

Other nonfinancial factors as well as factors such as the land donation, potential payment of additional county taxes, tax rebates and incentives, donation to develop certain green technology or environmental offsets (hybrid buses, parks, and the like) were outside the purview of this financial analysis, but are nonetheless important aspects in the negotiations.

### **Project Update**

On January 29, 2009, the State Lands Commission voted down the project two (Lt. Governor Garamendi and State Controller John Chiang) against one (Deputy Finance Director Tom Sheehy). As of writing this case study, PXP has appealed to the State Legislature to get the State Lands Commission's vote overturned.

### **CASE STUDY: HOW REAL OPTIONS MITIGATES IT ENTERPRISE SECURITY RISKS**

*This case was written by David M. Bittlingmeier (david@bittlingmeier.com). David has a B.S. from St. Mary's College and an M.S. from Golden Gate University, and has numerous years in strategic enterprise security, designing, developing, and implementing various enterprise policies and procedures, enterprise-wide security awareness training, business continuity, project management, and technical consultation experience, where he has provided professional judgments and advice to all levels of management. As a consultant, he has worked on ensuring compliance with industry best practices, business continuity, disaster recovery planning, ISO 17799, NIST standards, OCC, Basel II, BITS regulation, and has offered enterprise security management perspective for executives seeking an unbiased source of education, insight, and expertise in order to ensure the success of their business. In addition, he has consulted with (ISC)2, where he was both part of the team that developed/modified the training to prepare security professionals for the CISSP exam and then was/is a supervisor during the CISSP exams, wrote the strategic security plan for one of the major departments of the State of California, speaks at International Enterprise Security Conferences, is an ongoing attendee of the U.S. Secret Service San Francisco Electronic Crimes Task Force, was a contributor of Risk Analysis: 1st Step in HIPAA Security publication, as well as being a member of the High Technology Crime Investigation Association, Inc. David has received praise for his ability to explain complexity in lay terms from various sources such as San Francisco Mayor's Criminal Justice Council, California Youth Authority, and others.*

This case study provides a quick overview of IT Enterprise Risk Management analysis drawn from numerous local, national, and international security reviews he has completed, including, yet not necessarily limited to, third-party service companies, mail services, various outsourcing functions/processes, venture capitalist projects, insurance companies, financial companies, and so forth from multimillion to multibillion dollar organizations, and as such the case study is an illustration of those robust review processes. Within the case study is a short composite case with a sample report that outlines both issues and possible solutions. Finally, adding the strategic real options and integrated risk analysis such as applying Monte Carlo risk simulations offer solutions to the effective allocation of major funds on enterprise security projects. While the benefits of IT are clear, managing the risks that can be introduced to the business from IT processes, policies, and technology failures are not easily inferred and yet these risks can have serious impacts in terms of achieving compliance with:

- Regulations
- Protecting brand reputation
- Ensuring overall corporate performance

The process introduced in this case study is the Risk Assessment Process (RAP) process, which helps facilitate excellence in governance by aligning:

- IT policy, risk, and operations management
- Corporate business initiatives
- Strategy
- Operational standards
- Enterprise security

RAP is a comprehensive solution that reduces the cost, complexity, and cumbersome nature of complying with numerous regulatory mandates. RAP facilitates the ongoing review, attestation, and remediation process, while helping to identify similarities between regulations to reduce redundancy and duplication of effort and provides the confidence that compliance is achievable, risks are mitigated, and corporate policies and procedures are enforced. As regulatory pressures continue to mount, businesses that take a more practical, cross-regulatory approach to managing compliance will alleviate increasing cost and complexity while gaining valuable insight into risks to key business processes that could affect the company's performance in the form of legal action, fines, penalties, and damage to a company's reputation.

Enterprise Security Risk Management is a complex and difficult problem that can be made efficient and manageable through RAP's consolidation,

identification, and harmonization of overlapping regulatory demands—interdependencies that cannot be seen using spreadsheets—and enables transparency and visibility to stakeholders throughout the organization. The process ensures that risks are properly associated to business strategy and needs while it helps to manage a multitude of technology risks. Such processes have become increasingly more difficult and require a holistic approach wherein the interdependencies between risk and business performance are easily understood and manageable. For example, currently organizations in general have had to rely on a fragmented and disparate approach to managing supplier risks. Reliance on a silo risk management approach is not only costly and inefficient, it lacks the contextual understanding of the real impacts that risk in technology processes and policies have on the business.

