments ideally aim to achieve either elimination of risk (improve security infrastructure), transfer of risk (purchase insurance), acceptance of risk (absorb potential losses) or a combination of the three.

Figure 2—ROSI Calculation Using NPV					
#	Numbers should be in the 000s Rounded -	Options			
		A	B	C	D
i	Financial investment levels at time t = 0	0	650.00	1,300.00	1,950.00
ii	Total potential loss from cybersecurity breach without investment at time, t = 1	10,000.00	10,000.00	10,000.00	10,000.00
iii	Probability of loss at each financial investment level denoted in i	.75	.50	.40	.33
iv	Expected loss at each investment level (iv) = (ii) X (iii)	7,500.00	5,000.00	4,000.00	3,300.00
v	Present value of expected loss at time, t=1 at each investment level (v) = (iv)/(1 + k) Note: k = interest rate	6,522.00	4,348.00	3,478.00	2,870.00
vi	Present value of total expected cybersecurity costs = investment costs + present value of expected loss from breaches (vi) = (i) + (v)	6,522.00	4,998.00	4,7778.00	4,820.00
vii	Present value (PV) of incremental benefits (B) of increase in investment level (B ₁ /(1 + k) = reduction in PV of expected losses (i.e., reduction in column D values)	N/A	2,174.00	870.00	609.00
viii	Incremental level of investment (C ₀), increase in investment levels, i.e., increase in ii values	N/A	650.00	650.00	650.00
ix	Incremental net benefits of increase in financial investment level resulting in NPV = B ₁ /(1 + k) – C ₀ (ix) = (vii) – (viii)	N/A	1,524.00	220.00	41.00

2.2.10 Given the time value, money must be included in all cost-benefit analyses extending over several time periods. **Figure 2** shows the NPV method.

2.2.11 The incremental benefit of an investment is the present value of the reduction in expected losses. The present value of the expected loss for each investment level is given in **figure 2** in 'v' and reduction in the present value of the expected loss is given in 'vii'. In addition, the values derived in 'ix' represent the NPV for the additional financial investment level (e.g., see columns A through D). Accordingly, to find the optimal investment level, keep increasing the investment as long as the NPV of the incremental investment is positive.

2.2.12 Calculation of ROSI in tabular form, without consideration of the time value of money, is predicated upon the cost of prevention. It is evident from the approach that determining ROSI requires enterprises to have repeatable and consistent security metrics from which to identify and extract meaningful values.

2.3 Security Metrics

2.3.1 Security metrics are measures designed to facilitate decision making and improve performance and accountability through collection, analysis and reporting of relevant performance-related data. Security metrics focus on the actions (and results of those actions) that enterprises take to reduce and manage the risks of loss of reputation, theft of information or money, and business discontinuities that arise when security defences are breached. Primary considerations for development and implementation of a security metrics programme include the following:

- Metrics must yield quantifiable information such as percentages, averages and numbers.
- Data supporting metrics must be readily available.
- Only a repeatable process must be considered for measurement.
- Metrics must be useful for tracking performance and directing resources.
- Metrics should not be expensive or laborious to gather.

2.3.2 Security metrics may be of varied types such as:

- Implementation metrics—Measure the implementation of the security policy.
- Effectiveness/efficiency metrics—Measure results of security solutions.
- Impact metrics—Measure impact on business due to security events.

The types of metrics that can realistically be obtained and are useful depend upon the enterprise's security programme and control implementation. Over a period of time, the focus of gathering metrics shifts with maturing controls.

2.3.3 Data collection is a very important aspect of security metrics. Steps to be considered for data collection include:

- Metrics roles and responsibility, including responsibility for data collection, analysing and reporting
- Audience for the data collection
- Process for collection, analysing and reporting
- Co-ordination with all functions in the enterprise
- Creation or selection of data collection and tracking tools, and modification if required
- Collection of data, consolidation, storing, sorting in a format conducive to data analysis and reporting
- Metrics summary reporting formats
- Gap analysis, identification of cause and corrective action

