

# Appendix H

## Protection Needs Elicitation

---

### Table of Contents

List of Figures .....	iii
List of Tables.....	iii
H.1 INTRODUCTION .....	H-1
H.1.1 Purpose.....	H-1
H.1.2 PNE and the INFOSEC Business .....	H-4
H.1.3 PNE, ISSE, and SE Process .....	H-5
H.1.4 PNE and Common Criteria.....	H-6
H.1.5 PNE and DITSCAP .....	H-7
H.1.6 PNE and Risk Management.....	H-8
H.2 OVERVIEW.....	H-9
H.2.1 PNE Practitioner Characteristics .....	H-9
H.2.2 Acronyms.....	H-10
H.2.3 PNE/ISSE Documents .....	H-10
H.2.4 Seven Procedures.....	H-11
H.2.5 Approaching the Customer .....	H-11
H.2.6 Acquiring the IMM.....	H-11
H.2.7 The Least-Privilege IMM .....	H-11
H.2.8 Threat Analysis .....	H-11
H.2.9 Customer Priorities .....	H-12
H.2.10 Preparing the IPP .....	H-12
H.2.11 Customer Buy-In.....	H-12
H.3 APPROACHING THE CUSTOMER.....	H-12
H.3.1 Making Initial Contacts .....	H-13
H.3.2 Learning the Business and Mission .....	H-14
H.3.3 Developing Contacts.....	H-14
H.3.4 Selling the Value of PNE.....	H-15
H.3.5 PNE Project Planning .....	H-16
H.3.6 Setting Project Roles and Responsibilities .....	H-17
H.4 ACQUIRING THE IMM.....	H-17
H.4.1 Information Management and Models.....	H-18
H.4.2 What Has the Customer Already Done.....	H-19
H.4.3 Description of IMM.....	H-20

UNCLASSIFIED

Appendix H  
IATF Release 3.1—September 2002

H.4.4 Other Models ..... H-21

H.4.5 Why IMM Is Important..... H-25

H.5 THE LEAST-PRIVILEGE IMM..... H-25

    H.5.1 Least-Privilege Concept..... H-26

    H.5.2 Consolidation..... H-26

    H.5.3 Information Domains..... H-27

    H.5.4 Revised IMM..... H-28

H.6 THREAT ANALYSIS ..... H-28

    H.6.1 Identifying Harm to Information ..... H-29

    H.6.2 Identifying Potentially Harmful Events..... H-30

    H.6.3 Combining HTI and PHE to Estimate Information Threats ..... H-31

H.7 CUSTOMER PRIORITIES ..... H-34

    H.7.1 Presenting the Threat Analysis ..... H-34

    H.7.2 Obtaining the Customer’s View ..... H-35

    H.7.3 Managing Reactions ..... H-35

    H.7.4 Setting Priorities ..... H-36

    H.7.5 Achieving Consensus..... H-36

H.8 PREPARING THE IPP..... H-36

    H.8.1 Explain the IPP Purpose and Type of IPP ..... H-37

    H.8.2 Identify Existing Policies, Regulations, and Procedures..... H-37

    H.8.3 Establish Roles and Responsibilities ..... H-38

    H.8.4 Identify Decision Makers..... H-39

    H.8.5 Define C&A Procedures ..... H-39

    H.8.6 Identify Security Service Requirements ..... H-39

    H.8.7 Document Results..... H-42

H.9 CUSTOMER BUY-IN ..... H-42

    H.9.1 Explain Ownership (Again)..... H-43

    H.9.2 Explain the Need for High-Level Endorsement ..... H-43

    H.9.3 Explain the Need for Maintenance ..... H-43

    H.9.4 Explain the Need for Necessary Resources ..... H-43

H.10 SUMMARY ..... H-44

PNE GLOSSARY AND ACRONYM LIST ..... H-45

REFERENCES..... H-47

PNE ANNEX A: IMM EXAMPLE

PNE ANNEX B: CORPORATE IPP

PNE ANNEX C: DIVISION IPP

**List of Figures**

Figure H-1.	Requirements Hierarchy.....	H-2
Figure H-2.	Requirements—Need Versus Solution.....	H-4
Figure H-3.	PNE Within the INFOSEC Business .....	H-5
Figure H-4.	SE (and ISSE) Process .....	H-6
Figure H-5.	Protection Profile.....	H-7
Figure H-6.	DITSCAP Subprocesses of Phase 1—Definition .....	H-8
Figure H-7.	Risk Management.....	H-9
Figure H-8.	Seven Procedures .....	H-11
Figure H-9.	Information Management Model .....	H-19
Figure H-10.	IDEF Model Example .....	H-22
Figure H-11.	IDEF With Buffers and Release.....	H-22
Figure H-12.	IDEF Modified .....	H-23
Figure H-13.	Structured Analysis Model.....	H-24
Figure H-14.	Types of Harm to Information .....	H-29
Figure H-15.	Sources of Potentially Harmful Events .....	H-30
Figure H-16.	Adversaries.....	H-30
Figure H-17.	Information Threat .....	H-32
Figure H-18.	Map Type of Harm to Security Service .....	H-41

**List of Tables**

Table H-1.	Requirements—Need versus Solution .....	H-3
Table H-2.	Simple Example of an IMM.....	H-20
Table H-3.	Table Model of IMM.....	H-24
Table H-4.	Least-Privilege Example .....	H-26
Table H-5.	Categories Before Consolidation .....	H-27
Table H-6.	Categories After Consolidation.....	H-27
Table H-7.	Information Domain Example.....	H-27
Table H-8.	PHE and HTI Measures.....	H-32
Table H-9.	Information Threat Data.....	H-33
Table H-10.	Information Threat Combination Matrix.....	H-33
Table H-11.	Information Threat Table (ITT) .....	H-34
Table H-12.	Information Threat Table .....	H-40
Table H-13.	Information Threat Data.....	H-40
Table H-14.	Map ‘Information Threat’ to ‘Strength’ .....	H-41
Table H-15.	Data for Information Protection Requirements.....	H-42

**UNCLASSIFIED**

Appendix H  
IATF Release 3.1—September 2002

**This page intentionally left blank**

# Appendix H

## Protection Needs Elicitation

---

### H.1 Introduction

Information systems security engineering (ISSE) is defined in Chapter 3 as a sub-process of systems engineering (SE). The basic activities of SE are to—

- Discover Needs.
- Define System Requirements.
- Design System Architecture.
- Develop Detailed Design.
- Implement System.
- Assess Effectiveness.