In today's highly regulated business environment, companies are required to comply with a multitude of global regulatory mandates, including privacy, industry, and process regulations. Regardless of a company's current compliance environment, similarities across regulations create overlapping management, documentation, and audit demands, which can overwhelm efforts to effectively identify and manage risk. RAP makes governance practicable, enabling a company to sustain compliance across multiple best practice frameworks and regulations while managing IT control and risk according to the business processes they support. With RAP, a company will instill risk management and governance as part of the corporate culture, making procedures more effective and efficient while providing management with peace of mind that the corporate brand is protected, providing management with the visibility, control, and decision support required to manage supplier risk and optimize business performance. RAP is a key building block in implementing an enterprise-wide security risk management approach as it delivers a policy-driven, process-centric way to manage risk through:

- Control assessments
- User surveys
- Logical and repeatable workflow
- Industry standard best practices criteria

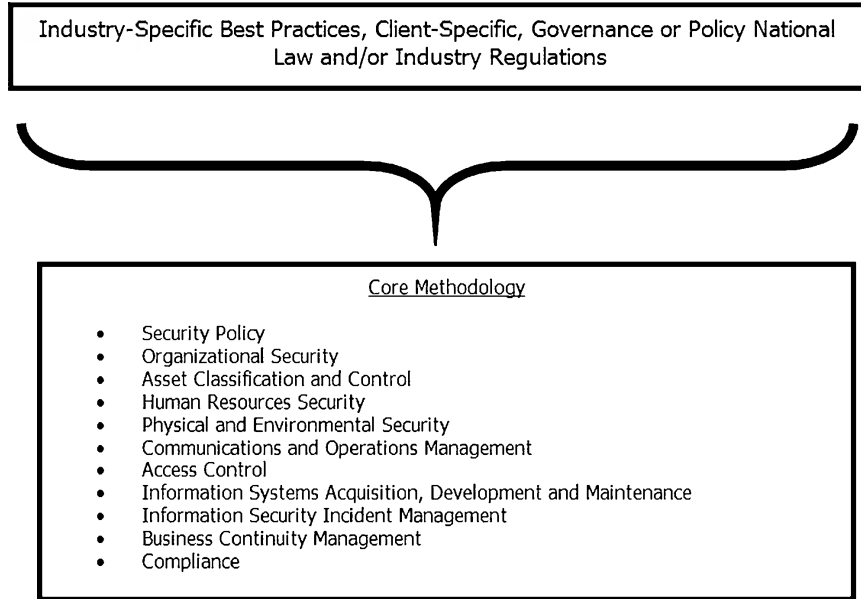
We are able to apply Risk Simulator input assumptions to both BAROV and Client Company's subject matter expert risk rankings, and then run simulations on the matrices in order to determine the total grand risk score for the Client Company (see Figure 14.77). Furthermore, we are able to develop optimization models where each element may be subject to a decision variable in terms of the cost required to correct any outstanding issues, compared to possible benefits/losses obtained from having/not having an "in compliance" security level, and run it based on the Client Company's budget

constraints. Using probabilistic distributions obtained from the simulation(s), we are now able to identify the chances that a specific category's risk and impact may exceed tolerable limits, as well as identify the critical success factors (sensitivity analysis and Tornado analysis are usually run on these assessment matrices). A strategy is then created of multiple phases (sequential compound option) on when certain elements of the issue(s) identified can/need(s) to be first to be fixed, when it/they then becomes the less/more critical in other phase(s), all the while were so warranted accounting for interrelationships among any/all Enterprise projects. For example, if a certain project requires another as a prerequisite (say some platform technology that first needs to be implemented before any subsequent projects can be implemented) or any mutually exclusive redundant projects (the implementation of one project makes another obsolete or unnecessary). At the end of the day, at what point does not stopping project A become cost effective and/or project B becoming cost-effective or ending project A completely or moving toward project B become the best and optimal overall strategy? As most companies have hundreds of these projects, BAROV could demonstrate both the dependency and the costs between projects, thereby giving a pragmatic real-world risk of project A versus project B, and so forth.

