ISO17799 Policy Gap Analysis

Prepared for

John Smith

Big Company Inc.

by

Fred Cohen & Associates

in partial fulfillment of Purchase Order DH203022

Executive Summary

In November of 2004, John Smith of Big Company (CLIENT) asked Fred Cohen & Associates (FCA) to perform a policy gap analysis comparing existing and internally published policies with the ISO17799 standard. The results of this analysis were then compared to the results from the recent protection posture assessment to understand how effective those policy elements were at meeting CLIENT's needs.

Over the period of effort, CLIENT provided FCA with copies of all security-related policies then available and FCA produced the gap analysis contained herein. From this analysis, it appears that CLIENT has a large number of policies that, in fragmented parts, substantially cover 73 of the 128 elements of the ISO17799 standard, poorly cover another 30 elements of the standard, and provide no coverage of the remaining 25 elements of the standard.

Despite the substantial coverage of 73 policy elements, the presence of these policies are not reflected in internal compliance or understandings demonstrated by employees. In addition, the overall condition of those policy elements are not at proper assurance levels for the needs of CLIENT. As a result, there are significant gaps between the needs and the policies and between the policies and the desired standards.

FCA recommends a policy reconciliation and rewrite. This involves writing a comprehensive security policy that follows the ISO17799 structure while incorporating existing policy elements for backward compatibility and internal consistency. The resulting policy will then update and replace the larger number of more fragmented policy elements that have evolved over many years with a new policy that covers the issues more comprehensively, is properly adapted to CLIENT's current needs, and can be read and understood in a few hours. This policy should also meet all policy-level compliance requirements and be suitable to pass relevant audits.

This policy rewrite would be best if completed prior to any upcoming audits that might be positively affected by the effort.

Table of Contents

Background, Scope, and Overview

Background

In September of 2004, John Smith of Big Company (CLIENT) asked FCA to perform a gap analysis assessing the current security-related policies of CLIENT relative to the ISO17799 standard in order to understand the policy needs at CLIENT in more detail. During the month of September, a policy analysis team took material provided by CLIENT and reviewed all provided policies relative to the ISO17799 standard to understand these issues. These efforts included but were not limited to:

- Review all currently available CLIENT security policies.
- Perform line-at-a-time comparison of policy elements to ISO17799 standards and map the policy elements into the ISO17799 sections.
- Produce a gap analysis.
- Compare these results to the protection posture assessment results and reconcile differences.
- Provide analysis of results.
- Write and deliver this report.

Scope

The scope of this effort was limited to security-related policies that had, at the time of the start of the effort been published as official policies on the internal CLIENT Web site and made available for employee use. Additional policies exist and have been approved, but were not available for employees or FCA at the time of the start of this effort.

The Study and Results

The approach taken by this effort involved detailed review of the documents shown in Table 1 on a line-by-line basis. Each document was give a two-letter abbreviation for ease of reference.

Document name	*Abbreviation*
AcceptableUseTechnology	AU
Authentication---Access-Control-Policy	AA
Business-Systems-Quarterly-Audit-Procedure	BS
C-TPAT Policy - 04-27-04 09002	CP
Data-Encryption-Policy—Rev-A	DE
eDirectory-Associated-Applications-Policy	DA
Electronic-Messaging-Attachment-Blocks	EM
Enterprise-Electronic-Messaging-Policy	EE
Email-Acceptable-Use-Policy—Rev-A	EA
Firewall-Change-Procedure—Rev.-A	FC
Firewall-Configuration---Maintenance	FM
Information misuse	IN
Information-Security-Compliance-Policy	IC
Information-Security-Management-Poli	IM
Information-Security-Policy	IS
Internet-Acceptable-Use-Policy—Rev-G	IA
IS Policy overview	IO
IT-Facilities-Physical-Access-Policy	IF
IT-Security-Incident-Response-Procedures	IR
Laptop-Computer-Security-Policy—Rev-C	LC
Mainframe-Systems-User-Account-Management	MS
Network-Equipment-Archiving-Procedures	NE
Partners--Vendors---Customers-Access	PV
Personnel-Security-Policy--Rev-A	PS
Privacy-Policy--Rev-A	PP
Data-Center-Phones	SJ
Software-Policy--Rev-A	SP
Special-Access-Policy--Rev-A	SA