The ISSE process is involved in each of these basic activities. This document describes Protection Needs Elicitation (PNE), that part of Discover Needs in which information protection needs are determined or elicited from customers.

ISSE practitioners must understand the merits of ISSE so they can educate customers. The ISSE practitioner, like the systems engineer, must achieve a balance between satisfying best practice and the desires of customers to advance to an expedient implementation. The goal of the ISSE activities process covered in this appendix is to describe ISSE best practice.

#### H.1.1 Purpose

This section defines the protection needs elicitation activity and directs the PNE practitioner to—

- Help customers model their information management.
- Help customers to define an information threat. (Typically, customers know more about their threats than the systems security engineer does.)
- Instruct the customer to document perceived threats and responses to them.
- Help customers to prioritize their protection needs.
- Prepare information protection policies that security architects can use.
- Achieve customer buy-in. (If the PNE practitioner applies the following principles, the resulting analysis will be understandable, acceptable, and supported by the customer. This buy-in is critical to any program.)

Although there are many activities that support the business or mission of an organization, such as manufacturing or the use of weapon systems, information management is the chief concern

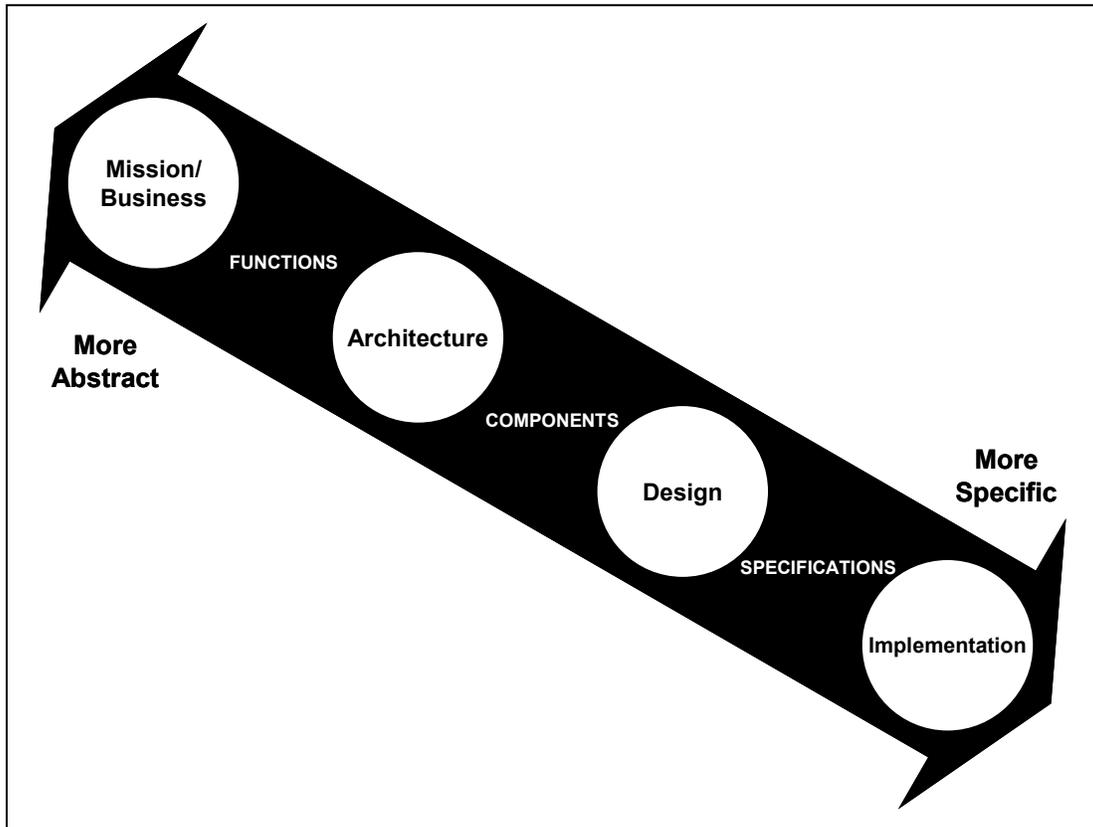
# UNCLASSIFIED

here. Before the information system solution is designed and implemented, requirements should be thoroughly analyzed and prioritized. This activity not only saves the customers substantial cost and time, it also produces better operational results. A similar information-requirements analysis is also valuable relative to an existing system—before installing upgrades, and before analyzing the risk posture of the system even when no changes are planned.

Information management always carries with it the risk of unwanted disclosure, modification, or loss. Customers realize the importance of their information but usually need help in discovering their protection needs and priorities. This appendix defines a method for eliciting those customer protection needs.

The word “needs” here is interchangeable with “requirements.” Many meanings are associated with “requirements.” Some rank desires, needs, and requirements alongside nice-to-have, very useful, and essential. Rather than making distinctions, it is important to recognize and prioritize needs and requirements and especially to distinguish between “good” and “not good” requirements.

A layered requirements hierarchy may be envisioned (see Figure H-1) that asserts a layer (shown to the left in Figure H-1) that imposes requirements on the next lower layer. What are called “requirements” may help identify which layers are affected.



iatf\_h\_1\_0084

Figure H-1. Requirements Hierarchy

What is considered a good requirement depends on where one is in the hierarchy. What remains consistent is that requirements become more specific as one moves downward in the hierarchy and more abstract as one moves upward. A good requirement does not jump elements of the layers. It gives practitioners the flexibility to exercise their skills to produce better results.

Table H-1 illustrates a jump from a protection need to a specific solution. A practitioner who uses a solution-based approach (sometimes hard to avoid) should not spend much time with architecture or component design. A better approach would be to seek the need underlying the design limitation and to obtain customer concurrence.

