Critical Elements of Information Security Program Success
Critical Elements of Information Security Program Success

Information Systems Audit and Control Association®
With more than 50,000 members in more than 140 countries, the Information Systems Audit and Control Association (ISACA®) (www.isaca.org) is a recognized worldwide leader in IT governance, control, security and assurance. Founded in 1969, ISACA sponsors international conferences, publishes the Information Systems Control Journal®, develops international information systems auditing and control standards, and administers the globally respected Certified Information Systems Auditor™ (CISA®) designation, earned by more than 44,000 professionals since inception, and the Certified Information Security Manager® (CISM®) designation, a groundbreaking credential earned by 5,500 professionals since its inception.

Disclaimer
The Information Systems Audit and Control Association (the “Owner”) has designed and created this publication, titled Critical Elements of Information Security Program Success (the “Work”), primarily as an educational resource for chief information officers, senior management and IT management. The Owner makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of any proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, the chief information officers, senior management and IT management should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

Disclosure
Copyright © 2005 by the Information Systems Audit and Control Association. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system, or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise), without the prior written authorization of the Information Systems Audit and Control Association. Reproduction of selections of this publication, for internal and noncommercial or academic use only, is permitted and must include full attribution of the material’s source. No other right or permission is granted with respect to this work.

Information Systems Audit and Control Association
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: research@isaca.org
Web site: www.isaca.org

Critical Elements of Information Security Program Success
Printed in the United States of America
Acknowledgments

From the Publisher
The Information Systems Audit and Control Association wishes to recognize:

The ISACA Board of Directors
Everett C. Johnson, CPA, Deloitte & Touche LLP (retired), USA, International President
Abdul Hamid Bin Abdullah, CISA, CPA, Auditor General’s Office, Singapore, Vice President
William C. Boni, CISM, Motorola, USA, Vice President
Jean-Louis Leignel, MAGE Conseil, France, Vice President
Lucio Augusto Molina Focazzio, CISA, Colombia, Vice President
Howard Nicholson, CISA, City of Salisbury, Australia, Vice President
Bent Poulsen, CISA, CISM, VP Securities Services, Denmark, Vice President
Frank Y am, CISA, CIA, CCP, CFE, CFSA, FFA, FHKCS, Focus Strategic Group,
Hong Kong, Vice President
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA,
Past International President
Robert S. Roussey, CPA, University of Southern California, USA, Past International President

The Author and Focus Group
Sharon O’Bryan, CISA, CISSP, Author, OAS Inc., USA
Randy Caraway, CISM, CISSP, PMP, JP Morgan Chase, USA
Claudio Cilli, Ph.D., CISA, CISM, CISSP, Tangerine Consulting, Italy
Milthon Chavez, CISA, CISM, CIFI, Centro Empresarial Sabana Grande, Venezuela
Michel Lambert, CISA, CISM, Commission Administrative des Regimes de Retraite
et d’Assurance Quebec, Canada
Yves Le Roux, CISM, CISSP, Computer Associates, France
Itamar Mor, CISM, MPA, Comsec Consulting, Israel
Takuya Morita, CISA, CISM, CIA, Sumitomo Mitsui Banking Corporation, Japan
Michael Roberti, CISM, CISSP, GSEC, Harris Corporation, USA
Rolf von Roessing, CISA, CISM, CISSP, FBCI, KPMG, Germany
Ken Shaurette, CISA, CISM, CISSP, NSA-IAM, MPC LLC, USA

CISM Certification Board
David Simpson, CISA, CISM, CISSP, Chair, CQR Consulting, Australia
Kent Anderson, CISM, Network Risk Management LLC, USA
Evelyn Anton, CISA, CISM, UTE, Uruguay
Claudio Cilli, CISA, CISM, CIA, CISSP, Tangerine Consulting, Italy
Robert Coles, CISA, CISM, MBCS, UK
Ms. Kyung-Hee Oh, CISA, CISM, CISSP, Green Soft, Korea
Hitoshi Ota, CISA, CISM, Mizuho Corporate Bank Ltd., Japan
Ashok Pawar, CISA, CISM, CAIIB, State Bank of India, India
Gary Swindon, CISM, Orlando Regional Healthcare, USA
# Table of Contents