Based on a company's business objectives, the inherent risks associated will determine the tier ranking system using a value of 1 to 5 Likert scale (the scale can also be color-coordinated such as: 1 = Green, 2 = Yellow, 3 = Orange, 4 = Red, 5 = Black), indicating the level of risk involved, from low to high. In general, compliance reviews dictate that formal reviews must be conducted on at least an annual basis, and more frequently if warranted based on risk. Using a pragmatic, real-world-based stance in conducting reviews we understand how policy, procedures, and management controls mitigate risk. Based on a comprehensive and customizable risk-assessment approach, this RAP methodology can be used across multiple industries and functions. It can be used as the basis for performing up-front due-diligence, a one-time controls review, or an annual assessment of controls and/or best practices (Figure 14.74 illustrates this compliance core methodology).

### **A Sample Implementation**

This sample implementation is derived from extensive on-site reviews (companies' names and proprietary information are intentionally kept confidential and we only present a generic example case) in the United States, India, and China, of due-diligence reviews across numerous industries including yet not limited to financial services, insurance companies, onshore/offshore IT service providers, manufacturing, and other functional areas for compliance issues in general, while specifically reviewing Enterprise Security of internal,



**FIGURE 14.74** Assurance of compliance with legal requirements.

external, outsourced, and offshore service security, highlighting the needs for BAROV methodologies to ensure enterprise security that meets or exceeds industry-standard security practices that are cost-effective, robust, functionally effective, and real time. Information systems are designed and deployed to support business and legal requirements, leverage cost efficiencies, and improve internal and external communication. However, organizations, like the people they are designed to serve, are organic—they grow, evolve, and change continuously. It is impossible for the infrastructures supporting such environments to maintain their secure integrity and cost-effectiveness without persistent vigilance and wisely spent renewed investment, which BAROV allows and facilitates. Striking the balance between sharing information among all necessary parties and maintaining adequate protection for the company's proprietary information is crucial in any business environment. In a networked world, information is the central nervous system for the organization with the risk of proprietary knowledge and confidential information being exposed to potential perpetrators. These perpetrators prey on the vulnerabilities that are inevitable in an IT system. Opportunities emerging from such vulnerabilities range from defacing corporate web sites to stealing valuable assets where infrastructure resources are appropriated covertly for seditious activities. Eradicating all threats would make the

infrastructure useless. System security and performance objectives tend to be at odds. However, steps can be taken to optimize and balance these seemingly diametrically opposed poles. BAROV has developed the process and assessment methods to help companies have a way to cost-effectively identify, prioritize, and achieve their security goals without depleting system performance. A summary of the four phases applied and nine processes are shown later in this case study, providing a summary of BAROV's usual recommend tasks, using a prioritized approach that qualitatively considers security benefits and levels of effort. The methodology is developed to help initiate discussions regarding which recommendations to implement immediately, in the future, or not at all, within the context of the company's business requirements, security goals, and budget constraints. Due to the limited scope of this case study, any company-specific requirements would need a unique and detailed analysis prior to the remediation efforts here.

### **Sample Analysis Report**

This section shows a sample BAROV analysis report issued to a company based on answers provided during personal interviews with the company's staff and on independent examination of documents and facilities by the BAROV team. The company analyzed is a multinational billion-dollar organization that is currently outsourcing a relatively small quantity of work items to Outsourced Company and before expanding its activities, hired BAROV to review the risks, if any, related to this business expansion and outsourcing activities, with a detailed report that outlines the risks and steps to either remove or mitigate the said risks that are identified.

**Approach** BAROV identified certain risks in its contract operations using agreed on work programs to address the risks. We also reviewed more than four dozen presentations and hundreds of documents in both English and Chinese, covering all the major policies and procedures within the scope of this engagement. Furthermore, we interviewed more than 42 company employees and the results of our review are presented in the form of an assessment report.

**Findings** After careful review of our findings and recommendations regarding the activities supporting Outsourced Company combined with their staffs' responses, we present the following overall finding. With minor correction actions, as pointed out by the team and completed while on-site, no instances of substantial nonconformance to the expectations matrix in the methodology were found in our review of Outsourced Company.

This does not mean there is absolutely no risk, but our review did not uncover any significant risks within Outsourced Company's operations or systems of internal control. In our professional judgment, the management controls operated by Outsourced Company mitigate the risks identified by the Client Company.