2.3.4 Some common security metrics are:

- Baseline defence coverage (antivirus, antispyware, firewall, etc.)—Measures how well the enterprise is protected against basic information security threats
- Patch latency—The time between patch release and successful deployment in the enterprise. This is an indicator of the company's patching discipline and ability to react to incidents.
- Password strength—Reduces bad passwords. Identifies potential weak spots and encourages the use of strong passwords that are hard to break
- Platform compliance scores—Benchmarks hardware against acceptable standards
- Legitimate e-mail traffic analysis—Analysis of incoming/outgoing traffic volume, traffic size and traffic flow pattern within the enterprise as well as external to the enterprise.
- Application risk index—Aids in categorising potential risk as high, medium or low

2.4 Optimum Investment in Information Security: Gordon-Loeb Model

2.4.1 Lawrence A. Gordon and Martin P. Loeb, University of Maryland (USA), presented an economic framework that characterises the optimal monetary investment to protect a given set of information assets. The model determines the optimal amount for an enterprise investment towards protecting a set of information in a single period model. It is shown that for a given potential loss, the optimum amount to spend to protect an information asset does not always increase with and increase in an information set's vulnerability. In addition, the model shows that the amount a firm should spend to protect information assets should generally be only a small fraction of the expected loss.

2.4.2 An information set is characterised by the following three parameters:

- λ —The monetary loss conditioned on a breach occurring

- t —The probability of a threat occurring
- v —The vulnerability, defined as the probability that a threat once realised (i.e., an attack) would be successful

Although the three parameters can change over time in the real world, the Gordon-Loeb model assumes them as pre-estimated constants.

The Gordon-Loeb model assumes the function $S(z, v)$ denotes the probability that an information set with vulnerability ' v ' will be breached—conditional on the realisation of a threat and given that the enterprise has made an information security investment of ' z ' to protect that information set. The function $S(z, v)$ is referred to as the security breach probability function. As is common with nearly all economic models, function $S(z, v)$ is assumed to be sufficiently smooth and well behaved continuously, in particular the twice differentiable.

In addition to a general theory, Gordon-Loeb studied several classes of security breach probability functions. One of them is: $S(z, v) = v^{\alpha z + 1}$

Where the parameter ' α ' (>0) is a measure of productivity of information security, a closed-form solution to an optimisation problem is derived that maximises the expected net benefits from an investment in information security (ENBIS) defined as: $ENBIS = \{v - S(z, v)\} t \lambda - z$.

The optimum investment is given by: $z = z^*(v) = \frac{\ln \{-1/(av\alpha \ln v)\}}{a \ln v}$

- 2.4.3** The model has two substantial restrictions—the loss ' λ ' is considered a constant and investment ' z ' is continuous, while the reality is the loss is not a constant and investments are discrete.

3. OBJECTIVES

3.1 Audit

3.1.1 The audit approach to ROSI should be directed towards:

- Ensuring availability of fully defined security requirements for the entire enterprise and/or programmes or projects identified for security coverage within the enterprise
- Establishing business goals that must be achieved by individual business units or the enterprise as a whole, focusing on critical impacts of security as a cost
- Awareness of management and business users towards system vulnerability, availability and reliability
- Analysis technology and operational efficiencies in terms of cost benefits and effectiveness in meeting security goals

3.1.2 Understanding employee/user perception of security is an important consideration for security investment and one of the means of achieving this is through an employee survey. The employee survey must be properly construed and should have a direct correlation between the survey score and financial performance. The survey should ask questions that have coarse quantitative answers or answers that imply a quantitative value. For example, how many spam messages do you receive every day (0-10, 10-30, 30-50, more than 50) or how often is the files server unavailable for more than 10 minutes (daily, weekly, monthly, rarely)? It is important to quantify risk and exposure in a repeatable and consistent manner. This is possible through an effective survey and scoring system for productivity and security, combined with external measurements of value propositions. IS auditors should review the internal survey where one is available.

3.1.3 Downtime assessment can provide an important postmortem analysis of lost productivity during a security incident. Productivity loss must also be considered in calculating the ROI of security solutions. **Figure 3** shows the average downtime and factors that affect productivity.