ACKNOWLEDGMENTS .................................................................3

EXECUTIVE SUMMARY ..........................................................5

PROJECT GOALS ......................................................................7

INTRODUCTION .........................................................................8

CRITICAL ELEMENTS ............................................................9
  Priority Critical Elements and Solution Considerations ...................10
  Additional Critical Elements and Solution Considerations .............13

SUMMARY ................................................................................18

APPENDIX A—CRITICAL ELEMENTS MASTER LIST
  BY CATEGORY ........................................................................19

APPENDIX B—PRIORITY CRITICAL ELEMENTS
  SUMMARY TABLE ....................................................................21
The challenges of implementing an effective information security program are broad and diverse. To address these challenges the Information Systems Audit and Control Association (ISACA) sponsored an international focus group and survey, which resulted in this report, to identify the elements that impact information security program success.

The 10-person focus group consisted of information security management specialists from business, government and consulting, drawn from eight countries, including Canada, France, Germany, Israel, Italy, Japan, the United States and Venezuela. While this representation does not include all ISACA membership, it does draw upon diverse and incisive experience.

The responding survey group included 157 representatives from financial services, transportation, retail/wholesale, government (national, state and local), manufacturing, utilities, healthcare and consulting. The respondents’ geographical representation included Africa, the Americas, Asia, Europe and Oceania. Organization size was equally well represented within the survey group by respondent organizations ranging from “fewer than 50 employees” to “more than 50,000 employees.”

The process, in brief, included the development of a comprehensive critical elements list that was used by the focus and survey groups to select the top 10 elements critical for the success of information security programs. The results were compelling.

The focus group and the survey group independently identified senior management’s commitment to information security initiatives as the number one critical element impacting an information security program’s success. Both groups also consistently identified five additional critical elements in the top 10, including:

- Management’s understanding of information security issues
- Information security planning prior to the implementation of new technologies
- Integration between business and information security
- Alignment of information security with the organization’s objectives
- Executive and line management ownership and accountability for implementing, monitoring and reporting on information security

The remaining four critical elements making up the target top 10 of each group differed.
The subsequent sections of this report provide particulars associated with the identified critical elements in addition to solution considerations developed by the focus group. The critical elements have been divided into two categories: priority critical elements, which represent the six elements that were among the top 10 selected by both groups, and additional critical elements, which represent the remaining four elements that differed between the two groups. Each priority critical element is followed by three solution considerations for use by information security managers and business colleagues as thought-provoking ideas or action items.

The solution considerations identified for the six priority critical elements also help address a number of other critical elements, including all but one of the additional critical elements identified by the focus and survey groups. The additional critical elements identified by the groups are:

- Appropriate employee education and awareness on information asset protection
- Consistent enforcement of information security policies and standards
- Placement of information security within the organization hierarchy
- Budget for information security strategy and tactical plan
- Consistent board/executive management message with regard to information security priorities
- Focus on short-term goals resulting in long-term control weaknesses
- Ability to cost-justify information security
- Generally accepted information security best practices/metrics

In summary, the analysis clearly points to the need for executive and senior management and the information security manager to forge a relationship that enables a consistent message with regard to the priority the organization places on protecting valuable information and intellectual property assets. However, the analysis also points to the strong need for the message to be backed up with visible and consistent action. That action, say the results, is the establishment and consistent implementation of company policies and standards. Furthermore, the results indicate that without the highest level visibly monitoring the successful implementation of an information security strategy, inconsistent compliance will continue to erode progress and give false comfort regarding the asset protection. Day-to-day priority conflicts continue to affect the quality and consistency of information asset protection. To ensure that associated risks are taken seriously by every employee and agent of the organization, executive and senior management must become visibly interested in ensuring the information security program’s success within their organizations.
Project Goals

While many publications address technical risks and security concerns, few reports have identified, in a comprehensive manner, the wider aspect of success barriers that face information security managers and proposed potential solutions to those barriers. ISACA recognizes that the barriers that must be overcome by security managers and their business unit counterparts go beyond technical and regulatory compliance risks and include: organizational culture and relationships, budget, human resources, education and awareness, and outsourcing, to name a few. Through ISACA’s project sponsorship to facilitate the identification, analysis and this report, an important tool has been created to position for success the information security management programs and the organizations for which these programs are a part.

There are infinite analysis and focus opportunities concerning information security; therefore, the project goals were carefully outlined and include:

• Provide information security managers a peer perspective of critical elements to achieve a successful information security program implementation.
• Provide suggestions on solving, rather than simply stating, issues.
• Provide a report that can serve executive and senior management as well as information security managers.