**Recommendations** During our review process, we made numerous recommendations to Outsourced Company regarding process improvements that could increase mitigation of risk, reduce the opportunity for error, or generally improve Outsourced Company's policy and procedures. The fact that Outsourced Company agreed to implement all of the recommendations documented in this report showed their interest in being viewed as a world-class service provider; most were done immediately, but due to the effort needed, a few remain to be completed as outlined in the findings section. Although the responsiveness of Outsourced Company to the risks of the existing business relationship is both reasonable and adequate, it should be noted that differences in relevant law, regulations, standards, and audit practices with the United States merit recommendation that Outsourced Company conduct annual external/independent reviews of the ongoing adequacy of operations. These annual reviews should demonstrate that no material risks exist, or have developed, with the business relationship and service. In our professional judgment, Outsourced Company provides the following characteristics essential to the Client Company:

- Management is dedicated to "Best of Breed" Enterprise Security
- Environment is highly secure
- Infrastructure is robust and backed up
- Policy and procedures are adequate, with two caveats:
  - Translation to English would make them more accessible
  - Improvements in organization would make them more cohesive
- Material control processes are effective and followed

**Scope of Assessment and Report** This report is not an audit report or an internal controls certification. It is an independent assessment of specifically identified performance criteria agreed to by Client Company and for the exclusive use of Client Company. It is the sole responsibility of Client Company to determine the adequacy of the controls, take steps to ameliorate any deficiencies as soon as practicable, and conduct a follow-up review to verify remediation. This report provides a narrative of the review conducted by a team from BAROV on-site in Outsourced Company's factory during the specified contractual period. The report is based on answers provided during personal interviews with Outsourced Company's staff and on independent

examination of documents and facilities by the BAROV team. BAROV employed the staff and proprietary methodology of its affiliates to conduct this review.

**Background** Outsourced Company began its operations (on some specified date) and currently employs approximately 1,600 personnel in one plant. There are plans to build multiple plants over the next 10 years at the same campus. Current capacity is 1.25 million manufactured units per year, with plans to double capacity by 2015. Client Company is currently outsourcing a relatively small item to Outsourced Company. Client Company is concerned about security and controls in all of its operations, including those contracted to Outsourced Company. Client Company engaged BAROV to review enterprise security at Outsourced Company.

Our relationship with the Outsourced Company was at the highest professional level at all times. From time to time, this excellent working relationship seemed strained. We learned near the end of our visit that Outsourced Company had previously experienced a similar review from a different customer and during the review was told everything was going great; however, the final report to the customer's executives was less than flattering. In hindsight, what we perceived as a misunderstanding about the scope of our review was an understandable tension about our motivation. This underlying caution on the part of Outsourced Company, combined with the language difficulties and the disjointed structure of the documentation, required that we occasionally needed to review the same items more than once. In the end, the misunderstanding about our scope and working style was resolved.

**Approach** We reviewed over four dozen presentations and hundreds of documents in both English and Chinese covering all the major policies and procedures within the scope of this engagement. We interviewed more than 42 Outsourced Company employees.

**Risk Assessment** Following our methodology, the project scope is determined by performing an independent risk assessment of the services outsourced. For this project, Client Company directed the work toward those areas it deemed most important.

**Scope of Review** Based on our understanding of Client Company's situation and underlying risk, we performed the following work programs for this review:

- Security Policies
- IT Security Infrastructure
- Access Control—both physical and logical

- Business Continuation Management
- Malicious Software
- Network Management
- Cryptology and Files
- Materials Management
- Inventory Controls

### **Prior Audits or Reviews**

**Internal Audit Report** We viewed a copy of the latest internal audit report. BAROV's translator read the cover page and told us that there were no outstanding issues, but since it was written in Chinese we were unable to validate the contents. After conferring with Client Company it was decided that a full translation was low-priority for our review.

