Risk Management Approach Report

DATE HERE

Presented To:

CLIENT

by

Fred Cohen & Associates

in fulfillment of Purchase Order LBU-34-849-23

Table of Contents

Executive Summary

Starting in October of 2004, CLIENT tasked FCA with a series of deliverables starting with the reconciliation of existing policies and the creation of a new set of policies for CLIENT, some initial control standards, some initial procedures, and for a new process for risk management that is consistent with the new policies. As the last deliverable, starting in mid-December, 2004 and due by December 31, 2004, FCA prepared this Risk Management Approach report to provide guidance to CLIENT for risk management (RM) in accord with the recently developed CLIENT policies. This report provides:

- The set of processes to be used in the overall risk management process
- Guidance as to the conditions under which each process should be applied
- A specific process to be used as a base process for:
  - Identifying the issues to be addressed in the risk management process
  - Determining when to use more in-depth processes for high-risk issues
  - When to accept risks and not further pursue risk management
  - How to treat medium risks and what to analyze
- How to identify consequences and how to differentiate them
- How and when to identify threats and how to analyze them
- How and when to do vulnerability assessments and how to do them
- Risk management choices and when to choose which of them
  - When to accept risks
  - When to transfer risks
  - When to avoid risks
  - When to mitigate risks
- Risk mitigation approaches for cases when mitigation is chosen
- Mapping of policy elements into specific risk management mandates
- A schedule for risk management including:
  - Initial conditions required for risk management
  - Management actions required for operation of risk management processes
  - A schedule of activities that need to be done, how often, and linkage to rational
  - How to map this risk management program into corporate reporting mandates
- An initial threat assessment to be used in the first round of risk management

This report is designed to allow knowledgeable individuals with proper background and training to build a risk management program for CLIENT and to do initial risk management work, and to provide links to additional information that will be helpful in getting more detailed information required for carrying out individual processes.

The risk management process

The RM process to be used within CLIENT includes the following elements:

The evaluation processes which includes:

- Protection posture assessments are used to identify high risks and provide urgent, tactical, and strategic guidance for medium and low risks. These result in many cases where risks should be accepted, transferred, avoided, or mitigated using standard techniques.
- Scenario-based and game theoretic analysis are to be used to augment risk management for higher consequences involving medium threats.
- Systems analysis is to be used to augment risk management for high threat, high-consequence situations.

Evaluations must be done of issues specifically identified by policy (as codified herein) as well as for overall business purposes. Specific attention is to be paid to the issues identified in policy as part of each of the analytical methodologies identified.

A schedule of evaluations is provided and this should be used to create a regular risk management process to be undertaken by CLIENT management in order to keep up to date and adapt over time per policy requirements.

A reporting requirement for CLIENT management is also required and a process for translating the actual RM process into appropriate report formats is necessary in order to fulfill administrative needs.

The risk management process is owned by the owner of CLIENT and it is the owner's responsibility to assure that the process is rigorously undertaken, adequately funded, supported at all levels of management, and meaningfully applied.

Evaluation processes to be used

The three evaluation processes for overall risk management include protection posture assessments, scenario-based and game theoretic analysis, and systems analysis. Each involves threat, vulnerability, and consequence analysis and these are identified in the following subsections.

Methodologies

The methodologies are outlined in [LIMITED ACCESS REPORT CITED HERE], extracts of which are used here.

Protection posture assessments

This technique is based on the premise that if the proper people, processes, and support are in place, protection will be effective. It is typically used in conjunction with a Generally Accepted Information Security Principles (GAISP) and International Standards Organization (ISO) 17799 review and consists of determining how the organization implements its overall protection program relative to a set of things that are generally found to be present in well-protected environments and absent in poorly protected ones. The typical areas of inquiry include management, policy, standards, procedures, documentation, audit, testing, technical safeguards, personnel, incident handling, legal, physical security, awareness, training, education, and organization. Other similar studies are done from perspectives of integrity, availability, confidentiality, and use control, or from the informational, physical, or systemic perspectives. In all of these sorts of studies, the effort is directed toward assuring that the necessary factors are present for success. Where shortfalls are found, they are identified and addressed by management. These sorts of studies tend to be done periodically with expert assessment of the quality of the operation relative to each of these areas. Protection posture assessments can be combined with detailed analysis methods to cover specific situations with higher assurance.

Scenario-based risk assessment

Scenarios are generated to try to cover important portions of the space of possible events and outcomes. These scenarios can be “gamed” to explore options and generate group consensus on options for dealing with the risks. These games typically generate stronger group cohesion among the key players who are responsible for making decisions about risk management strategies, and help the group members act in concert when events occur. This carries the added benefits of generating management buy-in, training participants in how to respond, and gaining mutual understanding to facilitate future cooperation. Results are generally compiled by those operating the scenarios and then turned into reports with risk management options and analysis. Those reports are then translated into decisions by management and carried out by participants. Games such as this are run in-house by many companies and expert-facilitated games of this sort are offered by a limited number of consulting organizations in the marketplace.