Although the detailed results of this project are primarily intended for information security managers, the project objectives and results have been summarized in the Executive Summary to enable key information in this report to be shared with executive and senior management.
Introduction

This report reflects the experience and opinions of a diverse professional group regarding critical elements of information security program success. The participants included 10-person focus group and a 157-respondent survey group.

Both groups provided broad representation in terms of country, industry and size of organization. The focus group consisted of information security management specialists from business, government and consulting drawn from eight countries, including Canada, France, Germany, Israel, Italy, Japan, the United States and Venezuela. The survey group industry and country representation is depicted in figure 1.

Survey respondents were equally diverse in professional positions held, including C-level executives, senior management, information security managers, information security staff, research directors and consulting partners and staff.

<table>
<thead>
<tr>
<th>INDUSTRY REPRESENTATION</th>
<th>% TOTAL</th>
<th>COUNTRY REPRESENTATION</th>
<th>% TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Services</td>
<td>14.89%</td>
<td>Africa</td>
<td>1.42%</td>
</tr>
<tr>
<td>Transportation</td>
<td>2.13%</td>
<td>Asia</td>
<td>9.22%</td>
</tr>
<tr>
<td>Retail/Wholesale</td>
<td>0.71%</td>
<td>Europe</td>
<td>25.53%</td>
</tr>
<tr>
<td>Government</td>
<td>15.60%</td>
<td>North America</td>
<td>58.15%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>6.38%</td>
<td>South and Central America</td>
<td>3.55%</td>
</tr>
<tr>
<td>Utilities</td>
<td>4.26%</td>
<td>Oceania</td>
<td>2.13%</td>
</tr>
<tr>
<td>Healthcare/Medical</td>
<td>2.84%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consulting</td>
<td>39.01%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Services</td>
<td>14.18%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The critical elements are presented in two distinct subsections of this report: priority critical elements and additional critical elements.

The initial list of more than 70 elements was developed through a two-day focus group facilitated session. From that list, 35 elements\(^1\) were selected to represent the population from which each individual in the focus group and survey group (the groups) would identify the top 10. This selection process resulted in two distinct subcategories, priority critical elements and additional critical elements, with the priority critical elements representing six elements that both groups identified within their top 10 selections. Additional critical elements represent the remaining four elements from each group that were voted in the top 10 but differed between the focus group and survey group.

A key goal and differentiator of this report is to offer potential solutions. To accomplish this goal, yet keep the report focused, the number of solution considerations has been limited to three for each of the priority elements. Solution details will vary from organization to organization as well as from country to country. While the solution considerations presented in this report may be pertinent to some organizations, for others they are provided as thought-provoking ideas.

It is important to note that each organization should frame the information presented in this report within the context of its unique information security program requirements. The priority critical elements are:

- Senior management commitment to information security initiatives
- Management understanding of information security issues
- Information security planning prior to implementation of new technologies
- Integration between business and information security
- Alignment of information security with the organization’s objectives
- Executive and line management ownership and accountability for implementing, monitoring and reporting on information security

The additional critical elements are:

- Appropriate employee education and awareness on information asset protection
- Consistent enforcement of information security policies and standards
- Placement of information security within the organization hierarchy
- Budget for information security strategy and tactical plan
- Consistent board/executive management message with regard to information security priorities
- Focus on short-term goals resulting in long-term control weaknesses
- Ability to cost-justify information security
- Generally accepted information security best practices/metrics

\(^{1}\) Master list of elements, see Appendix A for additional information.
Priority Critical Elements and Solution Considerations

**Senior Management Commitment to Information Security Initiatives**

Senior management commitment is required of all enterprise and strategic initiatives; therefore, information security is part of a long list of projects and initiatives that must have senior and executive management commitment. Without commitment, these projects and initiatives would not be active. However, employees are faced with conflicting priorities on a day-to-day basis and, therefore, focus their efforts on those things that affect their performance evaluation and positively influence the reward system associated with their performance. As a result, that which is monitored by senior and executive management should be incorporated into the performance/reward system and, therefore, be successfully implemented.

Solution considerations should include the following:

- Senior management should require that all requests for technology expenditures include technology risk identification and risk mitigation requirements as part of the cost-benefit analysis, project objectives, deliverables and funding request.
- Senior management should communicate consistently that every employee is accountable for information security by ensuring that expectations are clearly communicated in the company’s information security policies and standards, and consistently demonstrate that violations will not be tolerated.
- Every employee, including management, should be required to attend an information security awareness update annually and new employees should be appropriately informed of the company’s information security concepts and practices.