**Assessment Reports** Each work program is summarized in a stand-alone Assessment Report (AR) in the following format. Each work program begins with a set of definitions and expectations that are repeated in this section of the AR for clarity in reading the report:

- *Situation*—This section describes the current policy and procedures (P&P) environment, with references to relevant documents in the work papers.
- *Findings*—This section presents the results of our inspection, citing specific incidents of nonconformance or issues that require discussion. We will specifically identify these incidents or issues as Item A, Item B, or Item C.
- *Recommendations*—We recommend the following actions: Item A, Item B, and Item C.
- *Disposition*—With regard to Item A, the Service Provider agrees with our recommendation and has already made changes that mitigate Item A. With regard to Item B, the Service Provider agrees with our recommendation and will make appropriate changes that mitigate Item B. With regard to Item C, the Service Provider believes that this issue is adequately addressed in another manner.
- *Conclusions*—This section provides our overall impression of this area of the assessment.
- *Follow up*—We recommend that Client Company ask the Service Provider to provide documentation of changes that mitigate Item B within a certain period to confirm the agreed upon changes. We recommend that Client Company review the Item C issue with regard to Client Company's policy, procedures, and governance framework.

Client Company should promptly discuss the Service Provider position with regard to Item C and ratify the approach or request that the Service Provider make changes to mitigate Client Company's concern.

### **Work Papers**

The report described above is fully supported by professional documentation or work papers (WP), which are maintained by BAROV. These work papers are contained in four folders with the contents as follows:

- Tab A—Work Program
- Tab B—Additional Pages to Work Program
- Tab C—Service Provider Documentation
- Tab D—Other Documents including Service Provider Policy

The following is a sample of a work paper, specifically on IT security policy.

#### **WP 1: Security Policy**

Suppliers should have adhered to a documented Enterprise Security Policy and Procedures (P&P) manual to ensure that only properly approved users are granted access to information systems and assets. Users should be granted access on a need-to-know basis, according to job responsibilities. There exists an information security policy, approved by management that is published and communicated to all personal who are responsible for its maintenance and review according to a defined review process. As part of the report, we will provide a situational awareness document, and list our findings, recommendations for correction, prescribed disposition of the problem, and any follow-up required. As an example of a follow up, we may recommend that the Client Company ask Outsourced Company to provide a copy of the agreed changes to the P&P within six months to confirm the changes required. We recommend that Client Company review the identified issues with regard to Client Company policy, procedures, and governance framework. Client Company should promptly discuss Outsourced Company's position and ratify the P&P approach or request that Outsourced Company make changes to mitigate Client Company's concerns.

**Quantitative Risk Simulation, Real Options Analysis, and Portfolio Optimization** WP2 to WP11 have been left out in this case study, but the sample seen in Figures 14.75 through 14.77 illustrate a Pre-Assessment Ranking Matrix used to understand the specific risk within a specific industry and rate those risks in order of risks to be reviewed. Using the example matrix

**Assumptions:**

Manager's information has been received  
 Rated for an On-site review

After all eleven (11) domains are completed the draft report needs to be completed. If issues need to be resolved do so, otherwise publish draft. After draft has been approved the Executive Summary needs to be completed, once approved published.

Fill out each of the eleven (11) workpages as required:

1. Security Policy
2. Organizational Security
3. Asset Classification and Control
4. Human Resources Security
5. Physical and Environmental Security
6. Communications and Operations Management
7. Access Control
8. Information Systems Acquisition, Development and Maintenance
9. Information Security Incident Management
10. Business Continuity Management
11. Compliance

with the following information:

(7) Page of (name):	Date: on-site	Prepared by: Your Name
Company ABC		

Page of needs to be filled out by hand as you ask the questions and receive the answers

Yes/No/NA Comments may be completed by hand or by computer (note this section will broaden as you type) please see samples below:

Questions/Control Activities	Rate	Yes/No/NA Comments
Does your organization have a formal Information Security Policy, which is published and approved by management?	1	A comprehensive formal Information Security Policy, which is published and approved by management which far exceeds industry standards was reviewed
Does your organization have a formal Information Security Policy, which is published and approved by management?	2	I reviewed their Information Security Policy, which is published and approved by management which meets industry standards

**FIGURE 14.75** List of working papers.

in Figure 14.76, we apply Risk Simulator input assumptions to the subject matter expert risk rankings, and we run simulations on the matrix in order to determine the total grand risk score for the Client Company. Using probabilistic distributions obtained from the simulation, we are now able to identify the chances that a specific category's risk and impact may exceed tolerable limits, as well as identify the critical success factors (sensitivity analysis and Tornado analysis were run on this assessment matrix). Furthermore, we developed an optimization model where each element was subject to a decision variable in terms of the cost required to correct any outstanding issues, compared to the benefit obtained from having an in-compliance security level, and ran it based on the Client Company's budget constraints. We were then able to create a strategy of multiple phases (sequential compound option) on when certain elements of the issues identified can first be fixed. Following this is the less critical next phase, all the while accounting for interrelationships among IT projects. For example, if a certain project requires another as a prerequisite (some platform technology that first needs