Covering approaches to analyzing protection

A covering approach is sometimes used for analyzing protection. The objectives of this approach are to provide a method of determining if a set of known attacks is “covered” by defenses and to find redundancies in coverage either to assure added coverage or to determine which protective methods can be reduced or eliminated while still covering identified attacks. Covering analysis stems from theoretical concepts that underpin optimization of digital logic designs and has a strong mathematical basis. The analysis is relatively simple to carry out and the results are straightforward to understand and apply. This technique is commonly used for combinational analysis situations rather than sequential situations. A more advanced approach using this model seeks to find the least expensive way to reduce or eliminate paths between the attacker and their goal. This approach also has the event-enumeration problem. The event enumeration problem involves the difficulty of identifying every possible sequence of events that can take place, associating consequences with these event sequences, and developing metrics for dete4rmining which event sequences are covered to what extent by each protective measure used.

Game theoretic approaches

Another analytical approach is based on game theory. In game theory, the game designer generates a set of game trees with expected outcomes for participants making sequences of “moves.” Without assessing the likelihoods of events, outcomes of different event sequences can be identified and ways to cut harmful sequences can be sought by selecting protective measures. This is different from the covering approaches outlined earlier because it allows response processes and timing to be taken into account. Optimized outcomes based on mathematical or numerical analysis of these games can be found. A good example of an analytical technique commonly used assumes we want to limit the worst-case loss to some fixed value. Options for placement of the least expensive protective measure that meets the requirement of worst-case loss can then be determined. There are well-known solutions to many of these min-max problems for select classes of games.

Systems analysis

Another model that has been applied in high-risk situations is “systems analysis.” This model is limited to high-risk situations because it is expensive and time consuming and, thus, the cost of analysis becomes a significant part of the overall protective cost. This model uses a systematic and detailed analysis of all sequences of events and interactions between interdependent parts of all systems under consideration. It is not practical for detailed use in a large modern infrastructure, although in critical infrastructure protection, the consequences may be high enough to justify its use. It is more typically used for analysis of control systems for chemical plants and similar situations in which there are limited information systems with well-defined functions controlling assets with risk to human life if these systems fail. Typically, these situations require redundant coverage of critical faults to a defined level of redundancy, extensive testing, and fail-safes to mitigate worst-case losses. This applies to CLIENT only if there are high consequences situations that justify this level of detailed analysis.

Consequence analysis

Consequence analysis is the first thing that risk management must do in gaining a detailed understanding of risks. The process for developing consequences involves interviews with top management and those responsible for each system, determining the losses associated with loss of integrity, availability, confidentiality, control over use, and accountability as a function of time, determining expected times for detection and mitigation of loss, and determining losses if detection or mitigation fails. A threshold for significant loss is determined by top management and for all significant losses, further analysis is done. For all insignificant losses, those losses are collected in a list of losses to be accepted by management and management must sign off that they have decided to accept those losses should they occur.

Threat analysis

After consequences are analyzed, for consequences of sufficient magnitude to be worthy of further investigation, threat analysis should be undertaken. Management must set a threshold for high consequences, and all other consequences worthy of consideration are treated as medium consequences. Threat analysis should involve a mix of techniques suited to the specifics of the threat environment. Enterprises should have the capacity to use any of these techniques in the appropriate context and the following table summarizes the contexts in which each should be applied.

Method	Consequence	Time	Threat	Cost
By type at a generic level	Medium	Short	Medium	Low
By type with classes inside groups	Medium-High	Medium	Medium-High	Medium
By type with classes and detailing for high relevancy	Medium-High	Medium-Long	Medium-High	High
Known Vulnerability Indications and Warnings	Medium	Short	Low	Low
Detailed Intelligence Analysis	High	Long	High	High
Investigation-based	Medium-High	Medium	Medium-High	Medium-High

Table 1: *Threat Analysis Techniques and Parameters*

More detailed information on threat analysis methods is available in [LIMITED ACCESS THREAT ANALYSIS REPORT CITED HERE]. An initial review of threats by type at a generic level was performed as part of this report and is included below. This is a preliminary review that meets minimum requirements for a generic by type review. For medium consequence items, a medium or high rated technique can be used. For high consequences, a high rated technique must be used. After the initial analysis of threats by generic type, for threats identified as highly likely to have capabilities and intent to attack CLIENT, techniques rated for high threats must be used. Based on these results, a threat analysis paper should be generated for CLIENT and updated at least yearly. Incidents, both within CLIENT and elsewhere in the world, should inform the threat analysis process, and specific CLIENT incidents should trigger investigation-based updates to the analysis.

