7 Executive security management

7.1 Responsibilities at organizational levels

Rate the following areas from 0 to10.

Item	*Rate*
Risk management and surety levels are defined by top management.	
If there is a separation between corporate and IT risk management, they are closely coordinated.	
If IT risk management is separated from corporate risk management it is operated by the CISO.	
Business life cycles and deterrence are top management responsibilities.	
For business life cycles, business acquisition teams include representation from the CISO function.	
Top management also sets policy, structures protection program management, and defines the placement of information protection by positioning the CISO within the company and defining the linkage between the CISO and HR, legal, the CIO, and others.	
TOTAL (sum the ratings and divide by 6)	

7.2 Enterprise security management architecture

Rate the following areas from 0 to 10.

Item	*Rate*
The overall control system that operates information protection is managed by the CISO.	
Top executives and board of directors directly control the functions and management associated with the CISO.	
The CISO functional responsibilities include policies, standards, procedures, legal, HR, and risk management activities.	
The CISO functional responsibilities include collaboration with or control of the policy team and the risk management team.	
The CISO functional responsibilities include collaboration with users, some of the project team, and developers.	
The CISO functional responsibilities include collaboration with the legal department, the HR department,	
The CISO functional responsibilities include assuring that adequate testing and change control, physical and informational technical safeguards, and incident handling activities are undertaken and involve close collaboration with developers, systems administrators, change control teams, response teams, and project teams.	

Copyright © 1977-2005 Fred Cohen & Associates – All Rights Reserved

Item	Rate
The CISO functional responsibilities include assuring auditing processes, knowledge and awareness programs, and documentation functions and involve work with auditors, trainers, experts, project teams, and of course everyone that has to document what they do.	
The CISO functional responsibilities include project management activities that span the enterprise.	
The CISO must assure that the enterprise fulfills separation of duties requirements, has adequate skill sets, has organizational mandate, and that groups operating in different parts of the organization collaborate for information protection purposes.	
Feedback mechanisms lead to adaptations through the control efforts associated with the CISO function.	
The most critical function and the purpose for the CISO function as identified by top management is to exert the controls that influence all of the different protection-related functions and to listen to the feedback and make decisions that help to adapt the overall enterprise protection system based on the feedback.	
The CISO communicates directly and effectively with top management on a regular basis.	
TOTAL (sum the ratings and divide by 13)	

7.2.1 Groups that the CISO meets with or creates and chairs

Rate the following areas from 0 to 10, sum the results and divide by 4.

Item	Rate
The CISO is responsible for assuring the ongoing value of all of the non-physical and non-fiscal assets of the company.	
The CISO manages the enterprise control system associated with information protection through groups.	
Functional groups in which the CISO participates perform the necessary functions for operating the protection program.	
Review board groups review and oversee the efforts of the functional groups and are led by or participated in by the CISO.	
TOTAL (sum the ratings and divide by 4)	

Copyright © 1977-2005 Fred Cohen & Associates – All Rights Reserved

7.2.1.1 Top-level governance board

Rate the following areas from 0 to 10.

Item	*Rate*
The top-level governance board is an outward facing function of the CISO that interacts with oversight.	
This group has legal responsibility for the business and its operations and determines the placement and reach of the information protection function in the enterprise.	
This group meets periodically with the CISO to review overall program performance and inquire about specific issues they deem worthy of their attention.	
Meetings are scheduled with this group at least once per quarter and, for select functions of the CISO like business continuity planning, additional meetings with many of the same people are also held.	
TOTAL (sum the ratings and divide by 4)	

7.2.1.2 Business unit governance boards

Rate the following areas from 0 to 10.

Item	*Rate*
Business units that are substantial enough to operate more like wholly owned subsidiaries than like departments typically have their own internal information protection functions that fulfill some or most of their needs.	
Boards exist within the substantial business units for their internal operations and interface with the CISO in order to provide enterprise-level information and assure at the enterprise level that information protection is as it is supposed to be.	
The exchanges are also used to save time and money by reducing unnecessary redundancy and improving process for all.	
TOTAL (sum the ratings and divide by 3)	

7.2.1.3 Policy, standards and procedures group and review board

Rate the following areas from 0 to 10.

