impruve
MANAGE RISK, MAXIMIZE REWARD

Synergy in Security

Why a combined ISO 17799 and OCTAVE approach makes sense

impruve
MANAGE RISK, MAXIMIZE REWARD

Synergy in Security
Why a combined ISO 17799 and OCTAVE approach makes sense

Table of Contents

Management Summary

Information systems today resemble museums more than medieval castles. The castle description of information security describes a perimeter-centric model of inside and outside. This doesn't apply as eInitiatives, third party support and outsourcing requires the perimeter to become *porous*. Like a museum, the challenge is to identify the critical assets and protect not just the perimeter of the network, but those assets as well.

An ideal approach would be one that integrates the audit, risk assessment, recommendations and strategy into a single system. It would offer a non-proprietary, tested methodology that could be replicated. The audit and risk assessment would also clearly define the mission critical elements; this makes the prioritization process in the recommendations and strategy deliverables straightforward. This is exactly the solution this paper outlines.

Impruve has developed an approach using elements of the Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) methodology developed at Carnegie Mellon University's Software Engineering Institute. The institute also manages the Computer Emergency Response Team (CERT), and is considered one of the most respected centers for information security in the world.

Impruve has combined OCTAVE with the global standard for information security – ISO 17799. The reasons to adopt this standard are the following:

1. Information security must be addressed holistically, if we focus on cyber security while ignoring physical security, we are not secure. The converse is also true.

2. The real cost of security is the cost of managing security. If we address security in a piecemeal fashion, it becomes more and more difficult to organize the various aspects – hence more difficult and expensive to manage. If we approach security from an architectural perspective, we can organize and manage much more efficiently.

3. The standard is globally recognized. Whatever national, regional, local or industry compliance issues we must adhere to – the standard has been and can be tailored to accommodate.

4. As the international standard, the adopting organization has a highly defensible and credible position if asked reasons for choosing this approach.

5. Should business to business issues come up, clients can point to the standard when discussing security with our trading partners.

6. Transference of risk may be of interest to us as a risk mitigation vehicle. The following companies provide cyber insurance and base the application process (in part) on ISO 17799 compliance: AIG, Zurich, Chubb, St. Paul, Progressive, and Lloyd's.[1]

[1] Electronic Security: Risk Mitigation In Financial Transactions, Public Policy Issues. Thomas Glaessner, Tom Kellermann, Valerie McNevin. World Bank Publication, June 2002. Page 41.

The Impruve approach includes audit, recommendations, strategy guidelines, and a risk assessment. The assessment is not simply a vulnerability assessment, but includes areas outside of the IT/IS boundaries. The assessment also involves the community. This offers several benefits:

- Provides security awareness and training. This goes beyond slogans or simple awareness campaigns, instead it ties security directly into the work performed. Risk becomes *relevant* to the worker's job.
- Mitigation, in the form of policy or technology, is readily understood and adopted. Security is everyone's job. The transformation extends beyond the information systems organization.
- Risks, threats and vulnerabilities are uncovered that may be obvious to the user community but less obvious to the information technology professionals. The assessment is more complete.

At first glance, this may appear to increase the complexity of the solution. In fact, it does not. The added effort is two tasks:

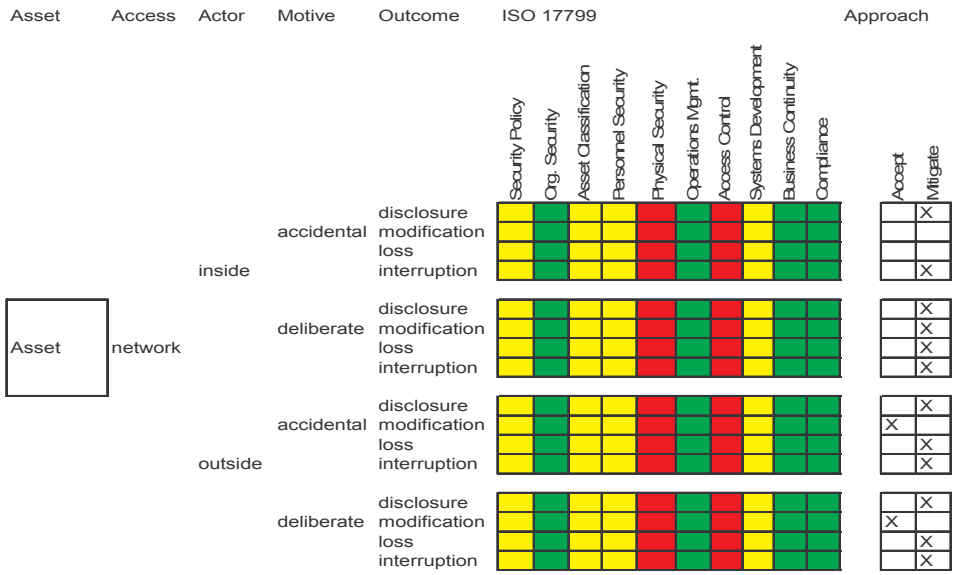
1. Risk tolerance – an analysis of the organization's tolerance for risk. What is a "high" risk event? What is a medium? A low risk event? This is a quick exercise that is used to prioritize the mitigations and can be reused with follow-on assessments.[2]
2. Identifying and defining the assets of the organization. Not just the applications and systems, but also the information assets. Which would be considered the critical assets? This is necessary for compliance to the global information security standard and for development or review of a Business Continuity Plan.