Based on threats and consequences, top management should be provided with options to accept, avoid, transfer, or mitigate risks and the risk management group report must identify the costs and consequences associated with each of the available options for each medium or high consequence.

Vulnerability analysis

The vulnerability analysis process is only undertaken in cases where the consequences and threats are great enough to justify a detailed analysis of vulnerabilities. This is done only after it has been determined that risk mitigation is either desired or a viable option for the particular

consequence under consideration. At that point, vulnerability assessment is to be undertaken by a qualified vulnerability assessment firm. This assessment is not the same as a penetration test or a test for known technical vulnerabilities. It must cover all aspects of protection, including but not limited to physical, operations, communications, and information security and must address all paths that can induce the identified consequences. This includes paths involving collusions of multiple insiders and consequences generated by aggregated interdependencies.

Selection of mitigation approach

The key decisions in RM are associated with risk acceptance, risk mitigation, risk transfer, and risk avoidance. Risk acceptance is the most common mode of operation today and it results in the staggering losses we see in the marketplace. When risk management is not properly carried out, residual risk is accepted by default. When proper risk management is undertaken, residual risk is quantified and understood by the decision makers. Risk transfer typically involves insurance of some sort, but risk is indirectly transferred to shareholders when a risk is accepted. Risk mitigation typically involves the implementation of a variety of safeguards intended to reduce risk while leaving an acceptable or transferable residual risk. Risk avoidance is practiced when other alternatives are unacceptable, and usually results in not pursuing opportunities.

Acceptable	Transferable	Reducible	Action
No	No	No	Do not engage in this—avoid the risk
No	No	Yes	Propose reduction and re-evaluate
No	Yes	No	Insure or avoid the risk
No	Yes	Yes	Balance reduction with insurance cost
Yes	No	No	Accept or avoid the risk
Yes	No	Yes	Balance reduction with acceptance cost
Yes	Yes	No	Accept or avoid the risk
Yes	Yes	Yes	Balance all three and optimize

Table 2: *The Forms of Risk Mitigation*

The form of risk mitigation to be taken can be decided by a relatively simple process. Table 2 provides guidance by indicating situations under which risk should be accepted without further mitigation, transferred to insurance or some other party, reduced by protective measures, or avoided by not pursuing the business opportunity. A more complex analysis can be done by weighting acceptability, transferability, and reducibility, and applying metrics, but the cases where such analysis is helpful are quite rare.

Specific mitigations

The selection of specific mitigation methods is an organizational process and should be undertaken in a timely fashion to best determine specific mitigations, costs, and residual risks. The specific mitigation costs and residual risk is then balanced against risk management options to verify that mitigation is appropriate and adequate in context.

Specific issues mandated by policy

CLIENT policy identifies specific risk management requirements. The fulfillment of these requirements is identified here in terms of what part of the policy they relate to, what the requirements are, and what approach should be taken to perform the required analysis.

General requirements

A general requirement that risk management be applied to evaluate all exceptions to policy goes across all of the policy areas in CLIENT. The policies developed for CLIENT were based on the ISO 17799 standard and there are not specific policy requirements associated with elements 1 or 2 of the ISO standard. However, for consistency in numbering, ISO elements were associated

with sub-policy numbers within the overall policy framework. Therefore sub-policy elements 3-12 are identified in the current CLIENT policy documents.

Sub-policy 3 – Information Security

Section 2.1.2.b - Cost & Impact - indicates that business efficiency will be considered in implementing controls. Therefore, risk management processes should consider cost and impact and should seek business efficiency by using more cost-effective methods over less cost-effective methods.

Section 2.1.2.c - Effects of Changes to Technology - requires that at least one full-time equivalent member of the risk management team be dedicated staying informed about changes in network and security technology. Appropriate education and experience is required for this position and the individuals comprising this component of the team should use access to research and advisory services as leverage in efficiently carrying out this task.

Section 2.1.1.c - Business Continuity Management - requires that business continuity considerations be used to determine what additional resources and capabilities are needed beyond those used for normal operations to determine how much redundancy to apply.

Sub-policy 4 - Access Control

Section 2.1.8 - Independent Review of Information Security: Internal Audit - indicates that internal audit independently evaluates risk management practices through periodic examinations of procedures. To support this process, the risk management process should document its decisions in a manner amenable to this review.

Section 2.2.1 - Identification of Risks from Third Party Access – mandates that risks associated with network and physical access by third parties be considered in risk management.

Section 2.2.1.a.5 - Monitoring Third Party Service Providers – indicates that third party risk management should include contractual provisions.