Item	*Rate*
The policy, standards, and procedures group is responsible for initial policy development, reconciliation of existing policies, policy rewrites, adaptation of policy to changes in the environment, development and maintenance of control standards from policies in conjunction with the operating environment, and development of procedures associated with meeting control standards.	
The policy review board is responsible for review and approval of policies, and includes top management that makes them official within the enterprise.	

Copyright © 1977-2005 Fred Cohen & Associates – All Rights Reserved

Item	*Rate*
The review and acceptance of standards by individual groups affected by those standards, approval of those standards by the proper level of management in different enterprise areas, and verifying the consistency of those standards with policies before acceptance is also controlled by this board.	
Individual managers are responsible for verifying that procedures meet standards and are responsible for assuring that this is done.	
Reporting structures provide documentation and audit provides verification that policies are in place and operated at all levels.	
Documentation of all aspects of this process are kept.	
Documentation facilitates review for new members of teams, for assurance processes to work properly, and for demonstration of regulatory compliance and other legal mandates.	
Documentation includes meeting minutes, periodic plans, deliverables, progress reports, and other related documentation of the process.	
Documentation includes original data collected in the process, such as copies of emails associated with policy reviews, schedules for processes in whatever form the projects are tracked, ultimate dispositions of all activities, funding and costs associated with the effort, and resulting formal outputs from the process.	
Project management is used for this process and is responsible for collecting, tracking, and reporting on all aspects of project progress, convening and scheduling meetings, and providing the CISO function with ongoing information on the overall effort.	
The audit process verifies that these responsibilities are being properly carried out by selective testing of consistency by examination, verifying that the approval process is generating meaningful review prior to approval, that approval or rejection of changes is done in a timely fashion, and that policies, standards, and procedures are followed.	
Audit of policy includes reviewing the documentation associated with the effort, verification of proper approvals for policies, standards, and procedures in actual use, and verification of the actual operation of the overall system by selective, periodic, random, and blind review of operations against procedures, standards, and policies.	
TOTAL (sum the ratings and divide by 6)	

Copyright © 1977-2005 Fred Cohen & Associates – All Rights Reserved

7.2.1.4 Legal group and review board

Rate the following areas from 0 to 10.

Item	*Rate*
Legal review of all policies is mandatory and top management sign-off is required for all policies.	
Standards are reviewed to assure that no laws are being violated.	
Personnel procedures are reviewed for issues associated with potential law suits and statutory violations.	
Privacy laws relating to background investigations, laws related to the specific industry, and the range of related issues associated with legal positions are particularly important in international businesses are understood and applied by inside counsel or outside counsel is used for these matters.	
The legal group is involved in incident response whenever investigatory processes are undertaken.	
The legal group review board activities are limited in scope to reviewing information protection matters.	
TOTAL (sum the ratings and divide by 6)	

7.2.1.5 Personnel security group and review board

Rate the following areas from 0 to 10.

Item	*Rate*
Personnel security is coordinated by HR and carried out by a group within physical security that deals with personnel protection, facilities security, and other related issues.	
Background checks are performed by an outside service.	
The CISO coordinates efforts to assure that personnel security meets the needs of the information protection program.	
Personnel interact efficiently and effectively with all enterprise components and systems associated with the human life cycle that imply protection changes.	
Actions implied by the information protection program as well as issues related to assurance of employee rights and the proper operation of the appeals process for incidents and other matters related to employees is properly handled by the HR department and reviewed by the HR review board.	
Tracking of personnel information is an HR function that is integrated with information protection issues in order for the coordination to take place.	
Clearance processes and status are HR department functions that integrate with other aspects of security as well.	
Documentation requirements are extensive for these processes, legal issues have to be considered, and review boards for processes as well as individual cases are required for personnel actions.	

Copyright © 1977-2005 Fred Cohen & Associates – All Rights Reserved

Item	Rate
Tracking of training and awareness programs is often handled by either the HR department or a separate training group, however, tracking of educational efforts as it relates to qualifications, benefits, salary, position, and other issues is within the HR function.	
The CISO has responsibility to assure that these processes are properly undertaken and that timely and accurate information is used.	
Audit is used to verify the process.	
The CISO coordinates with this HR activity and influences changes necessary so that it works effectively.	
TOTAL (sum the ratings and divide by 12)	

7.2.1.6 Risk management group

Rate the following areas from 0 to 10.