Document name	*Abbreviation*
Symantec-Alert-Response-Procedure--R	SR
System--Development-and-Maintenance	SD
System-Monitoring-Procedure--Rev-A	SM
System-Security-Certification-Procedure	SS
User-Account-Termination-Procedure-	UA
User-Self-Service-Password-Portal-Procedure	US
VIRUS_incident_v4execs	VI
Wireless-Acceptable-Use-Policy--Rev-G	WA

Table 1 – The 35 policies reviewed

The mapping is represented in table form with rows representing each ISO17799 element and columns representing each policy reviewed. Entries in each table element representing 'e' for an enterprise-wide policy element, 'p' followed by a section number for partial coverage of this ISO17799 element by the identified section of the policy, 'r' for a by-reference policy element where the policy references some other policy element that is supposed to cover the ISO17799 element, 'b' followed by a number to identify a particular bulleted item that is covered, and the number '1' to indicate that no coverage is provided. The full table is provided under separate cover as a spreadsheet.

Policy errors can be found by cases where referenced sections are not identified as having either partial or enterprise-wide policies. These typically happen when a policy is changed and the other policies that reference it are not changed to reflect this. Table 2 shows areas of ISO17799 that have no coverage at all under the current policies. This includes 25 policy areas, a substantial portion of the ISO standard, and enough lack of coverage that a detailed audit would likely indicate inadequacy in these areas.

Area in ISO17799	Coverage
4.1.4 Authorization process for information processing facilities	Not covered
7.2.2 Power supplies	Not covered
7.2.3 Cabling security	Not covered
7.2.6 Secure disposal or re-use of equipment	Not covered
8.2.1 Capacity	Not covered
8.6.2 Disposal of media	Not covered
9.4.5 Remote diagnostic port protection	Not covered
9.5.1 Automatic terminal identification	Not covered

Area in ISO17799	Coverage
9.5.2 Terminal log-on procedures	Not covered
9.5.6 Duress alarm to safeguard users	Not covered
9.5.8 Limitation of connection time	Not covered
9.7.3 Clock	Not covered
10.2.1 Input data validation	Not covered
10.2.2 Control of internal processing	Not covered
10.2.4 Output data validation	Not covered
10.3.3 Digital signatures	Not covered
10.3.4 Non-repudiation services	Not covered
10.5.2 Technical review of operating system changes	Not covered
10.5.4 Covert channels and Trojan code	Not covered
11.1.1 Business continuity management process	Not covered
11.1.2 Business continuity and impact analysis	Not covered
11.1.3 Writing and implementing continuity plans	Not covered
11.1.4 Business continuity planning framework	Not covered
11.1.5 Testing, maintaining and re-assessing business continuity plans	Not covered
12.1.7 Collection of evidence	Not covered

Table 2 – Areas not covered by current policies

Table 3 is a roll-up of policy areas with only limited partial coverage. These are areas in which policy exists but is inadequate to address the requirements of the standard or the CLIENT's needs. In this table 'P' stands for partial coverage, 'R' is for by-reference coverage, and the document identification and section numbers are used to identify specifics. For example, section 4.1.1 of the ISO17799 standard is only partially covered by a reference in section 5.0 of the Internet Acceptable use policy (IA), which means that it is in fact not covered meaningfully at all.

Area	Coverage
4.1.1 Management information security forum	PR IA-5.0
4.1.5 Specialist information security advice	PR IA-5.0
4.1.7 Independent review of information security	P EM-5.2, EA-5.1
4.3.1 Security requirements in outsourcing contracts	P PV-6-9

Area	Coverage
5.2.1 Classification guidelines	R IS-7
5.2.2 Information labeling and handling	R IA-3.1, P IO
7.1.5 Isolated delivery and loading areas	P CP-28
7.2.1 Equipment siting and protection	P LC-7
7.2.4 Equipment maintenance	P AU-b3 NE-3.1
7.2.5 Security of equipment off-premises	P PV-8.0,9.1 LC-7.0, IS-3,3.0
7.3.1 Clear desk and clear screen policy	P LC-7.0
8.1.5 Separation of development & operational facilities	R IS-2,5.0
8.4.1 Information back-up	P EE-6.1.3.1.1.1, 6.14-. 1.4.1.3.2
8.6.1 Management of removable computer media	P DE-7.1
8.6.4 Security of system documentation	P DE-12.0 IO-?
8.7.1 Information and software exchange agreements	P IO-?
8.7.5 Security of electronic office systems	PR CP-Physical, IA-8.0, 9.0
9.4.3 User authentication for external connections	PR IO-10.0, 6.2.1
9.4.4 Node authentication	P EA-6.10.1, PV-8.1
9.4.6 Segregation in network	P NE-3.2.1, IS-14.0
9.4.8 Network routing control	P NE-3.2.1
9.4.9 Security of network services	P NE-3.2
9.5.5 Use of system utilities	PR IF-6.0
9.5.7 Terminal time-out	R IS-12.2
9.6.2 Sensitive system isolation	PR IF-6.0
9.8.2 Teleworking	P IS-15-18
10.3.5 Key management	P IS-27.6-7, R PP-7.3
10.4.2 Protection of system test data	P SD-12.0
12.1.3 Safeguarding of organizational records	P DA-3.1, EE-6.1.3.1
12.2.2 Technical compliance checking	P NE-4.4
12.3.2 Protection of system audit tools	P SD-12.0