**Table H-1. Requirements—Need versus Solution**

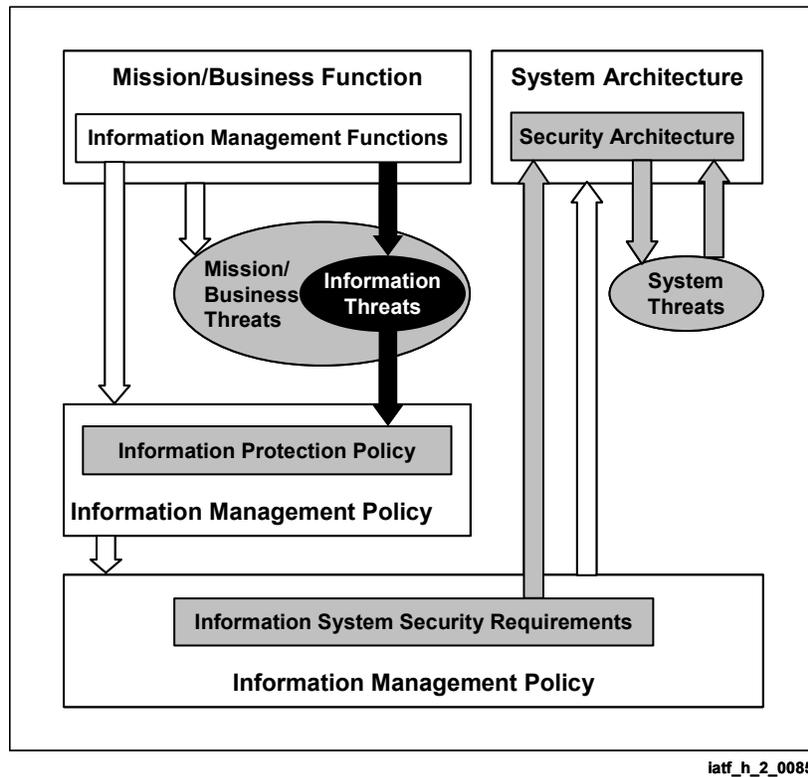
Basis of Requirement	Value of Approach	Typical Criteria			Example
Need	Good	Need	What	Abstract	I need protection from disclosure of my information.
Solution-based	Not good	Solution	How	Specific	I need KG-175 TACLANE COMSEC devices.

Although the specifications requirements (from design to implementation) may ultimately include a crypto-device such as a KG-175, the conceptual requirement (from architecture to design) is transmission confidentiality. The corresponding functional requirement (from mission to architecture) is a need to protect the information from disclosure while it is being transferred between any two entities.

Figure H-2 illustrates the relationship between the PNE portion of ISSE and SE. Assuming that business or mission success depends on successful information management, information management functions (models) form the basis for information system requirements that are consistent with the organization’s information management policy. A system architecture can be proposed to meet the information system requirements. ISSE is indicated in Figure H-2 by the four shaded areas. PNE is indicated by the darker shading.

Adversaries can threaten the success of the business or mission. Threats may be directed at the information management functions and also at people, manufacturing processes, or product management. The response to the possibility of threats to information is an Information Protection Policy (IPP) that directs and prioritizes the response to those threats. Through system definition, some of the elements of the IPP are allocated to the target system to become the information system security requirements. Those requirements lead to the design of a security architecture.

The system architecture provides a baseline definition for threats to the system or specific attacks on it that will need to be countered by the security architecture. This appendix is concerned with the information management functions, information threats, and the IPP part of the ISSE process shown in Figure H-2.



**Figure H-2. Requirements—Need Versus Solution**

PNE supports many disciplines, programs, processes, and activities. For example—

- The Information Systems Security (INFOSEC) business.
- The SE process, which includes the ISSE process.
- The evaluation of security products, including those in which Common Criteria language is used.
- The Department of Defense (DoD) Information Technology Security Certification and Accreditation Process (DITSCAP).
- Risk management.

## H.1.2 PNE and the INFOSEC Business

ISSE combines security disciplines, technology, and mechanisms (see Figure H-3) and applies them to satisfy the protection needs of the customer. The result is an information system that incorporates the security architecture and mechanisms that best meet protection needs within the cost, performance, and schedule allowed by the customer. PNE is the ISSE customer interface activity. SE engages the customer for the other requirements.