Item	Rate
The risk management group is responsible for evaluating risks and making determinations about when risk can be accepted, transferred, avoided, or mitigated.	
Top management is intimately involved in risk management decisions.	
The CEO is on the risk management review board.	
Members of oversight functions are on the risk management review board.	
Top management and members of the risk management review board understand the risk-related issues associated with information protection.	
The CISO heads the risk management review board for information protection.	
The CISO is responsible for making preliminary evaluations for all risks in this area and sole responsibility for decisions about low risk situations.	
Risk management is a well documented process.	
Risk management is consistently across the enterprise.	
Risk management uses well qualified individuals who understand how to make good judgments and understand the technology that forms the basis for the evaluations undertaken.	
The risk management group is tightly integrate with the CISO function.	
TOTAL (sum the ratings and divide by 11)	

Copyright © 1977-2005 Fred Cohen & Associates – All Rights Reserved

7.2.1.7 Protection testing and change control group and review board

Rate the following areas from 0 to 10.

Item	*Rate*
The protection testing and change control group (or groups) are responsible for measuring the effectiveness of protection on systems that warrant such controls and assuring to the desired degree of certainty that those systems operate as they are supposed to.	
Results of protection testing and change controls are reviewed as a matter of course before results are accepted and systems are transitioned from testing into operational use.	
Changes to medium or high consequence systems have to be approved by all of those responsible for those systems and all of those impacted by those systems or those changes before changes are permitted to take place.	
All affected owners are notified prior to significant changes that may affect their systems through the change control group.	
All significant changes to systems affecting other systems are tracked and approved by the change control group.	
The change control group records all tests performed as part of change control and verifies that changes meet the requirements of interdependent systems.	
The change control and protection testing group(s) are independent of other groups.	
The change control and protection testing group(s) have separate research and development from production.	
Protection testing is different from vulnerability scans and such scans are not considered adequate for protection testing purposes except for low risk systems within low risk zones where even aggregated risks are low.	
Generally speaking, systems under change control are medium of high surety systems in medium or high risk applications.	
TOTAL (sum the ratings and divide by 10)	

7.2.1.8 Technical safeguards group and review board

Rate the following areas from 0 to 10.

Item	*Rate*
The technical safeguards group is responsible for the job of risk mitigation.	
They oversee the application of technologies to systems in order to reduce the vulnerabilities of those systems and the consequences of failures in those systems.	
For low risk systems, as determined by risk management, the technical safeguards group is left largely on their own in terms of protection with the objective of maximizing effectiveness while minimizing costs.	

Copyright © 1977-2005 Fred Cohen & Associates – All Rights Reserved

Item	Rate
The CISO function oversees the protection of low surety systems and seeks to make certain that they are not able to unduly influence medium or high surety systems through architectural methods, like the network zoning policies, and similar high or medium surety methods.	
For medium and high risk systems and content, the technical safeguards team has to gain approval from risk management for mitigation approaches but takes on the primary lead for the design and implementation of technical safeguards.	
They are subject to audit as well as oversight, including review by the zoning board for zone-related changes and oversight by the CISO function.	
Documentation is critical, legal approval has to be gained for certain potentially invasive surveillance technologies, and interface to the HR application environment is central to success of technical safeguards depending on identity management solutions. The CISO is responsible for liaison between the legal and HR departments for approvals of these actions and for making determinations about protective measures with these sorts of effects.	
The technical safeguards team implements policy, helps develop and follow standards, creates procedures and gets their approval, sends changes through change control for high and medium surety systems, acts as experts for some aspects of training and awareness, and receives education in order to continue to be effective in their tasks.	
The technical safeguards team documents all of its activities and is responsible for verifying documentation of activities undertaken by those who implement safeguards.	
TOTAL (sum the ratings and divide by 9)	

7.2.1.9 Zoning boards and similar governance entities

Rate the following areas from 0 to 10.

Item	Rate
Network zoning is controlled either by a zoning board or by the CISO in conjunction with the technical safeguards team.	
Zoning boards typically include those impacted by a change in zones or, during the creation of zones, those responsible for working within those zones.	
System owners, network owners, risk management, audit, and incident response teams participate in zoning board meetings.	
Additional requirements for classified systems and other special purpose environments that have to meet additional regulatory or jurisdictional requirements are covered by appropriate subgroups of the zoning board.	
TOTAL (sum the ratings and divide by 4)	

Copyright © 1977-2005 Fred Cohen & Associates – All Rights Reserved

7.2.1.10 Physical security group and review board

Rate the following areas from 0 to 10.