Section 2.2.1.a.6 - Subordinate CAs For External Organizations – indicates that risk management should review in detail any case where NS acts as a subordinate Certificate Authority (CA) of an external organization. This requirement indicates that at least scenario-based or covering approaches must be used, and if the consequences are high, systems analysis will be required.

Section 2.2.1.a.7 - Cross-Certification of CAs – requires that if a CLIENT Certificate Authority (CA) must cross-certify an external CA, an extended risk assessment must be done by the PKI team, Legal, Audit, and CIS, The results of this extended assessment will be used in the risk management process.

Section 2.2.1.e - Types of access – implies that risk parameters associated with physical and logical third party access will be defined by the RM activity. It also identifies that the preferred sort of access is the one that lowers risk and indicates the need to trade off cryptographic coverage and its limitations with physical access and its limitations.

Section 2.3.1 - Security requirements in outsourcing contracts – indicates that before outsourcing involving Network Infrastructure or Network Traffic (as defined in the policies) a risk analysis must be included along with other business criteria for management decision-making. The specific analytical method should be based on risk levels associated with the activity and the systems affected. In this case it will be useful to leverage pre-existing information on threats, vulnerabilities, and consequences, to identify the specific issues associated with the particular outsourcing, and

to create a mini-assessment based on existing assessments related to Network Infrastructure and Network Traffic.

Sub-policy 5 - Asset Classification and Control

Section 2.2.1 - Classification Guidelines - Classifications and associated protective controls require risk management to consider business needs and risks

Sub-policy 6 – Personnel Security

Section 2.1.1 – Security in Job Definition and Resourcing – includes indirect risk management input into appropriate personnel security checks.

Section 2.1.2 - Personnel Screening and Policy – includes requirements for definition of the process for clearance determinations, again with input from risk management.

Sub-policy 7 – Physical Security

Section 2.1 – Physical Security - indicates that risk management should specify physical security requirements.

Section 2.1.1 - Secure Areas – indicates that physical barriers commensurate with risks should be used for systems containing sensitive, high-value, network control, or network audit information.

Section 2.1.2 - Physical Security Perimeter – indicates that risk management will dictate the criteria for the use of physical security zones in CLIENT. The principle requires that different zones must use different protection mechanisms such that a single vulnerability or failure in authorization or configuration cannot cause a protection failure that affects multiple zones protecting the same physical site or asset. Exceptions must be justified and filed where they will be available to each subsequent risk analysis associated with that asset and reconsidered in full detail at every subsequent review. Physical barriers, including walls, must also be evaluated during a risk analysis as barriers to entry and for fire and flood, to determine if it is necessary for them to be attached to a structural ceiling or floor (rather than a suspended ceiling or floor).

Section 2.1.3 - Physical Entry Controls – indicates that the appropriateness of additional controls for physical security are a risk management function.

Section 2.1.4 - Securing Offices, Rooms, and Facilities – indicates a mandatory risk management process associated with the creation, maintenance, and operation of a secure area. This includes:

- Site security for buildings, facilities, and equipment,
- Decisions about intruder detection systems and regularity of testing above and beyond policy mandates
- Decisions about selection of multiple technology sensors
- Coverage of unoccupied areas.
- Distance requirements for hazardous or combustible materials from secure areas.
- Distance requirements for fallback equipment and back-up media

Section 2.1.6 - Isolated delivery and loading areas – indicates a requirement that adequacy of security controls over delivery and loading areas are determined by risk management.

Section 2.2.1 - Equipment sitting and protection – indicates that any events or event sequences found from Business Continuity Management analysis must take into account threats that are identified to the Network Infrastructure through the threat assessment process. Impacts of disaster happening in nearby premises must also be considered.

Section 2.2.5 - Security of Equipment off-premises – includes risk considerations of the use of off-premises equipment.

Sub-policy 8 – Operational Management

Section 2.1 - Operational Procedures and Responsibilities – indicates that RM must identify where segregation of duties is required to reduce the risk of misuse.

Section 2.1.5 - Separation of Development & Operational Facilities – indicates specific requirements for separation that apply to this issue.

Section 2.1.6 - External Facilities Management – indicates that risks associated with third party contractors must be identified in advance and requires contractual mitigation as a minimum. Specific requirements include:

Identifying sensitive or critical applications more suitably retained in-house;
Implications for business continuity plans;
Adequacy of required security standards, practices, and processes for meeting and measuring compliance;

Section 2.2 - System Planning and Acceptance – mandates that risks management verify that advanced planning is adequate to mitigate against systems failures to ensure the availability of adequate capacity and resources.