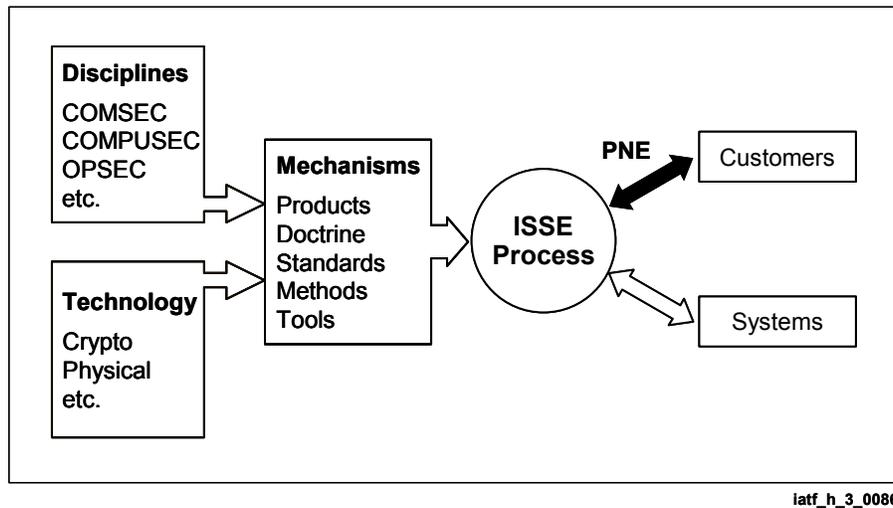


Figure H-3. PNE Within the INFOSEC Business

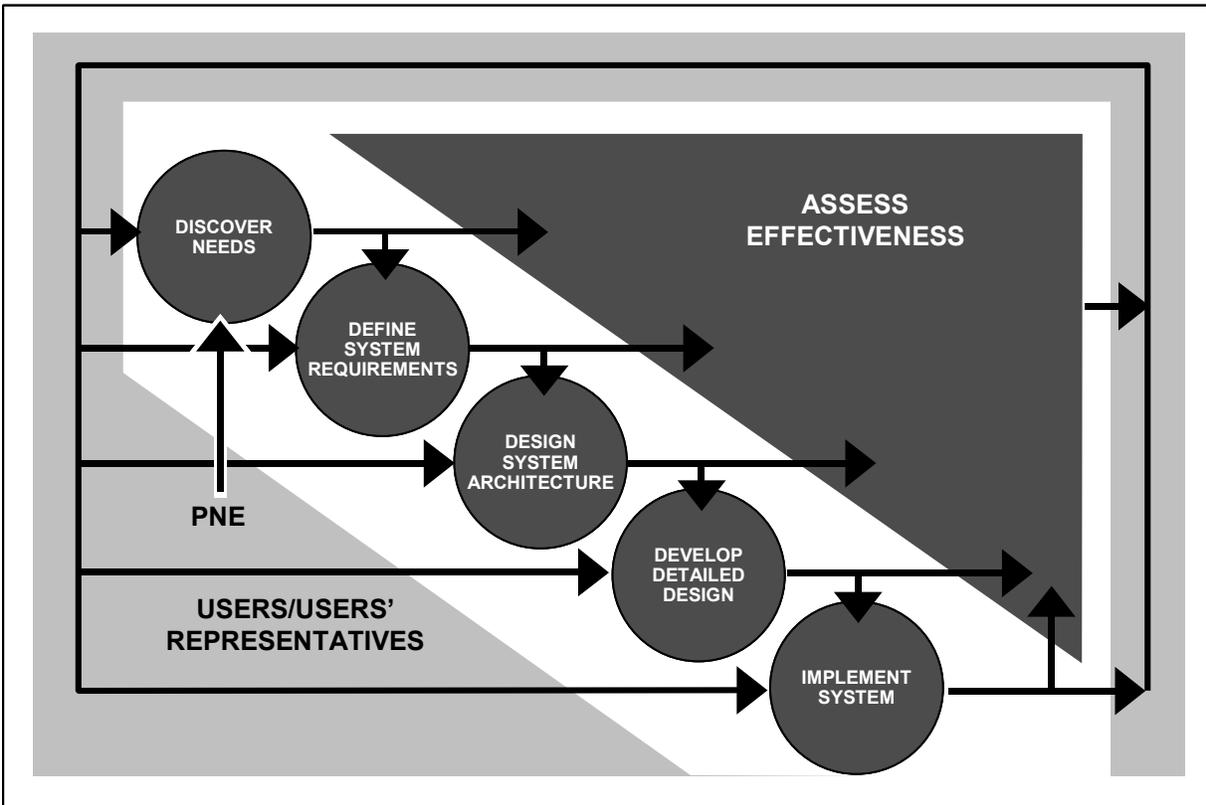
## H.1.3 PNE, ISSE, and SE Process

Because ISSE is a specialty within SE, it follows the methods of that discipline. ISSE usually works in an environment in which the customers may have their own methods or processes. PNE is part of all ISSE activities and probably provides the biggest potential cost-saving opportunity within the ISSE process. The security and nonsecurity benefits of PNE are discussed in Section H.3.4. Figure H-4 depicts the six activities of the SE and ISSE process that draw from and respond to users and customers:

- Discover Needs.
- Define System Requirements.
- Design System Architecture.
- Develop Detailed Design.
- Implement System.
- Assess Effectiveness.

In the Discover Needs activity, ISSE—

- Analyzes mission and business.
- Analyzes information management.
- Elicits data on mission capability needs, including information threatened and information protection needs (PNE).
- Achieves stakeholder consensus on those needs, including information protection needs.



iatf\_h\_4\_0087

**Figure H-4. SE (and ISSE) Process**

Clearly, PNE performs Discover Needs activities. The Discover Needs activity does in fact elicit information protection needs on the basis of what harm there would be to the mission or business if information were disclosed, modified, unavailable, or lost.

PNE is an integral part of Discover Needs. The mission and business needs include protection needs. But the scope of PNE is limited to information management. PNE is not engaged with either architecture or implementation.

Finally, there is a valid rationale for using the PNE “achieving user/customer consensus” function in the ISSE Assess Effectiveness activity.

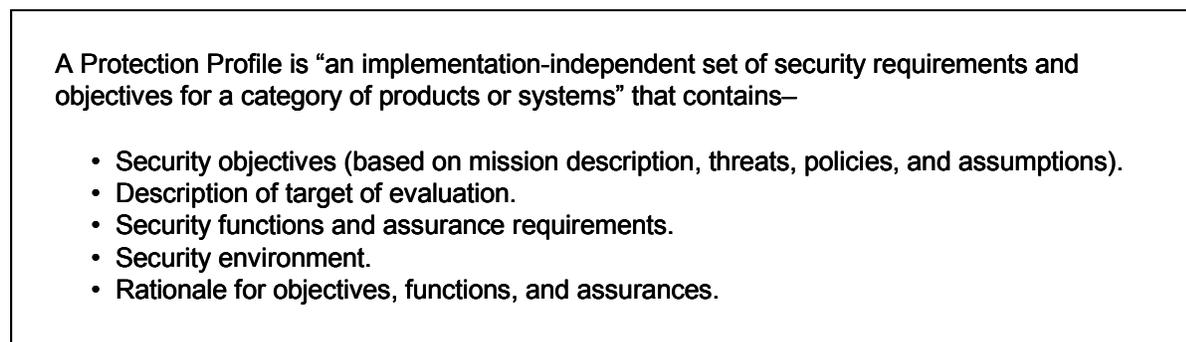
## H.1.4 PNE and Common Criteria

The Common Criteria have evolved from international computer security product evaluation criteria. The Common Criteria language is a selectable set of statements defined as security functions and an independent set of assurance levels that describe function success. Because use of Common Criteria is still primarily oriented toward security products, the relationship between PNE and Common Criteria is complicated. PNE provides the information protection portion of the mission or business description. That information may be applied to creating two types of

Common Criteria documents, a protection profile and a security target. Because both documents refer to a security product or system called a target of evaluation (TOE), they cannot be completed until a system or product is designed. PNE provides Common Criteria information for—

- Creating a description (a Protection Profile) of an organization’s protection needs for the TOE, using mostly pre-specified functions and assurance levels—the Common Criteria language. The Protection Profile provides a statement, independent of implementation, of the functions and assurances the organization needs.
- Creating a description (the Security Target) of a solution after evaluating how a particular security solution or category of solutions satisfies a particular TOE’s Protection Profile. The Security Target, which is directly related to a TOE, explains how the TOE meets function and assurance needs.