Item	*Rate*
Special requirements and collaboration associated with data centers, wiring, wire closets, conduits, perimeters for medium and high risk systems, protection of paper and other media in storage, before input, and after output, physical aspects of information and equipment life cycles, and integration of physical and informational access controls are met by the physical security group.	
The CISO is responsible to report physical security inadequacies and, if mandate is given, to manage the mitigation process.	
The CISO participates in the physical security review board or other similar process to assure that information protection needs are met.	
TOTAL (sum the ratings and divide by 3)	

7.2.1.11 Incident handling group and review board

Rate the following areas from 0 to 10.

Item	*Rate*
The incident handling group is responsible for information technology aspects of business continuity planning, disaster recovery, and day-to-day incident detection and response within the information technology function.	
They are, necessarily, separate from the technical safeguards team because they are tasked, among other things, with detecting trusted insider abuse.	
The incident handling group is not permitted to control any systems, and act only through the systems administration group for low-risk systems and change control for medium and high risk systems to carry out any changes.	
This separation of duties is key to proper operation and the incident handling team acts as part of the assurance process.	
The incident handling team is responsible for identifying event sequences that can cause potentially serious negative consequences.	
The incident handling team is responsible for devising the means to detect these sequences in a timely enough fashion to mitigate harm to within enterprise specified tolerances.	
The incident handling team is responsible for devising the warnings and response regimen that mitigates these consequences in the required time frames.	
The incident handling team is responsible for defining the conditions under which these response processes get invoked.	
The incident handling team is responsible for initiating, managing, and carrying out these responses when they are required.	

Copyright © 1977-2005 Fred Cohen & Associates – All Rights Reserved

Item	Rate
The incident handling team is responsible for devising the process used to determine when response processes can be terminated and normal operations continued.	
The incident handling team is responsible for carrying out those termination processes when necessary and appropriate.	
The incident handling team is responsible for after-action reports, documentation, and other related matters that produce an incident handling system that adapts properly with time.	
The incident handling team is responsible for	
Incident handling is part of the review process for technology changes.	
For low consequence systems, intrusion detection and response processes may be embedded in the systems themselves and run by systems and network administrators, however, these systems provide feeds to the incident handling group so they can remain aware of situations in those environments that may eventually effect other systems.	
Incident handling includes documentation requirements for the collection and retention of forensic evidence associated with legal matters, and the documentation of event sequences that ultimately lead to employee sanctions and other related actions.	
The business continuity and disaster recovery plans are the responsibility of incident response and are documented by this group.	
The interface to the legal department runs through a manager or the CISO for incidents of significant import.	
HR records get generated as a result of these actions and the HR information associated with positions, roles, and other elements used in identity management are key to understanding and characterizing event sequences as incidents.	
Incident handling policies, standards, and procedures are part and parcel of the group's function.	
Risk management helps to decide how much incident handling effort is required for which systems.	
Change control provides information used in incident handling through test results that provide calibration information and configuration management that helps to determine criticality and severity of incidents.	
Incident handling feeds data to auditors for evaluation of the incident handling capability and its operation and as information for audit review of the operations area.	
Incidents drive awareness programs and the incident response team acts as a provider of critical information for the awareness and knowledge requirements.	
The incident handling review board is designed to provide management with information about incidents and to get feedback on the process so as to improve it over time.	

Copyright © 1977-2005 Fred Cohen & Associates – All Rights Reserved

Item	Rate
Quarterly reviews of incident handling and additional reviews when incidents cause substantial harm are undertaken.	
Reviews of individual incidents are created as part of the documentation process complete with after action reports indicative of suggested process improvements.	
The review board reviews after-action reports prior to quarterly meetings and summaries of these reports are included in the overall review of the program.	
TOTAL (sum the ratings and divide by 28)	

7.2.1.12 Audit group and review board

Rate the following areas from 0 to 10.

Item	Rate
The audit group is part of the corporate internal audit function.	
The audit group has a very broad range of responsibilities for reviewing and reporting on CISO functional responsibilities.	
The audits of each of the functions of the CISO should also go to the CISO so that the CISO can adapt the operation to meet the need.	
IT audit has the responsibility to review the performance of every aspect of the information protection program as well as responsibility to verify that no undetected incidents take place by acting as an independent incident detection group.	
TOTAL (sum the ratings and divide by 4)	

7.2.1.13 Awareness and knowledge group and review

Rate the following areas from 0 to 10.