Section 2.3 - Protection against Malicious Software – mandates taking all necessary and prudent precautions to deter, prevent, detect, react, and adapt to the introduction of malicious software in any of its systems. But section 2.3.1 - Controls against malicious software – mandates that protection against malicious software be based on system selection, configuration management, change control, system access mechanisms, and security awareness. Risk management should determine the specific tradeoffs associated with combinations of these factors and identify specific systems, configurations, and contexts appropriate to specific environments.

Section 2.6 - Media Handling & Security – requires that appropriate operating procedures be established to protect valuable content from corruption, loss of utility, leakage, or unauthorized, inappropriate, or unaccounted for use. Evaluation of these procedures for suitability is a risk management function subject to policy requirements of sub-sections of 2.6.

Section 2.7.2 - Security of Media in Transit – indicates the need to identify and evaluate transport and courier methods and individuals or companies, adequacy of background checks in use, appropriate controls for sensitive and high-valued content in transport, and encryption adequacy and use in this context.

Section 2.7.5 - Security of Electronic Office Systems – mandates that risk management evaluate all NS offices to determine proper classification of those systems and their content and to identify appropriate control mechanisms associated with those systems.

Sub-policy 9 – Policy access control

Section 2.1.7.3 - User password management – indicates that risk management must determine the propriety of use of authentication technologies.

Section 2.1.9.3 - User authentication for external conditions –indicates that risk management must determine the authentication method requirements for access by remote users to any non-generic non-publicly distributed NS content.

Section 2.1.9.4 - Node Authentication – indicates that risk management must determine the authentication method requirements for computer-to-computer connections.

Section 2.1.10 - Operating system access control – implies that risk management should identify reasonable, necessary, and prudent methods to prevent unauthorized computer access to computers containing, processing, or using CLIENT sensitive, high-valued, network control, and

network audit information. It also indicates that risk management should evaluate certain access control methods in these systems.

Section 1.10.1 - Automatic terminal identification – indicates that risk management should identify needs for automatic terminal identification.

Section 1.10.2 - Terminal log-on procedures – indicates that risk management should identify adequate identification and authentication requirements for secure access to sensitive, high-valued, network control, and network audit information.

Section 1.10.3 - User Identification and Authentication – indicates a similar requirement for all other information.

Section 1.10.8 - Limitation of Connection Time – identifies risk management as the process that determines the need for restrictions on connection times to NS sensitive, high-value, network control, or network audit systems.

Section 1.12.2. - Procedures and Areas of Risk – identifies that the type of monitoring required for individual facilities is determined by risk management. Risk factors should be reviewed with a frequency based on:

the criticality of the application processes;
the value, sensitivity or criticality of the information involved;
the past experience of system infiltration and misuse;
the extent of system interconnection (particularly public networks).

Sub-policy 10 – Systems development and maintenance

Section 2.1 - Security requirements of system – indicates that risk management framework is defined in this document and that requirements and controls reflect the business value of the information assets involved and the potential business damage which might result from a failure or absence of security. Hardware, software, and facility selection must be at least as secure as warranted by the risks associated with those systems. More secure systems must be selected unless the lifecycle costs of the less secure system, including indirect and consequential damage, is demonstrated through the risk management process to be less than the price differential. This means that risk management must be invoked in order to make such decisions. The owner of CLIENT oversees the RM process and communicates results the management information security forum for their review.

Section 2.2 - Security in application controls – indicates that risk management should indicate control requirements for all non-sensitive systems.

Section 2.2.3 - Message Authentication – indicates that for high-valued and sensitive CLIENT information and systems, risk management should determine which transactions require message authentication.

Section 2.3.1 - Policy on the Use of Cryptographic Controls – requires that risk management should determine the suitability of cryptographic techniques.

Section 2.3.2 – Encryption – indicates that risk management is responsible for identifying encryption requirements, taking into account the type and quality of the encryption algorithm used and the length of cryptographic keys to be used. Risk management is also responsible for determining the adequacy of physical controls necessary to not require encryption of CLIENT sensitive, high-value, network control, and network audit information.

Sub-policy 11 – Business Continuity Management

Section 2.1.1 - Business Continuity Management Process - indicates the requirement for a business continuity plan (BCP) development, maintenance, and operation process based on; (1) Identification and prioritization of critical business processes; (2) Understanding the consequences that interruptions are likely to have on the business; (3) Considering the risk transfer, acceptance, avoidance, and mitigation options; (4) Formulating and documenting a business continuity strategy; (5) Formulating and documenting business continuity plans in line with the agreed strategy; (6) Regular testing and updating of the plans and processes put in place; and (7) Ensuring that the management of business continuity is incorporated in the organization's processes and structure. BCP reviews are at least once per year.