We assign a simple grading scheme to map organizations to 17799. In this case a "Green" would indicate addressed, a "Red" not addressed, and a "Yellow" somewhere in between. The audit provides a picture of where the organization is relative to the ISO 17799 framework.

These areas are ultimately mapped to the identified critical assets and used as part of the risk assessment. Further detail on the approach can be found in the Details section of this White Paper. The point is risk mitigation of critical assets is evaluated from a tactical as well as a strategic perspective. The strategic perspective impacts the entire organization. *Even those assets*

[2] A modified OCTAVE process is being used by the U.S. Government as a risk authentication guide for electronic authentication. This service is intended to provide various authentication mechanisms for Government services. Clients can review this work to determine if any of it may be applicable for current or future initiatives. Details are available at http://cio.gov/eauthentication/. The OCTAVE derived risk assessment is termed e-Risk and Requirements Analysis.

not evaluated as one of the critical assets benefit from strategic solutions. The additional benefit is the continual alignment of the organization's security posture with ISO 17799.



These worksheets become "living" documents that can show at a glance the areas that need improvement and the areas where ISO 17799 compliance is addressed.

The approach begins by creating an analysis team. This could include Impruve security professionals as well as members from the client organization. Impruve realizes this is more resources than clients may desire, but time requirements are minimal and can be tailored to particular environments. Ideally one of these members would come from the IT Department and one from another Department. The reasoning is to explore both technical and non-technical issues at the client's organization. Surveys and interviews are also necessary to gather organizational knowledge and perform elements of the audit.

The focus on *information* as opposed to *systems* is, in itself, a major benefit. Information extends beyond system boundaries, it moves to paper, handheld devices and other media. An information focus follows the information flow to highlight these migrations. This cannot be revealed with a system-focused assessment.

The other value that OCTAVE brings to the combined effort is the dynamic nature of the process. Where ISO 17799 is sometimes viewed as a static model, incorporating OCTAVE into the standard allows for subsequent assessments and audits while constantly raising the baseline security posture.

Introduction

Understanding

Impruve understands clients desire to manage information security as a paramount issue. The ability to align to a global standard is an important part of that process. Working with an Information Security Management System (ISMS) such as ISO 17799 allows organizations to address security pro-actively, avoiding the all too familiar habit of information security efforts working in an unmanageable, reactive mode.

Key Security Issues

At a general level, the key security issue for any organization is how to integrate technologies in a secure manner. This includes developing a culture that ensures proper management of these technologies. The involvement of the user community into the design process of a security system improves the appreciation, comprehension, and adoption rate of the security system. As businesses move forward with electronic projects, this respect and comprehension will provide increased value to the organization. Specifically, incorporating proper management of cyber documents has benefited firms in several areas:

- Faster lookup and retrieval of documents
- Ability to automate business processes
- Streamlined collaboration of jointly developed documents

These advantages cannot be realized without the education of the user community – the knowledge workers, with all aspects of information management, including security.

Additionally, the proper management of malevolent software (viruses, worms, Trojans, etc.) make the desktop analysis and mitigation approach (es) relevant. Over the last several years, malevolent software has created the greatest costs to organizations in terms of expense of remediation and sheer effort.[3] In a recent security conference in Silicon Valley, security executives were asked "What keeps you up at night?" The panel, consisting of security officers from Macromedia, McKesson, and Visa responded that their greatest concern in 2004 is Internet worms.[4]

[3] CSI/FBI 2003 Computer Crime and Security Survey, Types of Attack or Misuse in Organizations Reporting Financial Loss (by number). Page 11.