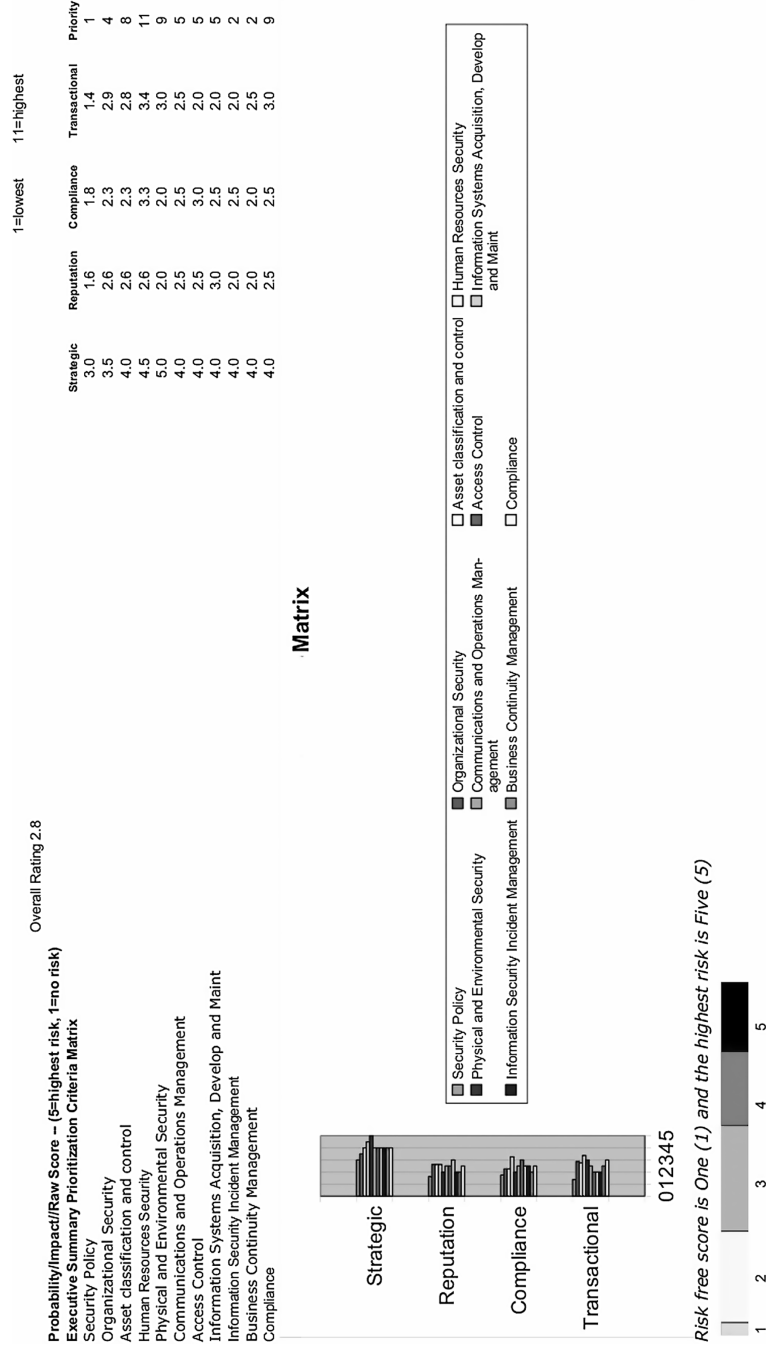
2.8 Overall Rating					
	Strategic	Reputation	Compliance	Transactional	
<b>Probability Risk Assessment</b>					
1 Security Policy	1	1.25	1.5	1.75	
2 Organizational Security	2	2.25	2.5	2.75	
3 Asset classification and control	3	3.25	3.5	3.5	
4 Human Resources Security	4	4.25	4.5	4.75	
5 Physical and Environmental Security	5	3	3	3	
6 Communications and Operations Management	3	3	3	3	
7 Access Control	3	3	3	3	
8 Information Systems Acquisition, Development and Maintenance	3	3	3	3	
9 Information Security Incident Management	3	3	3	3	
10 Business Continuity Management	3	3	3	3	
11 Compliance	3	3	3	3	
<b>Impact Risk Assessment</b>					
1 Security Policy	5	2	2	1	
2 Organizational Security	5	3	2	3	
3 Asset classification and control	5	2	1	2	
4 Human Resources Security	5	1	2	2	
5 Physical and Environmental Security	5	1	1	3	
6 Communications and Operations Management	5	2	2	2	
7 Access Control	5	2	3	1	
8 Information Systems Acquisition, Development and Maintenance	5	3	2	1	
9 Information Security Incident Management	5	1	2	1	
10 Business Continuity Management	5	1	1	2	
11 Compliance	5	2	2	3	
<i>Risk free score is One (1) and the highest risk is Five (5)</i>					
Values that are accepted	1	1.25	1.5	1.75	2
Values that are accepted	2.25	2.5	2.75	3	3.25
Values that are accepted	3.5	3.75	4	4.25	4.5
Values that are accepted	4.75	5			