Figure H-5 shows the content of a Protection Profile. The PNE process provides the security objectives. In reality, the TOE’s security functions and assurance level can be derived only from an analysis of the organization’s requirements and threats, from which the security objectives are drawn. The PNE security objectives are a detailed set of security services and strengths that are prioritized by the customer. They must be translated into the language of the Common Criteria, which is syntactically rigid but allows new functions to be created in the form of the language.



iatf\_app\_h\_5\_h005

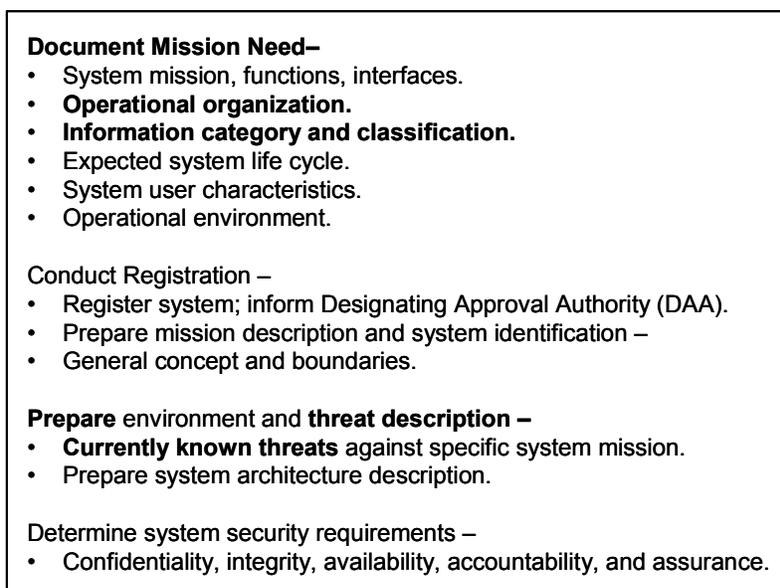
**Figure H-5. Protection Profile**

## **H.1.5 PNE and DITSCAP**

DITSCAP, the DoD’s standard process for certification and accreditation (C&A) of information technology (IT), provides an excellent list of things to be discovered and documented to guide the C&A process, but it provides no clues as to how to acquire the information. This appendix does. For DITSCAP, it is necessary to prepare and continually update a document called the System Security Authorization Agreement (SSAA). The SSAA serves as a control document for the security of the IT system from “womb to tomb” for both full and contingent accreditations. In the early phases of DITSCAP, the SSAA documents the requirements, including a form of a security policy. The DITSCAP has four phases—

- Phase 1—Definition.
- Phase 2—Verification.
- Phase 3—Validation.
- Phase 4—Post-Accreditation.

PNE satisfies some of Phase 1 of DITSCAP. The subprocesses of Phase 1 that match PNE are boldface in Figure H-6.

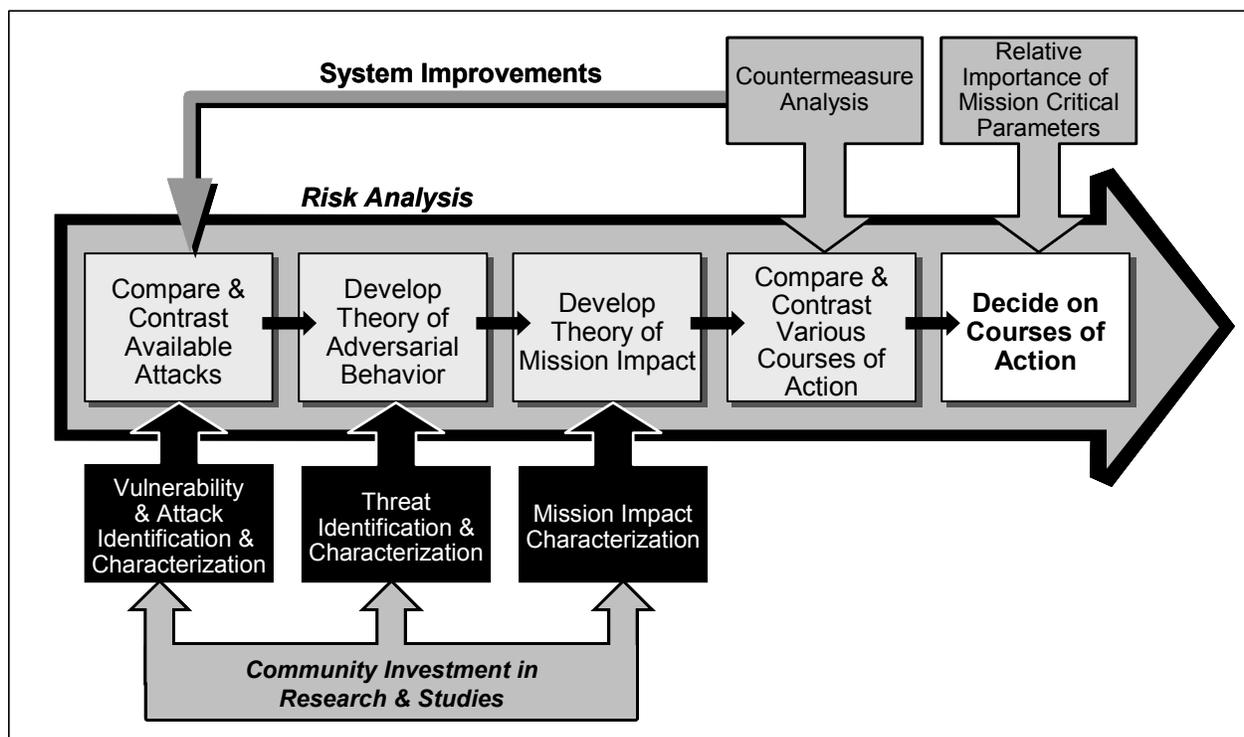


latf\_app\_h\_6\_h006

Figure H-6. DITSCAP Subprocesses of Phase 1—Definition

## H.1.6 PNE and Risk Management

Risk management programs require documentation of exactly the same mission and security needs as ISSE (see Figure H-7). The only difference is that the emphasis is assessing risks of and improving existing systems rather than designing new systems.



iatf\_app\_h\_7\_0144

Figure H-7. Risk Management

## H.2 Overview

This section summarizes the seven major PNE procedures, but begins by addressing the following three items—

- The characteristics expected of the PNE practitioner.
- Important acronyms.
- The types of documents that should result when the PNE process is completed.