**Management Understanding of Information Security Issues**

Establishing understanding of information security issues requires effective communication about the business risks that result from inappropriately designed and omitted technology risk management controls. Information security is one key aspect of technology risk management and the information security manager must be skilled at tying business risk to information security risk and expressing the risks at every management level within the organization. It is also necessary that each management level understand these risks and actively participate in ensuring that proper risk management solutions are identified and implemented in the most efficient and effective manner. Priority conflicts, lack of accountability and inadequate business communication skills of information security managers are all partially responsible for failure to improve management’s understanding of information security solutions that help ensure the confidentiality, integrity and availability of company information and intellectual property assets.
Solution considerations should include the following:
  • Information security managers must increase their understanding of the business and their skills in communication through industry-specific education and executive-level continuing education programs.
  • Information security awareness sessions should start at the executive level and hierarchically proceed to the inclusion of all levels of management and employees.
  • Information security managers should seek industry and other publications that target executive and senior management and ensure that those publications are made available to the management team.

**Information Security Planning Prior to Implementation of New Technologies**

Information security is a necessary component of corporate governance assurance. Whether the company is regulated, publicly held, large or small, the integrity of the financial statements relies on properly implemented information security programs. Technology implementation without incorporating proper controls undermines investment in information security and can cause damage to data and processing integrity that may go unnoticed until damage far exceeds the company’s risk threshold.

Solution considerations should include the following:
  • The company’s policies and standards must require review and formal authorization of changes to the technology environment prior to implementation. The designation of authority to provide such authorization should be a management position, without separation of duties conflicts, and include the responsibility of reporting the status of information security to the board.
  • Exceptions to the company’s policies and standards with regard to change management should be formally requested and approved by the company’s policy oversight committee or equivalent.
  • The information security manager and the audit manager should work closely to monitor the environment for technology implementations that do not meet the requirements of the company’s policies and standards.

**Integration Between Business and Information Security**

While certain aspects of an information security program follow a shared services model, most information security initiatives must be closely aligned with the underlying business initiatives they protect. However, the cost of protecting information and intellectual assets should not exceed the value of the assets. To properly align business risks and information security solutions, a cooperative dialogue between business areas and information security experts is necessary.
Critical Elements of Information Security Program Success

Each aspect of technology risk must be appropriately analyzed, including the risk to confidentiality, integrity and availability as it pertains to the entire transaction flow. Furthermore, the focus of this analysis should be on business transactions that are material to the business financials, require compliance with laws and regulations, and could negatively affect the company’s reputation.

Solution considerations should include the following:
• Senior management should ensure that business liaisons are held accountable for interacting with the information security manager to achieve mutually agreeable risk management objectives.
• Senior management should ensure that the business strategy is shared with information technology and appropriate risk management groups, such as information security. This will help ensure that necessary adjustments to the information security strategy and technology infrastructure capability can be proactively planned to help manage cost and risk.
• The information security status associated with high-risk legal and regulatory compliance should be monitored at the executive level to ensure that appropriate priority is given to risk management initiatives.

Alignment of Information Security With the Organization’s Objectives
Information security is frequently perceived as the responsibility of the information security department. This perception is generally perpetuated through information security initiatives being funded as stand-alone projects and the failure to inform employees of their role in the protection of information and intellectual property assets. For many companies, this is a cultural change and must be driven from the top. While cultural change requires a long-term commitment and is slow to realize, it is generally effectively started with the development of pertinent strategy statements and supporting management action requirements.

Solution considerations should include the following:
• An information security strategy that is aligned with the company’s risk management and corporate governance requirements should be developed and implemented.
• Each line of business that “owns” information requiring specific levels of confidentiality, integrity and availability should designate a liaison to work with the information security manager to ensure that requirements are properly reflected and prioritized in the information security strategy.
• Measurements of control effectiveness should include alignment with regulations and laws and those measurements should be reported to the board on a quarterly and annual basis through, or with, the chief legal counsel, chief compliance officer, and chief auditor or their equivalents.
Executive and Line Management Ownership and Accountability for Implementing, Monitoring and Reporting on Information Security

Failure to support and implement information security initiatives is frequently a matter of conflicting priorities. Conflicting priorities and ownership of process are generally resolved through the company’s system of performance rewards. That said, performance goals associated with information security must be reasonable and support, not hinder, business processes. Priorities must be clearly set and established in the security strategy with key performance indicators approved by the highest level of the organization to help ensure that the goals will be effectively and consistently managed, monitored and executed.