Section 2.1.2 - Business Continuity and Impact Analysis - Business continuity shall include identifying sequences of events that can cause substantial negative consequences to WF, including, but not limited to, sequences involving backup theft, corruption, or destruction, breaking key management systems, cable cuts, cascade failures, collaborative misuse, content-based attacks, data diddling, dependency analysis and exploitation, de-synchronization and time-based attacks, device access exploitation, distributed coordinated attacks, earth movement, electronic interference, emergency procedure exploitation, environmental control loss, environment corruption, error-induced mis-operation, errors and omissions, excess privilege exploitation, false updates, fictitious people, fire, flood, hardware failure - system flaw exploitation, illegal value insertion, imperfect daemon exploits, implied trust exploitation, inadequate maintenance, induced stress failures, infrastructure interference, input overflow, insertion in transit, interrupt sequence mishandling, invalid values on calls, man-in-the-middle attacks, modeling mismatches, modification in transit, multiple error inducement, network service and protocol attacks, peer relationship exploitation, perception management a.k.a. human engineering, piggybacking, power failure, privileged program misuse, process bypassing, protection mis-setting exploitation, race conditions, reflexive control attacks, relocation, replay attacks, resource availability manipulation, restoration process corruption or misuse, severe weather, simultaneous access exploitations, solar flares, spoofing and masquerading, deceptions, sympathetic vibration, system maintenance, testing, Trojan horses, undocumented or unknown function exploitation, viruses, volcanoes, and wire closet attacks.

This shall be followed by a protection posture assessment to determine the threats that can induce these consequences, the vulnerability to these events, and the magnitude and nature of the consequences of these sorts of event sequences. Assessment shall include lifecycle issues and impact of these event sequences in terms of time and cost to recover and business impact during those times. This assessment shall be carried out with full involvement of CLIENT owner and relevant staff members. This assessment must include the analysis of system interdependencies, effects of risk aggregation, and dependencies on non-CLIENT information and non-information resources. This assessment shall include all CLIENT business processes, must be reviewed at least once per year, and must be repeated at least once every three years or when substantial changes to the Network Infrastructure warrant re-examination as determined by CLIENT owner.

Based on the results of the protection posture assessment, a business continuity plan shall be developed, maintained, operated, and tested to assure that under every reasonably foreseeable event sequence that can be mitigated for aggregated costs within the reasonable value of the business, business continuity is assured.

Sub-policy 12 - Compliance

Section 2.2.1 - Compliance with Security Policy – includes the requirement for regular reviews including a regular schedule of risk management reviews.

Section 2.2.2 - Technical Compliance Checking - verifies that risk management decisions are being carried out. This includes review of standards being applied.

Section 2.3.1 - System Audit Controls – requires that disruption risks are minimized in testing and auditing.

A schedule of risk management activities

Threats and consequences have a way of changing over time. This means that risk management decisions must be revisited over time. Table 3 illustrates typical intervals between risk management assessments, based on threat and consequence levels. These intervals are normally based on the rate at which the consequences of change don't exceed levels management is willing to tolerate without notice. If the consequences of change are high enough to warrant management attention, then security managers need to reassess the risk, as well as the mitigation approaches they're using.

	Low Consequence	Medium Consequence	High Consequence
Low Threat	Mid-level mgmt updates annually	6-month review cycle, top mgmt update annually	Should not occur – threats are higher
Medium Threat	Mid-level mgmt update 9-12 months	3-9-month review cycle, top mgmt update quarterly	Continuous top mgmt updates monthly
High Threat	Should not occur—not worth operating	3-6-month review cycle, top mgmt update quarterly	Continuous top mgmt updates monthly

Table 3: *When to Reassess Risks*

All substantial incidents should trigger reviews to assure that they are within the risk management profiles set for allowable incidents and incident rates. Vulnerabilities may also be uncovered over time or induced by changes, but if the process of risk management is properly done, changes such as these should not require reassessment, but rather should fall within identified tolerances. CLIENT time frames will be based on the medium and high consequence columns and the medium and high threat rows. Other areas will not be analyzed in detail.

Initial conditions

The RM process depends on the following information being provided to the RM team:

Management must set threshold of significant loss
Management must set a threshold for high loss
Management must have adequate and appropriate personnel dedicated to RM
Management must provide adequate funding for the RM activity
Management must provide organizational mandate for cooperation with RM
RM information is to be treated as high-valued information in a compartment of its own

Management Decisions and Approvals

For insignificant losses, management must agree to accept those losses in writing or determine the level of significance should be changed.
Management must identify criteria for selection of transfer, acceptance, avoidance, and mitigation and must determine which combinations of techniques should be applied to each medium and high consequence event identified.
Management must allocate adequate budget to carry out whatever RM decision they determine to be appropriate.
Management must oversee the RM process and ensure that it is operating properly.
Management must determine when changes to this process should be made and what those changes are

Reviews of the following should adhere to the appointed schedules indicated; or when deemed necessary subsequent to a security incident and or breech.