[4] Security Venture Fair, January 21, 2004. Panel members were: Justin Dolly from Macromedia, Patrick Heim from McKesson, and Phillip Maier from Visa.

Details of Approach

This section details the approach to the specific topics outlined in ISO 17799 Any references to ISO 17799 shall be contained in parenthesis, be prefaced by 17799, and cite the clause, e.g. (17799 10.2.1).

Security Audit

Policy Review

The team evaluates the existing security policies at the client organization to compare to the policies outlined in ISO 17799. This involves determining whether a policy exists or another policy within the organization covers the areas outlined in 17799. It also involves structuring both the set of security policies as well as the content contained within the documents themselves.

The policy's effectiveness is measured by survey results and any historical evidence that may be present. It is also measured by both technical and non-technical analysis, in the case of some of the policies.

Impact of existing security controls on business efficiency is determined by surveys as well as interviews with select individuals within the organization. This is part of the ISO 17799 review process for security policies and is done periodically as part of compliance to the standard (17799 3.1.2 b).

Effects of changes to technology provide recognition that new technologies have an impact on the security posture of an organization and possibly on policies. Impruve's general approach is to develop policies in a modular format, so the policies may not be affected as much as the underlying procedures. Appendix A of this White Paper provides greater detail on this modular approach. This is not to say this format must be adhered to, only to suggest an option if the client desires one.

Impruve's philosophy regarding security policies is to take a minimalist approach. Adopt only the absolutely essential policies; as the intent is for the user community to read, understand and abide by the policies – therefore make the effort as palatable as possible. Impruve also recommends organizing policies by audience, unless there is a specific need; restrict the policies that apply to the IT group to the IT staff. Impruve has structured this with the policies referenced in 17799. See Appendix A in this document for more information.

Organizational Security Management

Organization of the existing security management within the client's domain is reviewed. The executive team that reviews the project could be considered a "pilot" Management information security forum (17799 4.1.1). Someone within the client organization,

perhaps the Project Manager, could be assigned as a manager for all security related activities (17799 4.1.1). Impruve recognizes that currently some organizations may not have the resources to commit someone to take responsibility for system security. The recommendation to create an information security position, even if part-time, is submitted as a suggestion.

Third party support contracts and Service Level Agreements (SLA's) are analyzed from an information security perspective. This may result in the recommendation of instituting standards and guidelines for future outsourcing contracts.

Physical and Environmental Security

Inspection of data centers, computer rooms and communication equipment take place as part of the audit portion of the engagement. In previous Impruve audits, one of the findings was simply to rearrange the location of some desks to prevent potentially sensitive documents from casual perusal.

Perimeter security assumes importance as to the level and depths of physical controls that are in place with respect to information technology. Power, cabling, protection against fire and water damage are covered in this area.

Secure disposal or re-use are examined. Procedures regarding clear desk and clear screen are suggested to reduce exposure to potentially sensitive material. Removal of property from the premises and securing equipment off-site are also subject to audit. Support and maintenance procedures are also reviewed.

Communications and Operations Management

This covers the procedures, responsibilities and documentation already in place. System planning and acceptance are reviewed and also feed into the System Development and Maintenance (17799 10) program in place. Specific attention will be given to the strategic systems and the highly sensitive information. In part this is built-in to the risk assessment process. Segregation of duties (to the extent possible) is also reviewed in this area (17799 8.1.4).

The vulnerability analysis reveals any issues related to patch management and timely updates. This is really covered under Operational change control (17799 8.1.2). Incident management procedures are reviewed (17799 8.1.3). Incident response capabilities and documentation will also be assessed (17799 6.3). If there is no formalized Incident Response Plan, one recommendation is to review the documentation available at CERT, specifically the Organizational Models for Computer Security Incident Response Teams (CMU/SEI-2003-HB-001) and the Handbook for Computer Security Incident Response Teams (CSIRTS) (CMU/SEI-2003-HB-002).

Backup and recovery procedures are examined in this area as well as Continuity Planning (3.4.1 g). The risk assessment, because of it's focus on mission critical assets, becomes a sound foundation for a continuity plan. Particular interest is the number of copies that

exist of data, and how each is managed. Additionally, a "time to data" metric is estimated by the participants. Providing clear guidance on the demarcation with the physical security that takes place, a review of management and storage of paper documents is also undertaken.