Table 3 – Areas with limited or only by-reference coverage

Table 3 references only areas in which a relatively small number of documents provided partial or referential coverage. There are 30 policy areas that are clearly not adequately covered by the policies analyzed. In many cases the partial coverage provided applies only to a small subset of all computers. For example, policy are 7.2.1 having to do with equipment siting and protection is only touched on at all by the policy on laptop computers and this clearly doesn't cover all of the related issues addressed by ISO17799. More complex areas may have 8 or more policy elements with partial coverage from many policy documents. This makes these sets of partially overlapping policies very confusing to analyze and to use. They were not fully analyzed in this effort because such analysis would not be particularly helpful in addressing the issues at hand.

Comparison to the Information Protection Posture Assessment (IPPA) findings

The recent information protection posture assessment produced results indicative of inadequate policy coverage relative to ISO17799 and this more in-depth analysis bore this out in greater detail. The review provided in Table 4 shows both the current gap analysis (Gap) and the previous protection posture assessment results with IPPA ratings given as “Poor”, “Fair”, or “Good” indicative of observed behaviors and Gap ratings of “N/A” for roll-up areas, “POOR” for areas with inadequate coverage, “NONE” for areas with no coverage, and no entry for areas where there were enough policy elements to make coverage substantial.

Area	Gap	IPPA
3 SECURITY POLICY	N/A	Fair
3.1 INFORMATION SECURITY POLICY	N/A	Fair
3.1.1 Information security policy document		Fair
3.1.2 Review and evaluation		Poor
4 ORGANIZATIONAL SECURITY	N/A	Poor
4.1 INFORMATION SECURITY INFRASTRUCTURE	N/A	Poor
4.1.1 Management information security forum	POOR	Poor
4.1.2 Information security co-ordination		Poor
4.1.3 Allocation of information security responsibilities.		Poor
4.1.4 Authorization process for information processing facilities	NONE	Fair
4.1.5 Specialist information security advice	POOR	Poor
4.1.6 Co-operation between organizations		Poor
4.1.7 Independent review of information security	POOR	Poor
4.2 SECURITY OF THIRD PARTY ACCESS		Poor

Area	Gap	IPPA
4.2.1 Identification of risks from third party access		Poor
4.2.2 Security requirements in third party contracts		Poor
4.3 OUTSOURCING	N/A	Fair
4.3.1 Security requirements in outsourcing contracts	POOR	Poor
5 ASSET CLASSIFICATION AND CONTROL	N/A	Poor
5.1 ACCOUNTABILITY FOR ASSETS	N/A	Poor
5.1.1 Inventory of Assets		Poor
5.2 INFORMATION CLASSIFICATION	N/A	Poor
5.2.1 Classification guidelines	POOR	Poor
5.2.2 Information labeling and handling	POOR	Poor
6 PERSONNEL SECURITY	N/A	Poor
6.1 SECURITY IN JOB DEFINITION AND RESOURCING	N/A	Fair
6.1.1 Including security in job responsibilities		Poor
6.1.2 Personnel screening and policy		Fair
6.1.3 Confidentiality agreements		Fair
6.1.4 Terms and conditions of employment		Fair
6.2 USER TRAINING	N/A	Poor
6.2.1 Information security education and training		Poor
6.3 RESPONDING TO SECURITY INCIDENTS AND MALFUNCTIONS	N/A	Poor
6.3.1 Reporting security incidents		Poor
6.3.2 Reporting security weaknesses		Poor
6.3.3 Reporting software malfunctions		Poor
6.3.4 Learning from incidents		Poor
6.3.5 Disciplinary process		Fair
7 PHYSICAL AND ENVIRONMENTAL SECURITY	N/A	Poor
7.1 SECURE AREAS	N/A	Poor
7.1.1 Physical security perimeter		Poor
7.1.2 Physical entry controls		Poor
7.1.3 Securing offices, rooms and facilities		Poor
7.1.4 Working in secure areas		Poor
7.1.5 Isolated delivery and loading areas	POOR	Poor
7.2 EQUIPMENT SECURITY	N/A	Poor