FIGURE 14.76 Assessment matrix.

to be implemented before any subsequent projects can be implemented) or mutually exclusive redundant projects (the implementation of one project makes another obsolete or unnecessary).

In keeping with the belief that neither “cookie-cutter” nor “boil the ocean” approaches are cost-effective or appropriate, we use the following enterprise security assessment methodology to plan for a customized program. Our security assessment consists of four phases and nine processes. Phase 1 has four processes, Phase 2 has two processes, Phase 3 has two processes and Phase 4 has one process (Table 14.7).

Each phase is designed to produce meaningful results for the organization. Please see the attached sample forms previously used to get a flavor of the details that might be requested. Phase 1 examines the enterprise by eliciting information from people working in multiple levels of the enterprise. Phase 1 also derives the security requirements of the enterprise, based on the need for confidentiality, integrity, and/or availability of the key information assets. This phase is important because it helps in integrating unique perspectives and knowledge from multiple organizational levels and helps to build an enterprise-wide view of assets, threats, protection strategies, and risk indicators. This information can then be used to establish the security requirements of the enterprise, which is the goal of the first phase. Phase 2 is then applied to identify infrastructure issues and builds on the



**FIGURE 14.77** Ranking matrix.

**TABLE 14.7** Summary of Four Phases and Nine Processes

<b>Phase 1</b>	<b>Enterprise-Wide Security Requirements</b>
Process 1	Identify Enterprise Knowledge
Process 2	Identify Operational Area Knowledge
Process 3	Identify Staff Knowledge
Process 4	Establish Security Requirements
<b>Phase 2</b>	<b>Identify Infrastructure Issues</b>
Process 5	Map Information Assets to Information Infrastructure
Process 6	Perform Infrastructure Vulnerability Evaluation
<b>Phase 3</b>	<b>Determine Security Management Strategy</b>
Process 7	Conduct Multi-Dimensional Risk Analysis
Process 8	Develop Protection Strategy
<b>Phase 4</b>	<b>Develop Customized Training Program</b>
Process 9	Develop Security Knowledge Gap Strategy

information identified during Phase 1. It uses the asset and threat information from Phase 1 to identify the high-priority components of the information infrastructure. Phase 2 also evaluates the information infrastructure to identify infrastructure vulnerabilities that are exposing the enterprise's assets as well as missing policies and practices. At the conclusion of Phase 2, the high-priority information infrastructure components, missing policies and practices, and vulnerabilities would have been identified. Phase 3 is then applied to determine the security risk management strategy, which involves analysis of assets, threats, and vulnerability information in the context of intrusion scenarios to identify and prioritize the information security risks to the organization. In addition, it develops and implements a protection strategy in the organization to reduce the risk to the enterprise. Therefore, Phase 3 creates a comprehensive risk management plan for implementing the protection strategy and managing risks on a continual basis. The prioritized list of risks generated is used in conjunction with information from the previous phases to develop a protection strategy for the enterprise and to establish a comprehensive plan for managing security risks, which are among the goals of Phase 3. In addition, should the information supplied by staff-level employees indicate that there was some dissatisfaction among some of the employees in the company, specifically, any technical issues, these disgruntled insiders might have both the motive and the means to steal the information and would add to the risks, thereby in all probability adding to the complexity of the project. By performing a comprehensive risk assessment that considers asset, threat, and vulnerability information and puts it into the context of the enterprise, the risks facing the enterprise can be identified. In addition, personnel from all levels can understand risks

when they are put into the context of the enterprise, and can make sensible decisions concerning a protection strategy.