Solution considerations should include the following:
- Information security should have an independent reporting structure to ensure that concerns, accomplishments and views on governance are properly represented to those ultimately responsible to the stakeholders.
- Pertinent key control objectives should be incorporated into the performance measurement process for all employees.
- Appropriate levels of management should have responsibility for ensuring that information security violation, authorization exceptions and other pertinent security measurements associated with their line of business processes are researched and acted upon on their behalf.

Additional Critical Elements and Solution Considerations

As noted in the introduction section of this report, the process of identifying the top 10 elements included results from a focus group and survey group. The results fell into two distinct subcategories—priority critical elements and additional critical elements, with the additional critical elements representing the four elements from each group not reflected in the priority critical elements.

While each of the additional critical elements stand alone as unique requisites for successfully implementing a viable information security program, all of the elements in this category, with the exception of generally accepted information security best practices/metrics, are reasonably addressed by the solutions presented for the priority critical elements. Therefore, the additional critical elements are presented in table format (see figure 2) to align the element, the solution considerations and the priority element from which the solution considerations have been taken. The solution considerations have been limited to three, as were the priority elements, with the objective of keeping the report on focus.
<table>
<thead>
<tr>
<th>Additional Critical Element</th>
<th>Solution Considerations</th>
<th>Solution Consideration Drawn From Priority Critical Elements</th>
</tr>
</thead>
</table>
| Appropriate employee education and awareness on information asset protection | • Every employee should be required to attend an information security awareness update annually and new employees should be appropriately informed of the company’s information security concepts and practices.  
• Senior management should communicate consistently that every employee is accountable for information security by ensuring that expectations are clearly communicated in company information security policies and standards, and consistently demonstrate that violations will not be tolerated.  
• Senior management should ensure that business liaisons are held accountable for interacting with the information security manager to achieve mutually agreeable risk management objectives. | Senior management commitment to information security initiatives |
| Consistent enforcement of information security policies and standards | • The company’s policies and standards must require review and formal authorization of changes to the technology environment prior to implementation. The designation of authority to provide such authorization should be of management position, without separation of duties conflicts, and responsible for reporting the status of information security to the board.  
• Exceptions to the company’s policies and standards with regard to change management should be formally requested and approved by the company’s policy oversight committee or equivalent.  
• Measurements of control effectiveness should include alignment with regulation and law and those measurements should be reported to the board on a quarterly and annual basis through, or with, the chief legal counsel, chief compliance officer, and chief auditor or their equivalents. | Information security planning prior to the implementation of new technologies |

Alignment of information security with the organization’s objectives
<table>
<thead>
<tr>
<th>Additional Critical Element</th>
<th>Solution Considerations</th>
<th>Solution Consideration Drawn From Priority Critical Elements</th>
</tr>
</thead>
</table>
| Placement of information security within the organization hierarchy | • Information security managers must increase their understanding of the business and their skills in communication through industry-specific education and executive-level continuing education programs.  
• The information security status associated with high-risk legal and regulatory compliance should be monitored at the executive level to ensure that appropriate priority is given to risk management initiatives.  
• Information security should have an independent reporting structure to ensure that concerns, accomplishments and views on governance are properly represented to those ultimately responsible to the stakeholders. | Management understanding of information security issues  
Integration between business and information security  
Executive and line management ownership and accountability for implementing, monitoring and reporting on information security |
| Budget for information security strategy and tactical plan      | • Senior management should require that all requests for technology solution expenditures include technology risk identification and risk mitigation requirements as part of the cost-benefit analysis, project objectives, deliverables and funding request.  
• An information security strategy that is aligned with the company’s risk management and corporate governance requirements should be developed and implemented.  
• Each line of business that “owns” information requiring specific levels of confidentiality, integrity and availability should designate a liaison to work with the information security manager to ensure that requirements are properly reflected and prioritized in the information security strategy. | Senior management commitment to information security initiatives  
Alignment of information security with the organization’s objectives |
### Figure 2—Solution Considerations for Additional Critical Elements (cont.)