Area	Gap	IPPA
7.2.1 Equipment siting and protection	POOR	Poor
7.2.2 Power supplies	NONE	Poor
7.2.3 Cabling security	NONE	Fair
7.2.4 Equipment maintenance	POOR	Poor
7.2.5 Security of equipment off-premises	POOR	Poor
7.2.6 Secure disposal or re-use of equipment	NONE	Poor
7.3 GENERAL CONTROLS	N/A	Poor
7.3.1 Clear desk and clear screen policy	POOR	Poor
7.3.2 Removal of property		Poor
8 COMMUNICATIONS AND OPERATIONS MANAGEMENT	N/A	Poor
8.1 OPERATIONAL PROCEDURES AND RESPONSIBILITIES	N/A	Poor
8.1.1 Documented operating procedures		Poor
8.1.2 Operational change control		Poor
8.1.3 Incident management procedures		Poor
8.1.4 Segregation of duties		Poor
8.1.5 Separation of development and operational facilities	POOR	Poor
8.1.6 External facilities management		Poor
8.2 SYSTEM PLANNING AND ACCEPTANCE	N/A	Poor
8.2.1 Capacity	NONE	Poor
8.2.2 System access		Poor
8.3 PROTECTION AGAINST MALICIOUS SOFTWARE	N/A	Poor
8.3.1 Controls against malicious software		Poor
8.4 HOUSEKEEPING	N/A	Poor
8.4.1 Information back-up	POOR	Fair
8.4.2 Operator logs		Poor
8.4.3 Fault logging		Poor
8.5 NETWORK MANAGEMENT	N/A	Poor
8.5.1 Network controls		Poor
8.6 MEDIA HANDLING AND SECURITY	N/A	Poor
8.6.1 Management of removable computer media	POOR	Poor
8.6.2 Disposal of media	NONE	Poor
8.6.3 Information handling procedures		Poor
8.6.4 Security of system documentation	POOR	Poor

Area	Gap	IPPA
8.7 EXCHANGES OF INFORMATION AND SOFTWARE	N/A	Poor
8.7.1 Information and software exchange agreements	POOR	Poor
8.7.2 Security of media in transit		Poor
8.7.3 Electronic commerce security		Poor
8.7.4 Security of electronic mail		Poor
8.7.5 Security of electronic office systems	POOR	Poor
8.7.6 Publicly available systems		Fair
8.7.7 Other forms of information exchange		Poor
9 ACCESS CONTROL	N/A	Poor
9.1 BUSINESS REQUIREMENT FOR ACCESS CONTROL	N/A	Poor
9.1.1 Access control policy		Fair
9.2 USER ACCESS MANAGEMENT	N/A	Poor
9.2.1 User registration		Poor
9.2.2 Privilege management		Poor
9.2.3 User password management		Poor
9.2.4 Review of user access rights		Poor
9.3 USER RESPONSIBILITY	N/A	Poor
9.3.1 Password use		Poor
9.3.2 Unattended user equipment		Poor
9.4 NETWORK ACCESS CONTROL	N/A	Poor
9.4.1 Policy on use of network services		Fair
9.4.2 Enforced path		Poor
9.4.3 User authentication for external connections	POOR	Fair
9.4.4 Node authentication	POOR	Poor
9.4.5 Remote diagnostic port protection	NONE	Poor
9.4.6 Segregation in network	POOR	Poor
9.4.7 Network connection control		Poor
9.4.8 Network routing control	POOR	Fair
9.4.9 Security of network services	POOR	Poor
9.5 OPERATING SYSTEM ACCESS CONTROL	N/A	Poor
9.5.1 Automatic terminal identification	NONE	Poor
9.5.2 Terminal log-on procedures	NONE	Poor
9.5.3 User identification and authentication		Poor