Reviews to be conducted:

Table 4 provides the list of RM reviews to be undertaken, the periodicity or other conditions of their review, and references to the source of the requirements. RM indicates this document, * indicates all policies have this requirements, while other sources refer to NS sub-policies and their respective sections. Periods are expressed in months. When an additional number is included in parentheses this is the number of months for high-consequence systems. PS stands for pre-signing, LC stands for laws change, and SI stands for a significant incident. RM approval before operation begins and prior to acceptance of any significant change is implied for all issues identified here. RM integration with CLIENT change management system must reflect this.

#	Requirement	When	Reference
1	Information protection posture assessment	36 (18)	RM
2	Review cost and impact metrics and values	SI, 18	3: 2.1.2.b
3	Review technology changes and impact on assessment	SI, 6	3: 2.1.2.c
4	Review business continuity management plan	SI, 12 (6)	3: 2.1.1.c
5	Supply RM documents to internal audit and apply feedback	12 (6)	4: 2.1.8
6	Review risks from third party access for each contract	PS, 12 (6)	4: 2.2.1
7	Review external subordinate certificate authority risks	PS, 6 (3)	4: 2.2.1.a.6
8	Review and update risk profiles for outsourcing contracts	PS, 12 (6)	4: 2.3.1
9	Risk management review of asset classification guidelines	SI, 12 (6)	5; 2.2.1
10	Provide requirements for background checks and risk metrics	LC, SI, 12	6: 2.1.1
11	Provide clearance guidance for personnel	SI, 24 (12)	6: 2.1.2
12	Revisit risk management decisions on physical barriers	SI, 12 (6)	7: 2.1.2
13	Review entry control augmentation requirements	SI, 12 (6)	7: 2.1.3
14	Office, room, and facility security protocol review	SI, 12 (6)	7: 2.1.4
15	Isolated delivery and loading areas review	SI, 24 (6)	7: 2.1.6
16	Equipment sitting and protection review	SI, 24 (6)	7: 2.2.1
17	Review risk profiles for off-premises equipment	SI, 6(3)	7: 2.2.5
18	Segregation of duties review	SI, 12(6)	8: 2.1
19	Separation of development & operational facilities review	SI, 12 (6)	8: 2.1.5
20	Review adequacy of required third party controls	SI, LC, 12(6)	8: 2.1.6
21	Verify adequate planning for capacity and availability	SI, LC, 12(6)	8: 2.2
22	Review and recertify tradeoffs justifying lower surety systems	SI, LC, 6 (3)	8: 2.3
23	Review media handling and security procedures	SI, LC, 12(6)	8: 2.6
24	Review media in transit adequacy	SI, LC, 12(6)	8: 2.7.2
25	Office system classification and control review	SI, LC, 12	8: 2.7.5
26	Review propriety of authentication technologies	SI, 12 (6)	9: 2.1.7.3
27	Review external authentication technologies	SI, 12 (6)	9: 2.1.9.3
28	Node authentication technology review	SI, 12 (6)	9: 2.1.9.4
29	Operating system access control reviews	SI, 12 (6)	9: 2.1.10
30	Automatic terminal identification adequacy review	SI, 12 (6)	9: 1.10.1
31	Terminal log-on procedure review	SI, 12 (6)	9: 1.10.2
32	Limitation of connection time review	SI, 12 (6)	9: 1.10.8
33	Review of procedures and areas of risk	SI, 12 (6)	9: 1.12.2
34	Security in application controls review	SI, 12 (6)	10: 2.2
35	Message authentication transaction review	SI, 12 (6)	10: 2.2.3
56	Cryptographic controls review	SI, 12 (6)	10: 2.3.1
37	Review of new encryption standards for possible changes	SI, 12 (6)	10: 2.3.2
38	Identify and prioritize critical business processes	SI, 12 (6)	11:2.1.1
39	Understand consequences of interruptions and other effects	SI, 12 (6)	11:2.1.1
40	Evaluate risk transfer, avoidance, acceptance, and mitigation	SI, 12 (6)	11:2.1.1
41	Provide risk-related documentation for the BCP process	SI, 12 (6)	11:2.1.1
42	Review BCP to reconcile with other RM issues	SI, 12 (6)	11:2.1.1
43	Review RM process to verify compliance with policy	SI, 12 (6)	11:2.1.2
44	Management review of RM process	SI, 12 (6)	12; 2.2.1
45	Review of standards in use for RM adequacy	SI, 12 (6)	12; 2.2.2
46	Review of audit processes for minimum risk	SI, 12 (6)	12; 2.3.1