Access Control

An evaluation of the access controls takes place at the Network, OS, and Appliance level. Applications are reviewed for technical adherence to access control policies. The vulnerability assessment is also used to determine the effectiveness of proper access controls in place. Audit trails are also evaluated as well as being entered in the Compliance section of ISO 17799 (17799 12).

eWorking arrangements will be reviewed and compared to known standards of best practice. In the United States, the American Telecommuting Association, as well as the Institute for the Study of Distributed Work are organizations the Impruve team has worked with in the past.

Systems Development and Maintenance

The team reviews any methodologies that may or may not be in place. System requirements documents should include security considerations. Data and input validation checks should occur to ensure accuracy. Audit controls should also exist within applications.

Cryptographic solutions may be explored if deemed a priority (17799 10.3). Although perhaps not an immediate issue, input is provided as part of the strategic deliverable.

Change control is a key element of Systems development and maintenance (17799 10.5.1). These procedures are reviewed. Knowing that a lot of this work is outsourced, the team evaluates any contracts or service level agreements that may specify adherence to a managed Systems Development Lifecycle (SDLC) process. This would include any software development (17799 10.5.5)

Business Continuity Planning

A review of the disaster recovery plan as well as the business continuity plan is undertaken. The risk assessment portion of the engagement can be used as a foundation for a Business Impact Analysis document if one is missing or outdated. The critical assets and procedures as uncovered in the risk assessment provide a clear indication of where emphasis should be placed if initiating a business continuity plan.

Impruve's emphasis on the role people and processes play in the information scope provides a comprehensive background for a business continuity plan. The scenario approach used to develop threat trees during the risk assessment process evaluates events comprehensively; mitigation focuses on critical system survivability.

Design of a continuity plan includes defining what events might trigger the plan to take effect, procedures to follow in the event of an emergency, fallback and resumption procedures, and responsibilities. System backup solutions, as reviewed, provide input into such a plan. Determinations as to on-site, off-site storage, recovery and test procedures have been shown to reduce the impact of a disaster – even if the disaster in question was not the anticipated event. An overall framework around business continuity is evaluated.

Compliance

Legal requirements are reviewed. Policy reviews (as described in the policy section) serve as inputs into this part of the audit. The team should be fully aware of the regulatory and compliance issues which need to be observed in the deployment of any system dealing with critical information

Technical compliance is also verified. The vulnerability assessment portion of the risk assessment could reveal technical compliance issues that need to be addressed. Audit capabilities are evaluated to determine what is being audited, and the management of the audit records. Typically what we've found in previous engagements was the default audit capabilities of the devices and systems were not modified from factory assignments, and may need adjustment.

Other aspects of the Audit

Impruve views the audit and risk assessment deliverables as concurrent activities. The advantage to this approach is the time savings in terms of not waiting for the audit to complete to begin the risk assessment. The audit takes the form of an ISO 17799 audit in terms of questions used by BS 7799 auditors. A complete set of questions will be reviewed and answered by the analysis team. A subset of questions will be used for the organizational surveys as input into the risk assessment.

Information for the audit will be gathered from surveys, interviews, the technical vulnerability assessment and policy review. The report will be delivered in a 17799 outline structure to provide a solid foundation for a strategy deliverable.

The 17799 categories not covered by the above paragraphs (Asset Classification and Control and Personnel Security) also are addressed to provide a complete gap analysis as part of the strategy deliverable. Addressing Scope and Location issues as initial areas in 17799 are also covered, but this is a minimal effort. It is mentioned here for the sake of completeness.

Risk Assessment

Impruve addresses the risk assessment requirement by integrating the OCTAVE methodology with 17799. This provides a risk assessment deliverable. The documents span the entire organization, and are not limited to the IS/IT confines. It should be emphasised that the use of the OCTAVE methodology is intended to provide a

framework for gathering and interpreting the data as part of the project. Well established and freely available, it is in no way prescriptive, and is simply provided to assist in the production of deliverables benchmarked against industry best practice.

This approach is flexible, does not impose any overheads or expose clients to any proprietary licensing agreement. Furthermore if ISO 17799 Certification should be sought, it is believed that the results of this audit process will clearly indicate what gaps exist between current and required practice.

OCTAVE provides clients with a *repeatable method* which can be re-used, with or without intervention from security consulting organizations – including Impruve. Details on the methodology are covered on the following pages; more information is available at www.cert.org/octave.