Area	Gap	IPPA
9.5.4 Password management system		Poor
9.5.5 Use of system utilities	POOR	Poor
9.5.6 Duress alarm to safeguard users	NONE	Poor
9.5.7 Terminal time-out	POOR	Poor
9.5.8 Limitation of connection time		Poor
9.6 APPLICATION ACCESS CONTROL	N/A	Poor
9.6.1 Information access restriction		Fair
9.6.2 Sensitive system isolation	POOR	Poor
9.7 MONITORING SYSTEM ACCESS AND USE	N/A	Poor
9.7.1 Event logging		Fair
9.7.2 Monitoring system use		Poor
9.7.3 Clock	NONE	Fair
9.8 MOBILE COMPUTING AND TELEWORKING	N/A	Poor
9.8.1 Mobile computing		Poor
9.8.2 Teleworking	POOR	Poor
10 SYSTEMS DEVELOPMENT AND MAINTENANCE	N/A	Poor
10.1 SECURITY REQUIREMENTS OF SYSTEMS	N/A	Poor
10.1.1 Security requirements analysis and specification		Poor
10.2 SECURITY IN APPLICATION SYSTEMS	N/A	Poor
10.2.1 Input data validation	NONE	Poor
10.2.2 Control of internal processing	NONE	Fair
10.2.3 Message authentication		Poor
10.2.4 Output data validation	NONE	Poor
10.3 CRYPTOGRAPHIC CONTROLS	N/A	Poor
10.3.1 Policy on the use of cryptographic controls		Poor
10.3.2 Encryption		Poor
10.3.3 Digital signatures	NONE	Poor
10.3.4 Non-repudiation services	NONE	Poor
10.3.5 Key management	POOR	Poor
10.4 SECURITY OF SYSTEM FILES	N/A	Poor
10.4.1 Control of operational software		Poor
10.4.2 Protection of system test data	POOR	Poor
10.4.3 Access control to program source library		Poor

Area	Gap	IPPA
10.5 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES	N/A	Poor
10.5.1 Change control procedures		Poor
10.5.2 Technical review of operating system changes	NONE	Poor
10.5.3 Restrictions on changes to software packages		Poor
10.5.4 Covert channels and Trojan code	NONE	Poor
10.5.5 Outsourced software development		Fair
11 BUSINESS CONTINUITY MANAGEMENT	N/A	Poor
11.1 ASPECTS OF BUSINESS CONTINUITY MANAGEMENT	N/A	Poor
11.1.1 Business continuity management process	NONE	Poor
11.1.2 Business continuity and impact analysis	NONE	Poor
11.1.3 Writing and implementing continuity plans	NONE	Fair
11.1.4 Business continuity planning framework	NONE	Fair
11.1.5 Testing, maintaining and re-assessing business continuity plans	NONE	Fair
12 COMPLIANCE	N/A	Fair
12.1 COMPLIANCE WITH LEGAL REQUIREMENTS	N/A	Fair
12.1.1 Identification of applicable legislation		Fair
12.1.2 Intellectual property rights (IPR)		Poor
12.1.3 Safeguarding of organizational records	POOR	Poor
12.1.4 Data protection and privacy of personal information		Poor
12.1.5 Prevention of misuse of information processing facilities		Poor
12.1.6 Regulation of cryptographic controls		Poor
12.1.7 Collection of evidence	NONE	Poor
12.2 REVIEWS OF SECURITY POLICY AND TECHNICAL COMPLIANCE	N/A	Poor
12.2.1 Compliance with security policy		Poor
12.2.2 Technical compliance checking	POOR	Poor
12.3 SYSTEM AUDIT CONSIDERATIONS	N/A	Poor
12.3.1 System audit controls		Poor
12.3.2 Protection of system audit tools	POOR	Poor

Table 4 – Section-by-section roll-up with IPPA results

All told, this analysis shows that in 73 areas policies appear to provide substantial coverage, while in 30 areas, policy coverage is poor, and in another 25 areas there is no policy coverage whatsoever. While detailed analysis of the

specifics of coverage provided for the 73 areas with substantial coverage was not undertaken beyond the policy mapping effort, this analysis shows that a substantial amount of effort is required in order to bring policies into compliance with ISO17799.

This analysis also indicates that the situation in terms of actual behaviors varies from the policy situation. For example, there are areas in which no policy is in place but observations during the IPPA indicate that protection measures are in place. This means that employees are doing the right thing in these cases even though policy does not provide explicit guidance. On the other hand, there are far more areas in which the IPPA rating indicates Poor performance and yet policies exist with substantial coverage. This indicates that the existing policy is not being effectively promulgated to the employees in these areas.