47	Legal compliance reviews	SI, 12	12; 2.1
48	Review and re-perform consequence assessments	SI, 12 (6)	RM
49	Review and re-perform threat assessments	SI, 12 (6)	RM
50	Perform vulnerability assessments	SI, 12 (6)	RM
51	Review of the risk management process	36 (18)	RM
52	Audit that the process is properly performed	12 (6)	RM
53	Review time requirements in risk management process	36 (18)	RM
54	Review of all exceptions	SI, 12 (6)	*; 3.2
55	Review changes for risk management impacts	SI, 12 (6)	RM

Table 4: *Risk management activities and timing*

Reporting requirements

The translation of the RM process identified here into existing reporting requirements should be fulfilled by listing identified medium- and high-risk event sequences. The probability field should indicate annual likelihood based on historical data or “n/a” if historical data is inadequate. If at least one incident occurred in the last year, the probability is ‘1’.

An initial threat basis

In order to provide an initial baseline for threat assessment, the following initial generic threat assessment relative to CLIENT has been undertaken. This threat basis must be revisited periodically per the schedule above and is only applicable to medium consequence situations. In addition, threats indicated here as medium or high should be reassessed using the techniques identified in the "Threats" section above and on a schedule indicated above. The generic threats identified here are only an initial starting point for assessment and are based on typical values across a broad spectrum of industries and locations. Appendix 1 provides more detailed information on each of the threats identified here.

Threat type	$Funding/job	Size	Motive	Rating	Access
Activists	10000	1 – 10000	Justice	Low	Insider
Club initiates	100	3 – 50	Acceptance	Medium	Internet
Competitors	>100000	2 – 5	Money	Low	Industry
Consultants	0	1	Money	High	Insider
Crackers	1000-100000	1 – 100	Malice	Medium	Internet
Crackers for hire	>100000	1 – 10	Money	Medium	Internet
Customers	1000	1 – 5	Money	Low	Partner
Cyber-gangs	<1000	10 – 100	Money	High	Internet
Deranged people	Usually small	1	Insanity	Low	Internet
Drug cartels	10M+	100-50000	Money/Power	Medium	Internet
Extortionists	100-10000	1 – 10	Money	High	Internet
Fraudsters	100 – 100000	1 – 20	Money	High	Internet
Government agencies	>1B	>10000	Patriotism	Medium	Insider
Hackers	100-10000	1 – 10	Exploration	Low	Internet
Hoodlums	100 – 10000	2 – 20	Money	Low	Internet
Industrial espionage	10000 – 100000	1 – 5	Money	Low	Industry
Information warriors	>100M	1 – 10000	Patriotism	Low	Insider
Infrastructure warriors	1B+	5 – 100	Patriotism	Low	Industry
Insiders	1000	1 – 5	Money/Revenge	High	Insider
Maintenance people	100	1 – 5	Money	Medium	Insider
Military organizations	1B+	5 – 500	Patriotism	Low	Industry
Nature	Unlimited	Unlimited	Randomness	High	Unlimited
Organized crime	>10000	1 – 5	Money	Medium	Internet
Paramilitary groups	10000 – 100000	5 – 25	Fun/Beliefs	Low	Internet
Police	1000 – 10000	1 – 500	Justice	Low	Industry
Private investigators	100 – 10000	1 – 10	Money	Low	Industry
Professional thieves	10000 – 100000	1 – 3	Money	High	Industry
Reporters	1000 – 10000	1	Exploration	Low	Internet
Terrorists	10000 – 100000	5 – 50	Religion / Power	High	Internet
Tiger teams	$15K-$150K	3 – 5	Money / Pride	Low	Industry
Vandals	0	1 – 10	Randomness	Medium	Internet
Vendors	1K-1M	1 – 20	Money	High	Insider
Whistle blowers	0	1	Justice	Low	Insider

Table 5: *Initial threat basis*

Summary

This report provides a process for risk management within CLIENT that is consistent with the new policies provided as an earlier deliverable within this overall effort. In addition to providing processes, this report consolidates the risk management activities associated with the policies into a single reference point to allow the risk management activity to proceed in a systematic way with a rapid startup. References are maintained throughout the process table that describes how often what activities need to be done, so that the individuals tasked with risk management can both find and read the underlying material for reference, and update the requirements in this process as changes are made over time to the policy elements that effect risk management process. Processes have been identified for differentiating three different levels of consequences and associating those consequence levels with requires threat and vulnerability assessment processes so as to minimize waste while providing a process that yields meaningful risk management. This report enables knowledgeable individuals with proper background and training to build the risk management program for CLIENT rapidly, starting with much of the initial work already completed.

Appendix 1 – Threat details

Each identified in the matrix in Table 4 is rated here as low (L), medium (M), or high (H) relative to the context of CLIENT.

[REDACTED]