Item	Rate
The awareness and knowledge group is tasked with providing a comprehensive information protection awareness program.	
This entails the collection, creation and dissemination of information appropriate to all of the individuals in the company, translated into proper language, written so as to meet social norms, and presented to convey the important information and specific instructions on how to behave with regard to information protection issues.	
Critical awareness issues are repeated twice a year, and employees who have not received the awareness training and demonstrated their understanding of it have to be decertified from performing tasks until they come into compliance.	
There is a system of tracking all users and their currency in security training and awareness for all tasks they are assigned to perform.	
As changes in responsibility occur, training and awareness are updated.	

Copyright © 1977-2005 Fred Cohen & Associates – All Rights Reserved

Item	Rate
The awareness program has to be updated on a regular basis so that it does not become stale.	
A variety of techniques are available and should be rotated and applied over time to keep interest levels high.	
The program produces well-documented results that are reviewed on an annual basis to assure that the program is operating properly.	
This review is done by the CISO as part of their normal process.	
Legal review and long-term documentation are retained to mitigate any disputes for the duration of the applicability of the training material, including all applicable statutes of limitations.	
TOTAL (sum the ratings and divide by 10)	

7.2.1.14 Documentation group

Rate the following areas from 0 to10.

Item	Rate
There is a corporate documentation standard, an archival function and document repository, a tracking process that includes aging and life cycle management for destruction processes, and a set of retention policies, standards, and procedures that support this function.	
A library system is used to track all of this information, including the requirement to categorize and retrieve data, librarians, and off-site backup storage of important documents.	
This system tracks all of the documentation produced through the CISO function and provides easy retrieval and access for authorized individuals including the CISO and all of the review boards relative to the material they review.	
This group also provides the means for audit and other related functions to gain access to materials, and provide historical data and research capabilities.	
Documentation is systematically produced through the use of professional project managers as part of the project management process.	
The CISO maintains a project management process surrounding all efforts both to track everything and to provide clear documentation of processes and outcomes.	
Documentation has proper classification and applicability in order to assure that it is properly protected within the enterprise protection architecture.	
TOTAL (sum the ratings and divide by 7)	

Copyright © 1977-2005 Fred Cohen & Associates – All Rights Reserved

7.2.2 Separation of duties issues

Rate the following areas from 0 to10.

Item	*Rate*
At the CISO level, management has to coordinate all aspects of the protection program for it to be effective.	
Separation of duties is accomplished by the role of audit and oversight in reviewing the CISO's performance.	
TOTAL (sum the ratings and divide by 2)	

7.2.3 Understanding and applying power and influence

7.2.3.1 Physical power

Rate the following areas from 0 to10.

Item	*Rate*
Because of physical security mechanisms and guard forces, physical security is a means of exerting CISO power.	
Having physical access to information systems and infrastructure, being able to lock offices or lock people out of facilities, and the use of guards to escort individuals to meetings are all examples of how physical power can be used by the CISO.	
Physical force is only used by the CISO as a last resort or when called for by standard policies and procedures.	
Physical escort is normally used when an employee is terminated, as disputes often arise in this context.	
Physical force is used when threats to health or safety or enterprise assets demand it.	
TOTAL (sum the ratings and divide by 5)	

7.2.3.2 Resource power

Rate the following areas from 0 to10.

Item	*Rate*
Money, facilities control (space), people (time), computing resources, network resources, control over the environment (ecology), and the threat of force are used by the CISO appropriately.	
Overt resource power is used by the CISO to produce compliance and, in some cases, identification.	
TOTAL (sum the ratings and divide by 2)	

Copyright © 1977-2005 Fred Cohen & Associates – All Rights Reserved

7.2.3.3 Positional power

Rate the following areas from 0 to10.

Item	*Rate*
Positional power is used by the CISO to gain access to information.	
Positional power is used by the CISO to grant access to others as needed.	
Positional power is used by the CISO to organize groups.	
Information is used for its exchange value or as a tool of persuasion.	
The ability to grant access is not used by the CISO for exchanges.	
Information and access rights are used to assure compliance.	
The right to organize is used to influence work roles, assignments, titles, and pay levels to reward those in the information protection program.	
Positional power in the information protection arena is exercised through the use of matrix management, project teams, reassignment of people to teams under the CISO, or other similar steps.	
TOTAL (sum the ratings and divide by 8)	

7.2.3.4 Expertise, personal, and emotional power

Rate the following areas from 0 to10.