An effective risk assessment methodology needs to have a fully-defined and comprehensive processes for identifying the assets and business processes to be protected before the subsequent vulnerability assessment can be conducted. OCTAVE addresses all these components in a very systematic fashion. The entire OCTAVE risk assessment process itself is comprehensive, compliant with ISO 17799, and has a well respected pedigree (developed by CERT & CMU/SEI). This translates into a very credible and defensible methodology for the adopting organization.

OCTAVE separates the activities needed to implement a risk assessment into discrete phases or steps. The deliverables for each key step are identified, and proven project management methods are used to ensure the delivery of these on time and to budget. At each step, the methodology provides templates for the products, plans, checklists and training material.

The OCTAVE methodology consists of a series of steps, backed up by a comprehensive set of documentation templates and checklists, provided in a simple and easy-to-follow format. The sequential OCTAVE processes are:[5]

- Identify Organizational Knowledge
- Create Threat Profiles
- Identify Key Components
- Evaluate Selected Components
- Conduct the Risk Analysis
- Develop a Protection Strategy

The OCTAVE processes are described below.

OCTAVE Process 1 Identify Organizational Knowledge

The first step in implementing a risk assessment solution is to understand the requirements. The questions to be considered during OCTAVE Process 1 include the following:

- *What are the business drivers?*
- *What level of security is appropriate?*
- *Where are the system vulnerabilities?*
- *What are the legal and regulatory compliance constraints?*

OCTAVE Process 1 shows how these requirements can be clearly identified and also considers possible solutions. Once the requirements are known, the next step is to produce a project definition. OCTAVE Process 1 provides a process and set of documentation templates and checklists to:

- Define the valuable assets in the organization
- Determine the gaps if any between organizational security practices and industry benchmarks (ISO 17799)
- Begin to introduce a culture of information security awareness within the organization
- Apply project management techniques to information security
- Produce a detailed project plan.

OCTAVE Process 2 Create Threat Profiles

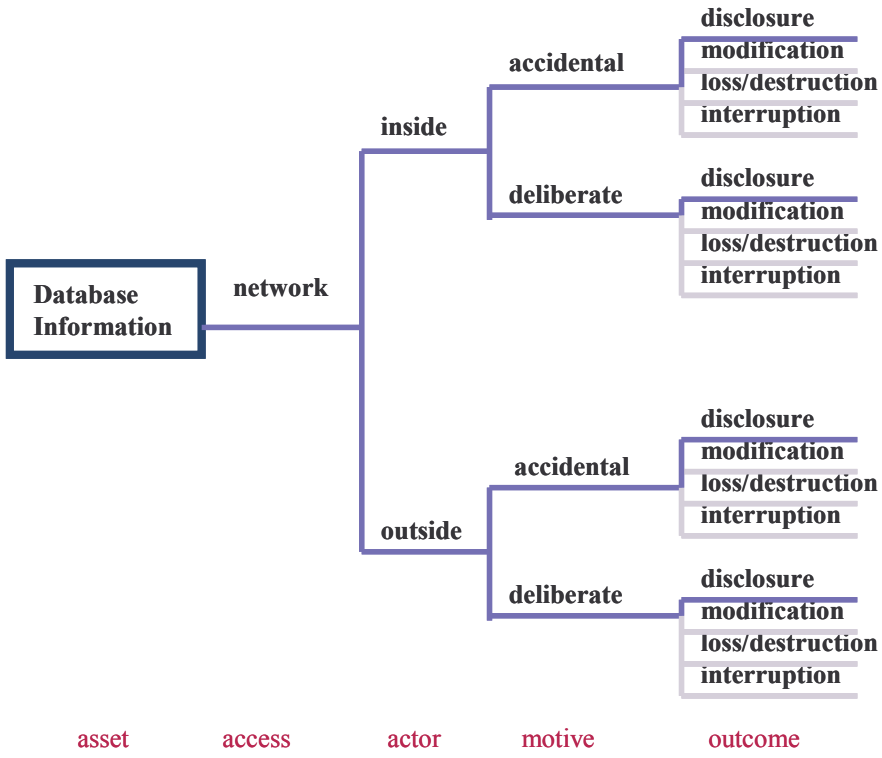
With any system it is important to understand where the risks are and where the system is most vulnerable. By now the initial workshops or questionnaires are completed and the information begins to be assimilated into a "fabric" of components that can actually relate to each other and determine what, if any, discrepancies exist.