### H.2.1 PNE Practitioner Characteristics

The ideal PNE practitioner is a systems engineer or systems analyst who has—

- Familiarity with the business and mission area.
- Good communications skills.
- An information security background.
- Program management experience.

The most important asset for the PNE practitioner is the ability to approach problems with a systems approach to problem solving. The ISSE engineer can think abstractly and can conduct analysis on the basis of intuiting eventual results. Engineering training often forces a degree of

detail and thoroughness that encourages engineers to use a bottom-up approach. This section emphasizes a top-down approach for the PNE practitioner as the preferred approach. The systems analyst can play a role identical to, or share responsibilities with, an information systems security engineer in the PNE process.

A general knowledge of the business or mission area is not essential for the PNE practitioner, but it does shorten the learning curve and facilitates communicating with the customer. In addition, program management experience for systems engineers, adds value to an SE team.

## H.2.2 Acronyms

The acronyms that have special relevance here are—

- **IMM**—Information Management Model.
- **IPP**—Information Protection Policy.
- **ISSE**—Information Security Systems Engineering (or Engineer).

## H.2.3 PNE/ISSE Documents

The following documentation could result from the PNE process.

- **Project Plan/Task Definition**—prepared by the information systems security engineers and briefed to the customer.
- **Customer Documentation**—although optional, customer documentation further supports the project plan and task definition with details of what is expected.
- **IMM**—an initial model of the eventual information system, which embodies the important concept of least privilege.
- **IPP**—the latest documented set of protection needs in the form of a policy, which represents the final result of the PNE. The policy contains a threat analysis describing potentially harmful events and their effects. The IPP also contains a prioritized list of needed security services.

Defining the information protection that is required can be very precise. Is the amount of detail produced by PNE useful and necessary? Indeed it can be. When the ISSE process arrives at risk analysis, a detailed IPP will be a sound basis for comparing what was required with what was accomplished. A disadvantage, though, is that details may be ignored during security-architecture and implementation, because the designers may take shortcuts and simplify the system for good, practical reasons. In each situation the information systems security engineer and the customer determine how much detail is needed. Further, both the customer and the accreditor should fully understand and accept the degree of detail.

## H.2.4 Seven Procedures

PNE requires the application of seven procedures (see Figure H-8).

## H.2.5 Approaching the Customer

After the initial contact, the PNE practitioner needs to understand—at more than surface-level—the customer’s business or mission. This understanding helps to build customer confidence, which is important in promoting the value of PNE to the customer’s security management program. At this stage, the practitioner presents the customer with a budget and an analysis plan that defines specific roles and responsibilities.

## H.2.6 Acquiring the IMM

A model is a representation of concepts with the purpose of reducing ambiguity. The ISSE engineers eventually become familiar with various customer models, but the models will all have common information elements that are useful to PNE. If the customer has not constructed an IMM, the information systems security engineer will need to develop one. The importance of information management is apparent from Figure H-2. Modeling at this stage, which visually presents how information is managed, includes incorporating the customer’s models into a comprehensive IMM.

## H.2.7 The Least-Privilege IMM

Information access is an IMM issue. The modeling of information management should naturally try to define only those people or jobs that are necessary to accomplish mission or business functions. Often, however, there is a need to review the results to redefine “necessary.” A least-privilege revision of the IMM helps to eliminate unnecessary access to information and provides a better baseline for threat analysis.

## H.2.8 Threat Analysis

“Threat analysis” means different things to different people. In PNE, threat analysis takes into account the information, information management, the definition of adversaries, adversary motivation, non-malicious harmful events, and the effects of harmful events. It is important to note that during the PNE phase of ISSE there is no definition of the system and hence no possible notion of vulnerabilities.



iatf\_h\_8\_0090

**Figure H-8. Seven Procedures**

## H.2.9 Customer Priorities

Providing the best information to help the customer recognize threats will result in the most successful threat analysis. The threat analysis should be prioritized and at a level of detail that the customer can absorb. Reactions to the threat analysis within the customer's organization may be diverse, which will require resolution.

## H.2.10 Preparing the IPP

The IPP is a policy document (note that "policy" has as many definitions as "threat"). The IPP lists the requirements for any solution to protect the managed information. It is a vehicle for resolving issues by coordination (through publishing, reviewing, and commenting and modification). The intent of PNE is to produce a very detailed IPP, covering all types of information, user privileges, and required security services. The IPP is useful to the security architect, who is one of the principal targets for its application.

## H.2.11 Customer Buy-In

Achieving customer support of the agreement to maintain and enforce the IPP, including the application of the resources and agents responsible for its execution, completes the PNE procedure. Customer support of the agreement is crucial for—

- Definition of the system solution.
- Development of a security architecture consistent with the IPP.
- Development of a system consistent with the IPP and the security architecture.

The following sections provide more detail about the seven PNE procedures and offer ISSE strategies for planning a PNE project.

## H.3 Approaching the Customer

Probably the most critical step in any ISSE project is Approaching the Customer. Some believe that the information systems security engineer should not talk with the customer but only with the customer's technical representatives. However, if all the information systems security engineer knows about the project is what the system engineers convey, the project will be severely handicapped. The information systems security engineer must be grounded in the customer's needs so it can try to satisfy them. The engineers must explain suggested plans and services and obtain the customer's concurrence. Obviously, this activity is marketing and



iatf\_h\_8\_0090

contracting. It is critical that the PNE practitioner be professionally prepared by—

- Knowing as much as possible about the customer.
- Leveraging initial contacts.
- Presenting the benefits of proposed services to decision makers concisely.

Whether seeking a contract or undertaking tasks, the engineers and systems analysts must clarify their roles and responsibilities and those of co-workers before work begins.