<table>
<thead>
<tr>
<th>Additional Critical Element</th>
<th>Solution Considerations</th>
<th>Solution Consideration Drawn From Priority Critical Elements</th>
</tr>
</thead>
</table>
| Consistent board/executive management message with regard to information security priorities | • Communicate consistently that every employee is accountable for information security by ensuring that expectations are clearly communicated in company information security policies and standards and consistently demonstrate that violations will not be tolerated.  
• Senior management should ensure that business liaisons are held accountable for interacting with the information security manager to achieve mutually agreeable risk management objectives.  
• Information security status associated with high-risk legal and regulatory compliance should be monitored at the executive level to ensure that appropriate priority is given to risk management initiatives. | Senior management commitment to information security initiatives  
Integration between business and information security  
Integration between business and information security |
| Focus on short-term goals resulting in long-term control weaknesses | • Senior management should require that all requests for technology solution expenditures include technology risk identification and risk mitigation requirements as part of the cost-benefit analysis, project objectives, deliverables and funding request.  
• Exceptions to the company’s policies and standards with regard to change management should be formally requested and approved by the company’s policy oversight committee or equivalent.  
• The information security manager and the audit manager should work closely to monitor the environment for technology implementations that do not meet the requirements of the company’s policies and standards. | Senior management commitment to information security initiatives  
Information security planning prior to implementation of new technologies |
<table>
<thead>
<tr>
<th>Additional Critical Element</th>
<th>Solution Considerations</th>
<th>Solution Consideration Drawn From Priority Critical Elements</th>
</tr>
</thead>
</table>
| Ability to cost-justify information security | • Senior management should require that all requests for technology solution expenditures include technology risk identification and risk mitigation requirements as part of the cost-benefit analysis, project objectives, deliverables and funding request.  
• An information security strategy that is aligned with the company’s risk management and corporate governance requirements should be developed and implemented.  
• Each line of business that “owns” information requiring specific levels of confidentiality, integrity and availability should designate a liaison to work with the information security manager to ensure that requirements are properly reflected and prioritized in the information security strategy. | Senior management commitment to information security initiatives  
Alignment of information security with the organization’s objectives |
| Generally accepted information security best practices/metrics | • The information security manager should participate in industry organizations that are actively working on developing metrics and practices that effectively balance business product development needs and risk management.  
• The information security manager should seek training in process management, such as ITIL.  
• The information security manager should work closely with line-of-business managers to ensure that measurements associated with information security tie to real business risks. | (Element is not addressed by solution considerations elsewhere defined.) |
Summary

The information contained in this report reflects a growing recognition that information security is not just an information technology problem; it is a business problem that cannot be addressed by simply hiring information security professionals and creating impressive titles. The ability to properly identify risks to information and intellectual property assets requires cooperation from participants across the entire organization.

Most important, however, is the need for executive and senior management to not only provide for the appropriate resources, but also to consistently support the tough decisions with regard to protecting those assets.

The results of the focus group and survey also indicate that without appropriately defined information security measurements, and board-level monitoring of those measurements, asset protection will continue to be trumped by “urgent” implementations that sidestep established policies, standards and procedures undermining the business technology infrastructure. Another key finding is that information security professionals are beginning to recognize that they need to develop a solid understanding of the business as their role becomes more visible in the organization, their decisions demand business risk justification, and the dependence on technology drives increased interaction with their legal and compliance counterparts in the organization.
Appendix A—Critical Elements Master List by Category

Culture
1. Board/executive management message with regard to information security priorities
2. Board/executive management monitoring of information security risks
3. Regular, ongoing information security items on the board agenda
4. Executive and line management ownership and accountability for implementing, monitoring and reporting on information security

Human Resources/People/Budget and Finance
5. Effective information security budgeting process
6. Budget for information security strategy and tactical plan

Organization/Organizational Relationships
7. Clearly communicated customer responsibilities and loss liability associated with the use of technology for customer transactions
8. Senior management commitment to information security initiatives
9. Management influence resulting in product/service selection that does not best solve the problem
10. Alignment between company objectives and security objectives
11. Integration between business and security
12. Defined management structure
13. Focus on short-term goals to prevent long-term security weaknesses
14. Information security appropriately defined with adequate visibility in the enterprise
15. Appropriate placement of security within the organization hierarchy
16. Integration of IT security with traditional/facility security