Item	*Rate*
The CISO effectively uses expertise is used for persuasion.	
The threat of force through expertise is avoided by the CISO except when involving questioning of suspects in relationship to incidents.	
The CISO uses the trust relationship advanced by friendliness with other top management to persuade them to help meet the duties to protect.	
Personal relationships are used to provide access and information.	
TOTAL (sum the ratings and divide by 4)	

7.2.3.5 Persuasion model

Rate the following areas from 0 to10.

Item	*Rate*
A defined and documented model of persuasion is used to influence others.	
Persuasion achieves change through a combination of learning and acceptance of the goal viewpoints.	
Learning is fostered by conveying the message effectively and having the target understanding it.	
Acceptance is fostered by bringing comfort with the message through assuring it is relevant and that the person being persuaded likes the idea.	
Target audience motives and value, information and language, perception and role, and attitudes and emotions are used to select persuasion techniques.	
In persuasive discussions both (or all) sides are presented with the favored viewpoint presented last.	

Copyright © 1977-2005 Fred Cohen & Associates – All Rights Reserved

Item	*Rate*
In persuasive discussions conclusions are clearly stated.	
In persuasive discussions repetition is used to make points, thus the formulaic approach of saying what you are going to say, saying it, and saying what you have said.	
In persuasive discussions a need is aroused and then satisfied.	
Threats are not used in persuasive discussions and fear uncertainty and doubt are avoided.	
Desirable messages are used wherever possible and put first when less desirable ones are also to be presented.	
In negotiations, everything desired is asked for and only backed off of slowly in exchange for large concessions.	
In negotiations, similar points of view are stressed to reduce disagreements without belittling other views.	
In negotiations, hard issues are tied to easy ones.	
Advice is sought on how to resolve problems without sacrificing enterprise needs to generates a cooperative environment.	
Defensive situations are avoided to prevent hardening views.	
Appeals to excellence, self worth, and fairness are used when feasible.	
An effort is made to make the audience feel worthwhile and to reinforce their opinions.	
Balance is presented without unnecessary lingering ambiguity.	
If a problem is created it can be readily resolved by agreeing with the presenter's view.	
Social forces are considered and the audience point of view accounted for.	
Facts, methods, goals, and values are used to influence decisions.	
Power issues are always considered.	
Favorable presenters are always introduced as experts.	
Media, presentation, clothing, degrees, experience, and references are used to increase credibility.	
Opinions on issues you don't know much about are not opined on to retain credibility, particularly among experts in technical matters.	
Letters or emails are used when establishing justification or to get a letter back or when interruption is dangerous.	
Face to face is used when presence brings regard or respect, when visual indicators help guide direction, or when more or less may be desired.	
TOTAL (sum the ratings and divide by 28)	

Copyright © 1977-2005 Fred Cohen & Associates – All Rights Reserved

7.2.3.6 Managing change

Rate the following areas from 0 to10.

Item	*Rate*
Expectations are managed to facilitate change.	
Explicit plans are used for substantial changes.	
Planning for change includes understand what will be different.	
Planning for change includes who it will affect,	
Planning for change includes how to prepare those affected.	
Planning for change includes determining how the change plan could fail.	
Planning for change includes determining how to treat the things that could cause it to fail before they cause it to fail.	
Change plans include a buy-in plan.	
Change plans include a communications plan.	
Change plans include a set of risk treatment plans.	
TOTAL (sum the ratings and divide by 10)	

7.2.3.6.1 The buy-in plan

Rate the following areas from 0 to10.

Item	*Rate*
The CISO has taken adequate steps to assure that executives and leaders know who is leading the efforts for change and have built up trust in the CISO and those individuals in order to assure that the executives and leaders will buy into the plan.	
Plans which are largely within a given executive's purview are championed by that executive and not just by the CISO.	
The champion for each change plan adopts that plan as their own.	
The CISO has direct access to the CEO and uses it only as needed to support enterprise-wide change efforts.	
Managers and other facilitators are alerted to executive support in order to see benefits in helping to make change.	
Security changes initiated by workers and managers are passed to the CISO for consideration prior to implementation so that the CISO can facilitate change.	
Efforts to make changes and success in those efforts are reflected in the metrics used to measure job performance throughout the enterprise.	
Managers are supported by the CISO in security-related changes.	
Workers are informed of what they have to do next and how their performance in those tasks will be measured as part of the buy-in effort.	
Rewards and punishments for workers and managers are clearly defined to facilitate their willful participation in making changes.	
TOTAL (sum the ratings and divide by 10)	

Copyright © 1977-2005 Fred Cohen & Associates – All Rights Reserved

7.2.3.6.2 The communications plan

Rate the following areas from 0 to10.