Comparison to information security framework

CLIENT uses a policy, standards, and procedures scorecard to measure its information security policy framework, and this is internally referred to as the "ISPF", reflecting its appearance in the internal power point slide format used to describe it. The cake consists of 10 "framework" policies that are supposed to conform with ISO17799 control standards, 18 "issue-specific" policies, 12 "procedures", and a set of "technology standards". The elements of the ISPF are included in this analysis with the top-level framework policies consisting of the documents identified herein as IM, IC, IS, IP, SD, IC, IF, PS, IO, and SA.

[DIAGRAM NOT INCLUDED IN THIS SAMPLE]

While the ISPF diagram indicates the 10 areas of ISO17799 that should be covered by these documents, the policies provided for this analysis have very limited coverage. Taking only the policy components identified here, coverage indicated in green by the ISPF diagram is not complete according to the detailed analysis. Thus the roll-up data appears based on this analysis to be in error.

Findings and Recommendations

Despite the presence of 35 policy documents reviewed in this gap analysis, the 9 areas of policy associated with the ISO17799 standard are only about 65% covered by those policy documents. This indicates a situation in which there are too many and too diverse a set of policies for proper coverage and proper understanding by employees. The analysis shows that coverage varies greatly in terms of depth of coverage across the areas of the standard, but this difference in depth does not appear to reflect any risk management activity. This is indicative of a historical development of policies without periodic reconciliation, consolidation, or a standards-based structure. The presence of the ISPF diagram is intended to provide clarity to management, but it appears that the mappings between the ISPF diagram and the actual policies is faulty and thus the ISPF diagram is misleading as currently presented.

The existing policies should be reconciled to form a smaller set of more well integrated and properly designed policy elements that provide better and more even coverage, are more consistent, and are at the same time of a size that allows them to be read and understood by the employees tasked with implementing them.

This process normally starts with new policy generation consisting of:

- The identification of a standard (ISO17799 in this case)
- The creation of a by-reference policy in which policy elements from existing policies are consolidated by reference into the new standards-based policy.
- The rewriting of policy elements to retain the existing policies and to augment it with policy elements from the gap analysis that were missing or inadequate to properly cover the standard.

This then produces a completed new policy that includes all of the elements of the old policy and all of the elements required for comprehensive coverage, organized per the standard and easily reconcilable to existing policies. This set of policies are reviewed by management for approval. The new set of policies is typically designed so that changes will be relatively rare and can be kept within the existing structure so that new policies do not have to be developed and changes can be understood easily by employees without increasing complexity over time.

Part of the policy simplification process involves the separation of policy from organizational implementation of those policies. In order to compensate for the removal of implementation specifics, a second tier of material is developed, typically called organizational control standards. These control standards are

more detailed specifications of operational aspects of policy implementation. For example, a policy might indicate that password length and composition requirements are specified by a control standard and that control standard might identify different password lengths and compositions for different sorts of systems. The control standards may then reference even more specific sets of procedures that walk through step-by-step processes required to set, modify, determine, and evaluate password length and makeup on a system-by-system basis.

The resulting policy, control standards, and procedures are then tracked over time to adapt to changes in regulatory and other conditions and to reflect changing times and technologies as well as to meet updates to the standard.

The overall effort starting from the current situation, assuming that only existing control standards and procedures are to be codified in the new policy structure, typically takes from three to six months to complete with activities and level of effort as shown in Table 5:

Activity	Effort (days)
By-reference policy creation	20-40
Policy completion	20-40
Control standards	20-40
Procedures	20-40
Total	**120**

Table 5 – Recommended further policy activities

Summary and Conclusions

CLIENT policies are substantially out of touch with CLIENT needs and with the ISO17799 standard. This comes from a combination of:

- too many policies at too broadly differing levels of depth,
- inadequate coordination or standardization of policy elements that has lead to inadequate coverage and unnecessarily high complexity,
- a lack of a clarity in policy deployment and dissemination that makes policy operationally ineffective, and
- inaccurate mapping of actual policies into management's ISPF diagram that cause a false sense of the actual situation.

The solution identified here is the development of a new set of policies written to be compatible with existing policies while improving coverage of standards and reducing complexity for the reader. These policies can then be used to replace existing policies while reducing employee complexity, retaining consistency, improving compliance, and reducing policy maintenance costs. The ISPF diagram should either be abandoned because of the inability to keep it accurately up to date, or updated to reflect the real situation. A more in-depth spreadsheet, such as the one used in the gap analysis, should be instituted during the period of policy transition to assure that accurate conditions are available. After policies are updated and consolidated, the spreadsheet should be retained in order to allow its use in updating policies to reflect changes in standards and to continue to provide detailed mapping of specific issues into policy elements.