- Phase 1:
  - Process 1: Identify Enterprise Knowledge. This process identifies what senior managers perceive to be the key assets and their values, the threats to those assets, indicators of risk, and the current protection strategy employed by the enterprise.
  - Process 2: Identify Operational Area Knowledge. This process identifies what operational area managers perceive to be the key assets and their values, the threats to those assets, indicators of risk, and the current protection strategy employed by the enterprise.
  - Process 3: Identify Staff Knowledge. This process identifies what staff-level personnel perceive to be the key assets and their values, the threats to those assets, indicators of risk, and the current protection strategy employed by the enterprise.
  - Process 4: Establish Security Requirements. This process integrates the individual perspectives identified in the first three processes to produce an enterprise view of the assets.
- Phase 2: Uses the asset and threat information from Phase 1 to identify the high-priority components of the information infrastructure (both the physical infrastructure and the computing infrastructure). It also evaluates the information infrastructure to identify vulnerabilities. Standard catalogs of information about intrusion scenarios and vulnerabilities are used as a basis for evaluating the infrastructure. The ultimate goal of Phase 2 is to identify missing policies and practices as well as infrastructure vulnerabilities. The following two processes comprise Phase 2:
  - Process 5: Map Information Assets to Information Infrastructure. This process combines Phase 1 asset and threat information with staff knowledge about the information infrastructure to establish asset locations, access paths, and data flows. This leads to the identification of the high-priority infrastructure components.
  - Process 6: Perform Infrastructure Vulnerability Evaluation. This process combines the knowledge about assets, threats, risk indicators, and security requirements determined in Phase 1 with staff knowledge about the information infrastructure and standard catalogs of intrusion scenarios and vulnerabilities to identify missing policies and practices as well as infrastructure vulnerabilities.
- Phase 3: This phase is applied to determine the security risk management strategy, and has two subprocesses. They analyze the assets, threats, and vulnerability information in the context of intrusion scenarios to identify and prioritize the risks to the enterprise. In addition, a protection

strategy is developed and implemented in the enterprise. The ultimate goal of Phase 3 is to identify risks to the enterprise and develop a protection strategy to mitigate the highest priority risks. The following two processes comprise Phase 3:

- Process 7: Conduct Multidimensional Risk Analysis. This process analyzes the assets, threats, and vulnerability information identified in Phases 1 and 2 using intrusion scenarios to produce a set of risks to the enterprise. The risk attributes of impact and probability are estimated and then used to prioritize the risks.
- Process 8: Develop Protection Strategy. This process develops the protection strategy by identifying candidate mitigation strategies and then selecting the appropriate ones based on factors such as cost and available resources. This process also develops a comprehensive security risk management plan for implementing the protection strategy and managing risks on a continual basis.
- Phase 4: This phase is used to develop customized training programs by analyzing the assets, threats, and vulnerability information in the context of intrusion scenarios, so that an organization can begin to understand what information is at risk. With this understanding, it can create and implement a protection strategy designed to reduce the overall risk exposure of its information assets. The following process comprises a single subprocess:
  - Process 9: Develop Security Knowledge Gap Strategy. This process combines all the above information and industry-specific issues to tailor a training program that “fits” the organization and its current situation to meet current best practices as well as due diligence in its security practices.

## **CASE STUDY: BASEL II CREDIT RISK AND MARKET RISK**

**Analytical Techniques for Modeling Probability of Default, Loss Given Default, Economic Capital, Value at Risk, Portfolio Optimized Value at Risk, Interest Rates and Yield Curve, Delta-Gamma Hedging, Floating and Fixed Rates, Foreign Exchange Risk Hedging, Volatility, Commodity Prices, and Over-the-Counter Exotic Options**

*This case study is written by the author based on consulting projects that he had performed on banks globally, and the case illustrations apply the Risk Simulator, Modeling Toolkit, and Real Options SLS software applications. For more details on some of these applications, please see two of the*