Technology and Technology-related Processes
17. Sufficient security planning prior to implementation of new technologies
18. Appropriate change management procedures
19. Ability to respond to spamming/phishing and related attacks
20. Balancing expectations with technical feasibility of automated solutions

Laws/Regulations/Governance/Policies and Standards
21. Compliance with multiple regulation jurisdictions along the transaction path
22. Appropriate/ineffective/conflicting legislation/regulation
23. Information security policies and standards enforcement
24. Consistent enforcement of information security policies and standards
Critical Elements of Information Security Program Success

Metrics
25. Enterprise risk management framework that integrates security
26. Universally agreed-upon methodology for risk assessment
27. Generally accepted security metrics for security best practices
28. Reporting and metrics tied to business goals and strategies

Training/Education/Awareness
29. Availability of trained and experienced information security professionals
30. Management understanding of security issues
31. Employee education, and education update, on information asset protection
32. Continuous security awareness
33. Knowledge of formal crime and incident reporting systems
34. Balanced user expectation vs. what is technically feasible
35. Pertinent education for security expert, i.e., continuing professional education (CPE)
### Appendix B—Priority Critical Elements Summary Table

<table>
<thead>
<tr>
<th>Critical Elements</th>
<th>Solution Considerations</th>
</tr>
</thead>
</table>
| Senior management commitment to information security initiatives | • Senior management should require that all requests for technology expenditures include technology risk identification and risk mitigation requirements as part of the cost-benefit analysis, project objectives, deliverables and funding request.  
• Senior management should communicate consistently that every employee is accountable for information security by ensuring that expectations are clearly communicated in the company’s information security policies and standards, and consistently demonstrate that violations will not be tolerated.  
• Every employee, including management, should be required to attend an information security awareness update annually and new employees should be appropriately informed of the company’s information security concepts and practices. |
| Management understanding of information security issues  | • Information security managers must increase their understanding of the business and their skills in communication through industry-specific education and executive-level continuing education programs.  
• Information security awareness sessions should start at the executive level and hierarchically proceed to the inclusion of all levels of management and employees.  
• Information security managers should seek industry and other publications that target executive and senior management and ensure that those publications are made available to the management team. |
| Information security planning prior to implementation of new technologies | • The company’s policies and standards must require review and formal authorization of changes to the technology environment prior to implementation. The designation of authority to provide such authorization should be a management position, without separation of duties conflicts, and include responsibility for reporting the status of information security to the board.  
• Exceptions to the company’s policies and standards with regard to change management should be formally requested and approved by the company’s policy oversight committee or equivalent.  
• The information security manager and the audit manager should work closely to monitor the environment for technology implementations that do not meet the requirements of the company’s policies and standards. |
### Priority Critical Elements Summary Table (cont.)

<table>
<thead>
<tr>
<th>Critical Elements</th>
<th>Solution Considerations</th>
</tr>
</thead>
</table>
| Integration between business and information security                            | • Senior management should ensure that business liaisons are held accountable for interacting with the information security manager to achieve mutually agreeable risk management objectives.  
• Senior management should ensure that the business strategy is shared with information technology and appropriate risk management groups, such as information security. This will help ensure that necessary adjustments to the information security strategy and technology infrastructure capability can be proactively planned to help manage cost and risk.  
• The information security status associated with high-risk legal and regulatory compliance should be monitored at the executive level to ensure that appropriate priority is given to risk management initiatives. |
| Alignment of information security with the organization’s objectives              | • An information security strategy that is aligned with the company’s risk management and corporate governance requirements should be developed and implemented.  
• Each line of business that “owns” information requiring specific levels of confidentiality, integrity and availability should designate a liaison to work with the information security manager to ensure that requirements are properly reflected and prioritized in the information security strategy.  
• Measurements of control effectiveness should include alignment with regulations and laws and those measurements should be reported to the board on a quarterly and annual basis through, or with, the chief legal counsel, chief compliance officer, and chief auditor or their equivalents. |
| Executive and line management ownership and accountability for implementing, monitoring and reporting on information security | • Information security should have an independent reporting structure to ensure that concerns, accomplishments and views on governance are properly represented to those ultimately responsible to the stakeholders.  
• Pertinent key control objectives should be incorporated into the performance measurement process for all employees.  
• Appropriate levels of management should have responsibility for ensuring that information security violation, authorization exceptions and other pertinent security measurements associated with their line of business processes are researched and acted upon on their behalf. |