[5] This is based on OCTAVE-S. The optional probability step is removed for the sake of simplicity.

Threat trees are used to map mission critical assets to possible threats and vulnerabilities. This moves the value far beyond the vulnerability assessment found in IT centric risk methodologies. These threat trees are based on Scenario Planning, the discipline of attempting to protect against the truly unknown. There is not enough information to reliably use historical data and therefore, probabilities. Any historical data available is input in a later process.

There are four threat trees created for each critical asset – Human Actors Using Physical Access, Human Actors Using Network Access, System Problems, and Other Problems. Other Problems describe events with the infrastructure outside of the organizations control; power, telecommunications, natural disasters, and third-party problems. System Problems detail software defects, system crashes, hardware defects and malicious code. This comprehensive approach often uncovers exposures other risk assessment methodologies miss.

Human Actors Using Network Access



OCTAVE Process 3 Identify Key Components

Process 3 introduces the technical vulnerability assessment and identifies those parts of the information system that impact the assets identified through the previous steps. Instead of simply evaluating the network from "inside the firewall" and "outside the firewall", a focus is given to the information systems which the critical business processes rely upon. This further aids in prioritization if a comprehensive scan reveals an overabundance of vulnerabilities.

OCTAVE Process 4 Evaluate Selected Components

This process involves determining what technical tools will be used to execute the vulnerability assessment. A survey is quickly conducted to determine if these tools are present within the organization, external to the organization, or some combination. This involves host intrusion detection tools, network intrusion detection tools, and catalogs of vulnerabilities. This is what most people think of when they think about an information security risk assessment but is incorporated into the organizational context via OCTAVE.

The best known catalogs of vulnerabilities are the CERT Knowledge Base and the Common Vulnerability Evaluation (CVE) managed by Mitre Corporation. Impruve's OCTAVE assessment incorporates both catalogs as well as information from IT vendors to provide a complete analysis.

OCTAVE Process 5 Conduct the Risk Analysis

This involves tying together the information gathered so far in the process- the threats, assets and vulnerabilities uncovered in the previous 6 processes and putting them into an organizational context. We take the information gathered and the threat trees created during processes 1-2 and the technical information gathered in processes 3-4 to define risk scenarios and risk analysis.

Process 5 provides narrative impact descriptions of the various risks to the critical assets identified. Evaluation criteria are also studied to determine what qualifies as a high, middle, or low impact on the organization to prioritize mitigation strategies.

OCTAVE Process 6 Develop a Protection Strategy

OCTAVE is completed in process 6, where the outputs from Process 5 are coalesced with industry guidelines to address best practice and regulatory compliance issues. The outputs from the OCTAVE are:

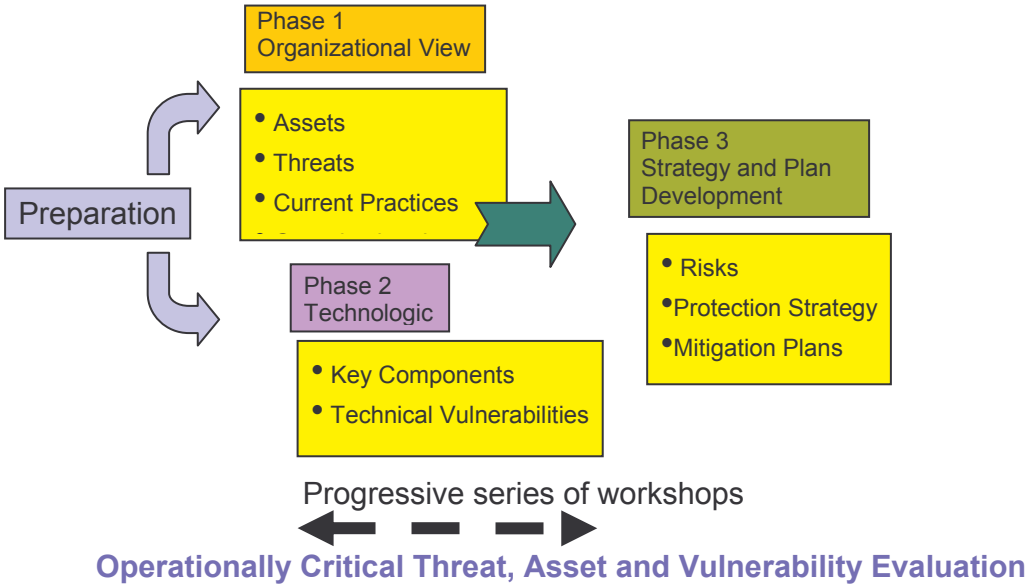
1. Protection Strategy – defines the strategic direction the organization is taking to address any gaps between existing practices and compliance. Specifically this will directly indicate the gaps between the clients existing information security framework and ISO 17799.