An important aphorism—and fact—is, in order to sell PNE, you must know PNE.

The activities in Approaching the Customer are—

- Making initial contacts.
- Learning the business and mission.
- Developing contacts.
- Selling the value.
- Planning for PNE.
- Setting project roles and responsibilities.

## H.3.1 Making Initial Contacts

The types of customer contact are—

- Technical—
  - Engineering.
  - Security.
- Management—
  - Chief (executive, operating, information, or security) officer.
  - Program/project leader.

In an IS modification or development program, the most likely initial point of contact (IPOC) for the information systems security engineer is the customer's technical representative—an engineer, a software/systems administrator, or a member of the corporate security staff who requires help in information security. The IPOC can facilitate information gathering and other contacts within the customer's organization. Communicating with the decision makers, whose participation and support is critical to a successful information protection program, is especially important.

In many instances, the customer's system is not only defined but is also mature. Security happens to be an afterthought, and many decisions have already been made about the purpose and design of the system. Nevertheless, the PNE practitioner must do the homework, using the IPOC to gain further information from the documentation or through interviews with customer

personnel. A prime objective is to meet with the decision makers—the DAA, Chief Executive Officer (CEO), Chief Operating Officer (COO), Chief Information Officer (CIO), or senior program manager—for initial input. Obtaining approval to proceed with PNE as part of the customer's program will later require briefing these same decision makers on the PNE plan.

## H.3.2 Learning the Business and Mission

Before discussing any tasking with the IPOC, the PNE practitioner must gather as much customer data as possible:

- Organization.
- Objectives.
- Major functions.
- Products.
- Supporting and supported organizations.
- Future plans.

The PNE practitioner gains the confidence of the IPOC when he or she demonstrates knowledge of the customer's business and mission and comprehension of the customer's information management and protection needs.

Unless the organization has a sensitive mission or a very poor marketing division, a wealth of information is usually available:

- **Published Information:** Mission statements, organizational advertising, trade and news magazines, government directives, and the World Wide Web.
- **People Networks:** Team members of previous traceable projects, business and government associates, and customer advocates.
- **Current and Past Contracts or Requirements:** The *Commerce Business Daily*, Requests for Quote, and the Web site: <<http://cbdnet.gpo.gov>>. The PNE practitioner may receive assistance from his or her own marketing division or from those who track current and past Requests for Proposals/Requests for Quotes (RFP/RFQ) released by the customer.

## H.3.3 Developing Contacts

The PNE practitioner must build associations and trust with two valuable sources: initial contacts, including the IPOCs and the decision makers.

Initial contacts are important because of their—

- **Leverage With the Decision Makers:** The IPOC, a friendly insider, opens the door to the organizational network. In particular, the IPOC can work the system to make

appointments with other needed contacts—especially busy decision makers—and knows how to approach them. However, the practitioner should first use other contacts the IPOC recommends before taking up decision makers' time.

- **Inside Coordination:** The IPOC can help make appointments, explain the purpose of PNE, keep track of schedules, and help to build trust.
- **Access to Information Sources:** The IPOC will be a good source of information about the project.

The PNE practitioner should have at least three sessions—other than interim reporting meetings—with decision makers:

- Briefing them on the purpose of PNE and getting their views on requirements.
- Presenting the plan for providing services and getting a commitment.
- Presenting the results of the PNE.

The PNE practitioner must be prepared for meetings with decision makers by—

- **Optimizing Available Time:** Decision makers are busy; it is important to be brief and to the point and to present a rational approach to getting the job done. One strategy is furnishing decision makers with background material before meeting.
- **Scheduling Carefully:** Know what needs to be accomplished and let decision makers know what is expected of them and what resources are needed.
- **Defining PNE Benefits (see Section H.3.4):** Build a solid case for the PNE project and how it benefits the customer's program.
- **Requesting a Decision (see Section H.3.4):** At the second meeting, the practitioner presents the PNE plan and gets a decision.

## H.3.4 Selling the Value of PNE

Selling PNE requires an understanding of and a belief in its merits. An experienced practitioner can present both nonsecurity and security PNE benefits to a customer.

The nonsecurity benefits result from in-depth analysis of the information to be managed by any solution. The analysis results in an IMM of the workings of any solution and a detailed definition of desired information management needs. The nonsecurity benefits of PNE include—

- **A Better Understanding of Information Management.** PNE analysis results in a document that presents who manages what information using what processes or functions (see Section H.4). This analysis nearly always appeals to managers who rarely have thought about that aspect of their organizational activities. If the customer has done the analysis, PNE will increase ISSE team knowledge and provide an independent check.

- **Requirements Analysis Before System Analysis Begins.** The IMM is a tool for presenting requirements to the system architect—the quality and detail of the analysis removes most of the ambiguity. The analysis can save time and money and avoid operational surprises.
- **A Baseline for Evaluating Results.** Whether constructed by the PNE practitioner or by the customer and reviewed by the practitioner, the IMM is an important requirements control document. For ordinary configuration control and requirements tracing, the IMM is the baseline for evaluating the results—the operational performance of the solution.
- **Defining needed administrative resources.** The information-centric approach naturally leads to questions (and answers) about managing the solution and the administrative data to make it work. In particular, the {WHO, WHAT, FUNCTIONS, PROCESSES} approach evolves into a definition of the administration resources needed and the roles of all of the systems administrators.

The security benefits of PNE include—

- **Documentation of Threat.** By categorizing information, the IMM becomes the basis for examining threats to information. The PNE threat analysis investigates the motivation any adversaries might have to attack the information and the likely effect of an attack. By involving the customer, the analysis effects a realization of potential harm and of the value of the customer's information.
- **Documentation of Policy.** After recognizing the potential harm and the value of information, the customer can arrive at decisions about priorities for protection and security services. This part of the PNE results in an IPP that reflects the concerns and decisions of the customer.
- **Prioritized Protection.** The customer's priorities as stated in the IPP are valuable information for the security architect who must use available resources efficiently by allocating resources in proportion to threat.