Item	*Rate*
A well-defined plan is in place for announcing specific items for awareness to target audiences.	
A well-defined plan is in place for discussing things with those audiences to develop mutual understanding, come to agreement so that people are aligned to the change, involve the targets to gain their willing participation, and prepare them so that they can successfully adopt the changes.	
The goal of the communications plan is for the targets of CISO change efforts to say “I know what is changing, why it is changing, and how it is happening.”	
Identified target audiences include executives, managers, staff members, casual employees, non-employee workers, and others as suited to the need and as affected directly or indirectly by the change.	
Individuals in each target audience are provided with the information they need to understand, from their point of view, what is changing, why it is changing, and how the change will happen.	
The communications plan specifically codifies when and how often each target audience should be communicated with and by whom, what is to be communicated with them and toward what objective (what, why, or how of the change), and the form of the communication should be selected to meet the need per the previous descriptions provided for in the persuasion model.	
The communications plan seeks to avoid errors of omission, errors of commission, and errors of substitution by providing the right amount of information in understandable terms.	
TOTAL (sum the ratings and divide by 7)	

7.2.3.6.3 The risk treatment plans

Rate the following areas from 0 to10.

Item	*Rate*
Risks to change are addressed by explicit risk treatment plans.	
Natural resistance to change is mitigated through the communication plan.	
Vested interest risks to change are mitigated through use of influence techniques.	
Performance metrics risks and other similar reward and punishment risks for those who participate in change are mitigated by the participation of champions and by redefining performance metrics relative to the changes.	
Organizational risks are mitigated by alignment of human forces and creating smooth transitions in that they don't unduly disrupt the normal course of business or create unnecessary friction.	

Copyright © 1977-2005 Fred Cohen & Associates – All Rights Reserved

Item	*Rate*
Organizational alignment is initiated by communication with stakeholders and aligning the leadership around vision, goals and metrics for success.	
Once the leaders agree on these factors, other stakeholders are fully engaged by the CISO and executive management.	
If stakeholders and executive management cannot be convinced, the change process will likely fail and the CISO then backs off of the plan and either adapts it or tries again with different persuasion methods.	
The plan includes ongoing processes involving stakeholders to keep them involved.	
Stakeholders who disagree with the change are influenced so as to not disrupt the process, perhaps by indirectly reducing the extent to which they care about the issue.	
Smooth transition is achieved whenever possible by minimizing friction through effective communications and preparations.	
To prepare for performance the specific information, skills, and knowledge needed by each of the different sorts of individuals involved is identified.	
To manage the transition smoothly, information is provided to bridge the gap between the previous and subsequent states.	
TOTAL (sum the ratings and divide by 13)	

Copyright © 1977-2005 Fred Cohen & Associates – All Rights Reserved

7.2.4 Roll-up

Enter the ratings from each of the above areas.

Item	Rate
Responsibilities at organizational levels	
Enterprise security management architecture	
Groups that the CISO meets with or creates and chairs	
Top-level governance board	
Business unit governance boards	
Policy, standards and procedures group and review board	
Legal group and review board	
Personnel security group and review board	
Risk management group	
Protection testing and change control group and review board	
Technical safeguards group and review board	
Zoning boards and similar governance entities	
Physical security group and review board	
Incident handling group and review board	
Audit group and review board	
Awareness and knowledge group and review	
Documentation group	
Separation of duties issues	
Physical power	
Resource power	
Positional power	
Expertise, personal, and emotional power	
Persuasion model	
Managing change	
The buy-in plan	
The communications plan	
The risk treatment plans	
TOTAL (sum the ratings and divide by 28)	

Startup	Diligence	Typical	Excellent	Best
0	5	4	7	8

Copyright © 1977-2005 Fred Cohen & Associates – All Rights Reserved