2. Risk Mitigation Plan – to address the vulnerabilities uncovered through the OCTAVE process. This and the following document are fed into the recommendations section of the deliverables.

3. Task List – to rapidly assign responsibility and timelines to ensure the process has relevance with respect to actually securing information assets. This also serves as remedial actions that can be implemented immediately or in the short term. As mentioned above, this also feeds into the recommendations section.

Impruve OCTAVE 17799 is designed for use by a company's own information security team or through consultants and systems integrators. Impruve gives each of the client's access to the knowledge and experience gained by Impruve Professional Services over years of implementing

large and small-scale security solutions. By separating the project into manageable phases, implementers can ensure that the risk assessment methodology meets business objectives.



Recommendations

The mitigation of identified risks is evaluated by the analysis team and presented to management as a milestone. Management reviews the analysis team's assumptions and agrees or disagrees to the prioritization scheme recommended. The metric is based on identified business impacts.

These recommendations also take into account the required resources necessary to implement. Impruve would like to suggest clients consider risk *acceptance* as a viable strategy. Low impact risks may not require action. Cost ineffective strategies are noted but discounted for pragmatic reasons. Previous sentences notwithstanding, the delivery is a complete and comprehensive list of risks and recommendations.

The organization of identified risks takes two main forms – risks identified as part of the overall Risk Assessment and risks uncovered as part of the Vulnerability Assessment. The technical vulnerabilities are detailed in an addendum to the Recommendations report. The risks will also be organized according to short term, medium term and long term mitigations. This follows the Task List, Mitigation Plan, and Protection Strategy outputs from the risk assessment.

The assessment rates the risks at high, medium, and low levels. Numeric values and probabilities can be assigned but this tends to "wash out" any outliers:

Impact	Probability		Risk
H	L	→	M
M	M	→	M
L	H	→	M

This may or may not be the approach a particular client desires. These issues should be reviewed and understood prior to working through risk assignments.

Generally speaking, the recommendation is to tackle no more than three "strategic" areas (17799 sections) during any given assessment. This is simply to make the job more manageable. It is completely up to the client but discussed here to recognize the fact that although information security is important, it is not the organization's primary mission.

Accreditation to Information Security Management Standard

It is our recommendation that ISO 17799 be considered, as it is the global standard for an Information Security Management System (ISMS). Based on the time frame and other motivations (desire to procure cyber insurance, work with other organizations), the 17799 roadmap can take two approaches:

1. Pursue a "gap analysis" strategy to ameliorate discrepancies between the present system and the standard. This has the benefit of the most expeditious path towards 17799 compliance. Prioritization is based on business impacts as determined by the analysis team and reviewed by management. ISO 17799 provides suggestions in the event prioritization proves difficult[6].

2. A second approach is to perform a follow-on risk assessment. This could be scheduled based on a time interval or a significant change to the environment (adopting new technologies that impact the organization). The advantage with this approach is that it breaks down the compliance issue into more manageable chunks. Another advantage is the risk assessment can evaluate other areas of the clients business, which, because of time constraints, could not be reviewed in the initial assessment.

Artifacts from the risk assessment aid in assessing the situation and strategizing on the best path forward.

Impruve: Experience, Expertise, Cost-Effective

In general, our experiences drive us to focus on the valuable information within an enterprise. A study of information flow allows analysis unique from a simple "inside the firewall, outside the firewall" review from some less experienced security consultants. Modern information systems

[6] The ISO 17799 Introduction section has a subsection, Information Security Starting Point, page x. This details the Standard's recommended prioritization scheme.

are more analogous to museums than medieval castles, with the recognition that the valuable artifacts require a focused protection strategy — as does the perimeter.

Impruve was one of the first licensed transition partners for Carnegie Mellon University / Software Engineering Institute's OCTAVE methodology, a practical guide to assist organization's designing and implementing an enterprise security system.