Figure 3—Factors That Affect Productivity and Average Downtime	
Problem	Average Downtime (in Minutes)
Application and system crashes	10
E-mail filtering, sorting and spam	15
Bandwidth efficiency and throughput	10
Inefficient and ineffective security policies	10
Enforcement of security policies	10
System-related roll outs and upgrades for IT	10
Security patches for operating systems and applications	10
Insecure and inefficient network topology	15
Viruses, virus scanning	10
Worms	10
Trojan, key logging	10
Spyware, system trackers	10
Popup ads	10
Compatibility issues—hardware and software	15
Permissions-based security problems (user/pass)	15
File system disorganisation	10
Corrupt or inaccessible data	15
Hacked or stolen information and data	15
Backup/restoration	15
Application usage issues	15
Source: Sonnenreich, Wes; 'Return on Security Investment (ROSI): A Practical Quantitative Model', <i>Journal of Research and Practice in Information Technology</i> , vol., 38, no. 1, February 2006, a publication of the Australian Computer Society, Australia, 2006	

- 3.1.4 IT audit and assurance professionals should be aware that there are number of ways in which lost productivity can provide a meaningful estimate of risk exposure, any of which could be used to calculate ROSI.
- 3.1.5 It is important for the enterprise to quantify risks mitigated to justify ROSI. Under normal circumstances, security solutions do not directly create any tangible value, rather they prevent loss. A loss prevented may be a loss that is unknown to the enterprise. For example, an enterprise's intrusion detection system (IDS) might show 20 successful break-ins last year to only 10 this year. Is it due to the new security solution implemented or were there less hackers attacking the network?

Figure 4—Productivity Loss Due to Security Solutions	
Problem	Average Downtime (in Minutes)
Application and system crashes	10
Bandwidth efficiency and throughput	10
Over-restrictive security policies	10
Enforcement of security policies	10
System-related roll outs and upgrades from IT	10
Security patches for operating systems and applications	10
Trouble downloading files due to virus scanning	10
Compatibility issues—hardware and software	15
Security problems due to too many passwords/permissions	15
Source: Sonnenreich, Wes; 'Return on Security Investment (ROSI): A Practical Quantitative Model', <i>Journal of Research and Practice in Information Technology</i> , vol., 38, no. 1, February 2006, a publication of the Australian Computer Society, Australia, 2006	

- 3.1.6 It is also important that enterprises capture the damage resulting from failures of security solutions to arrive at a correct ROSI. Security solutions do not work in isolation; the existence and effectiveness of other solutions have a major impact on the performance of the security solution. The most effective security solutions used are rarely implemented due to an unacceptable impact on productivity. **Figure 4** shows productivity loss resulting from implementing security solutions.
- 3.1.7 IT audit and assurance professionals should consider the fact that the cost of the security solution must include the impact of the solution on productivity, since more often than not this number is large enough to make or break the viability of the proposed solution. Security solutions become less effective over time as hackers find ways to work around them and create new risks. Therefore, it is important that the

enterprise has a system for regular assessment of the security solution performance. IT audit and assurance professionals should review such assessment reports and action undertaken thereon.

- 3.1.8** Apart from the initial design and deployment of the security solution, it is equally essential that enterprises have a good process for managing the implemented solution and realise that security is a dynamic exercise. For example, the IDS needs to be updated at frequent intervals with new ‘signatures’, security policies must be regularly reviewed and evaluated, software patches must be regularly updated and installed, and firewalls must be adjusted to reflect growth and changes in the IT infrastructure. IT audit and assurance professionals should review the sustenance plan of the implemented security solution.
- 3.1.9** IT audit and assurance professionals should also recognise the challenges enterprises face in effectively implementing security solutions, such as:
- Availability of skilled manpower
 - Retaining trained manpower
 - Monitoring security performance 24x7
 - Updating for the latest attacks, vulnerabilities, patches, technology advancements, upgrades and security solutions

4. CONSIDERATIONS

4.1 Audit

4.1.1 There are various ROSI models and there is no one model that fits all enterprises. Applicability of a model varies from enterprise to enterprise and depends upon various considerations, such as:

- Degree of exposure
- Nature of vulnerabilities
- Type of hazard
- Absence/weakness of compensating controls
- Geographical location—threat of external factors, such as war, vagaries of nature and such other uncontrollable events

4.1.2 Enterprises must have a well-defined process of data collection for security breaches and lapses. Data capture must not be restricted to events happening within the enterprise and should be extended beyond its regime giving due considerations to:

- Nature/type of business
- Business model (business to business, business to consumer, etc.)
- Critical business functions governed by IT
- Competitors and similar industry’s strategy toward IT security

Such data are processed and appropriately analysed, and the result is reviewed by top management.

4.1.3 Security investments are made after proper analyses of security requirements, risk assessments, product performance, vendor service level agreement and, most importantly, alignment of the security plan to the overall business objectives.

4.1.4 No security is complete without adequate insurance. The enterprise should be adequately protected by appropriate insurance

4.1.5 Security must be considered as a business protector and enabler not as an inhibitor. Justifying the cost of security is a matter of ensuring that the technology will enable that business, security policies and procedures align directly with business goals, and that managing and maintaining security technology results in the maximum value of the investment in security.

4.1.6 Trust is the highest form of security. The enterprise should be evolving into a ‘trusted enterprise’ by partnering with key stakeholders to protect the enterprise’s assets and proactively provide early warnings whenever breaches are anticipated.

4.1.7 Security policies and procedures should comply with applicable statutory and regulatory requirements.

5. EFFECTIVE DATE

5.1 This guideline is effective for all information systems audits beginning on or after 1 May 2010.

APPENDIX

Examples

A1. Example using $ROSI = \frac{(\text{Risk exposure} * \% \text{ Risk mitigated}) - \text{Cost of security investment}}{\text{Cost of security investment}}$

Company A has had virus attacks previously. It estimates that its average cost of damage and loss of productivity due to virus attacks is US \$25,000. Currently, Company A gets four attacks per year and expects to stop three of the four attacks by implementing a virus scanner solution costing US \$25,000. ROSI is calculated in the following example:

Risk exposure: US \$25,000 per exposure x 4 exposures in a year = US \$100,000

Risk mitigated by the solution: 3 attacks out of 4 attacks, i.e., 75%

Cost of security investment = US \$25,000

$$ROSI = \frac{(\text{US } \$100,000 * 75\%) - \text{US } \$25,000}{\text{US } \$25,000} = 200\%$$

In the example, it appears it is worth the investment on security. However, there are various assumptions and, therefore, the reality may be different. For example, what if, of the three attacks mitigated, each cost US \$5,000 whereas the fourth attack cost US \$85,000. The average would be US \$25,000; however, the fourth attack would be a costly attack.

A2. Example using $ROSI = R - ALE$, where $ALE = (R - E) + T$, i.e., $ROSI = E - T$.

Company A installs secure web servers to protect its business transactions over the Internet. The cost of the web server is US \$100,000. The company estimates its annual cost to recover, based on three major intrusions it had in the past, as US \$500,000, and the estimated savings gained by installing the web server as US \$250,000. In this example:

- $ALE = (\$500,000 - \$250,000) + \$100,000 = \$350,000$

- $ROSI = \$500,000 - \$350,000 = \$150,000$

References

Gordon, Lawrence A.; Martin P. Loeb; *The Economics of Information Security Investment*, ACM Transactions on Information and System Security, November 2002, p. 438-457

Matsuura, Kanta; *Information Security and Economics in Computer Networks: An interdisciplinary Survey and a proposal of Integrated Optimization of Investment*, Institute of Industrial Science, University of Tokyo, Japan, 2003

National Institute of Standards and Technology (NIST), *Security Metrics Guide for Information Technology Systems*, USA, 2003

Sonnenreich, Wes; 'Return on Security Investment (ROSI): A Practical Quantitative Model', *Journal of Research and Practice in Information Technology*, vol., 38, no. 1, February 2006, a publication of the Australian Computer Society, Australia, 2006

2009-2010 Professional Standards Committee

Chair, John Ho Chi, CISA, CISM, CBCP, CFE	Ernst & Young LLP, Singapore
Manuel Aceves, CISA, CISM, CGEIT	Cerberian Consulting, Mexico
Xavier Jude Corray, CISA, MACSc	Allsecure-IT Pty., Ltd., Australia
Murari Kalyanaramani, CISA, CISM, CISSP	British American Tobacco GSD, Malaysia
John G. Ott, CISA, CPA	AmerisourceBergen, USA
Edward J. Pelcher, CISA, CGEIT	Office of the Auditor General, South Africa
Rao Hulgeri Raghavendra, CISA, CQA, PGDIM	Oracle Financial Services Software Ltd., India
Elizabeth M. Ryan, CISA	Deloitte & Touche LLP, USA
Meera Venkatesh, CISM, CISA, ACS, CISSP, CWA	Microsoft Corp., USA

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Telephone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: standards@isaca.org
Web site: www.isaca.org