With decades of practical experience implementing information security solutions, Impruve's staff of information security professionals has developed a streamlined and customizable OCTAVE that incorporates the ISO 17799 framework and is adaptable for virtually any size organization.

Impruve has combined its extensive experience and expertise working with both global organizations and regional institutions to develop the OCTAVE 17799 methodology. The Impruve OCTAVE 17799 is a proven implementation methodology that synthesizes the knowledge of Impruve's professional services staff into a detailed step-by-step plan that will dramatically accelerate 17799 deployments and provide guidance on the management of the system.

Organizations receive the benefit of thousands of hours of effort rolled into this easy-to-use system. Using a set of customized templates, the system helps to implement and document these processes, thus addressing ISO 17799 requirements in a very efficient and cost-effective manner. This saves organizations time and significantly reduces the complexity and risk in deploying an information security management system.

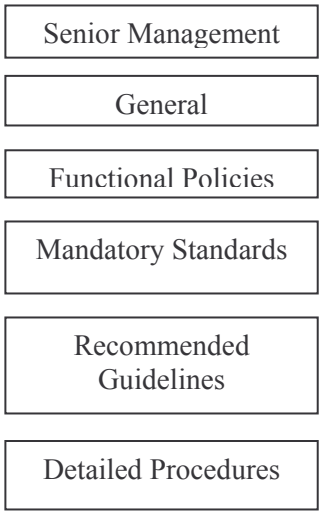
Appendix A Policy Guidelines

Policy solves at least three functions for an information security program:

- Provides a guide for users within an organization on what is and is not permissible;
- Supports actions that are desired by management but outside the scope of the technology;
- Creates a position for addressing regulatory requirements.

Policies should follow some order in terms of hierarchy as well as audience to provide organization and ensure the intended recipients have read and abide by the policies. The format we present here is based on a policy hierarchy outlined in *Mastering to Ten Domains of Computer Security*, Ronald Krutz and Russell Visor, The CISSP Prep Guide, 2001.

Policy



The hierarchy has at the highest level a *Senior Management Statement* which should serve to:

- Acknowledge importance of security and policies;
- Indicate support for information security throughout the enterprise;
- Commit to developing, implementing and managing standards, procedures and guidelines.

The *General Organizational Policies* is intended to set the overall scope and vision of the organization's security program. *Functional Policies* are intended to address specific topics. *Standards* are considered compulsory and must be uniformly implemented throughout the organization. *Guidelines* can indicate best practices on specific objectives. *Procedures* specify the steps required for specific situations.

The reason for this level of complexity in a policy program is to allow changes in technologies or processes to function independently of the policies. The overarching policy may stay the same but the procedures may be revised to satisfy environmental changes.

Mapping this format to 17799, we equate the *Senior Management Statement* with the Information Security Policy document (17799 Clause 3.1.1). Impruve labels the *General Organization Policies* Security Plans to reduce confusion between terminologies. The following are primary policies detailed in ISO 17799:

Information Security Policy
Incident Management Plan
Operating Procedure Plan
Access Control Policy
Registration Policy
Network Policy
Information Backup
Record Retention Policy
Change Management Policy
Acceptance criteria
Policy regarding compliance with software licenses
Business Continuity Plan
Confidentiality, non-disclosure agreements, service level agreements
Acceptable Use Plan (Policy)
Email Policy
Policy for voice, fax and video communication
Password Policy
Information Classification Policy
Storage and Handling of Information Assets
Cryptographic Policy
Mobile Computing Policy
Teleworking Policy

This is not exhaustive, but is used for the example. These can be mapped and charted according to the organization outlined above; the following chart shows one such mapping:

Overall Policy	Plans	Policies	Guidelines	Procedures
Information Security Policy				
	Operating Procedure			
		Access Control		
			Registration	
			Network	
				Information Backup
			Record Retention	
		Change Management		
			Acceptance criteria	
			Compliance with software licenses	
	Incident Management			
	Business Continuity			
	Acceptable Use			
		Email		
		Password		
		Voice, fax and video communication		
		Information classification		
			Storage and handling of information assets	
			Cryptographic	
		Mobile computing		
			Teleworking	

Confidentiality, non-disclosure agreements and service level agreements also need to be defined and mapped. Some policies will fit in several categories. The Acceptable Use Plan (or Policy) would be distributed to the entire community, whereas the Operating Procedure Plan may be limited to the Information Systems Department.

The point is to recognize that all users must participate in information security while striving to continually reduce the burden of the user's responsibilities.