### H.3.5 PNE Project Planning

The practitioner presents a PNE plan, with a budget, to the customer. The plan must be explained in the context of the customer's program and should include a justification in terms of benefits. The practitioner must show the customer the scope of the PNE effort (team and customer) to produce an IPP together with costs and schedule. The costs include those for both the PNE team and the required customer resources, such as IT, security, operations, and management personnel to meet with the PNE team, review documents, and make recommendations on policy and priorities.

The justification puts PNE in the context of the customer's program by stressing that information protection results from good requirements analysis. PNE benefits to the customer's risk management program include identifying potential losses and the potential reductions in risk. In

addition, the resulting IPP will inform the customer about resources needed to carry out the policy for security and administrative life-cycle security support (the IPP does not address nonsecurity system support).

## H.3.6 Setting Project Roles and Responsibilities

A project often faces obstacles if roles and responsibilities have not been assigned. Hence, the plan must identify all players and their expected contributions and commitment to the project. Typically, the major players are—

- Decision makers, who approve and direct the project.
- IPOCs (specifying the need for their continuing support throughout).
- Operations people (specifying the need for them to review and accept the requirements).
- Security administrators (specifying the need for them to define and coordinate support to the eventual system).
- Certifiers and accreditors (specifying the need for their involvement from the beginning and throughout the system's life cycle).
- The PNE team and its resources.

Completeness is important. Individuals must be specified to fulfill every project need. After the plan is submitted, the decision makers either accept the plan as is, request modifications, or reject the plan.

## H.4 Acquiring the IMM

Before a solution is selected, its function must be defined. It will manage information but what information will be managed, who will manage it, and what the managers do must be established.

This section describes the mechanics of modeling information management. The focus is on information rather than systems because the focus of the discipline is to produce a requirements analysis that is independent of solutions. The requirements documented will later be used to evaluate any proffered system solution in the ISSE process.

The topics in Acquiring the IMM are—

- **Information Management and Models**—The use of models is a proven technique for defining and exchanging concepts. Systems engineers use a variety of models as part of the design process. This



iatf\_h\_8\_0090

section deals with information management, modeling techniques, and the basic IMM.

- **What the Customer Has Already Done**—In the best possible scenarios, the customer has created or is creating a model of the desired information management. The job then requires the information systems security team to become familiar with the model. If the customer has not created a model, the information systems security team, regardless of the state of system development, must acquire the necessary information.
- **Description of IMM**—Data required by the IMM are best acquired by interviews and from documents. The techniques used during data gathering are discussed.
- **Other models**—
  - Integrated definition (IDEF).
  - IDEF with buffers and release.
  - IDEF modified.
  - Structured analysis model.
  - IMM table.
- **Why IMM is important.**

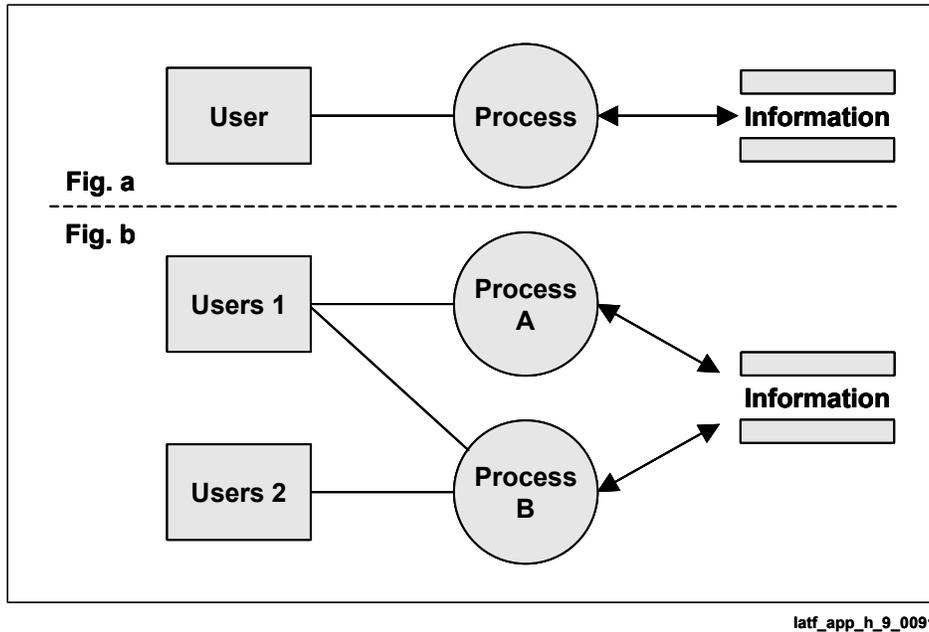
## H.4.1 Information Management and Models

The most primitive definition of “information management” is any method of—

- Creating information.
- Acquiring information.
- Processing information.
- Storing and retrieving information.
- Transferring information.
- Deleting information.

The word “processing” covers a broad set of manipulations of data that select, transform, reorganize, or otherwise process the many forms of data called information. Information management tools may be either off-the-shelf packages or custom applications.

Applying classic “structured analysis” [Yourdan] to information management yields the model in Figure H-9a. The basic model consists of users, processes, and information. The line connections imply that the user employs the process to manage the information. Any model can be expanded or decomposed into more complex models, as seen in Figure H-9b. The basic model can be decomposed but only according to specific rules. The decompositions of interest are those that create unique relationships among the three elements. Specifically, any deconstruction that does not change the users or the information category is typically uninteresting because of the least-privilege rule.



**Figure H-9. Information Management Model**

A complex model is technical data for systems people. The PNE practitioner should not use complex models to brief customers.

## H.4.2 What Has the Customer Already Done

A good systems engineering team will have documented much of the information needed. The PNE practitioner can discover whether the customer's systems personnel have analyzed and documented their systems requirements and information management. The IPOC can locate personnel operations who can access such documentation.

In general, there are three possibilities—

- **Information Management Already Modeled**—Discovering information management needs may be relatively easy because the customer has already done the work.
- **Model Needs Translation**—The second best situation is that the modeling has been constructed by the customer. However, this modeling may be inadequate and require additional information or restructuring. This situation may lead to fundamental changes in the customer model and, under the worst conditions, changes in customer design or the customer's assumed risk.
- **No IMM**—The PNE practitioner must do the research.

## H.4.3 Description of IMM

Another representation of the model in Figure H-9 is a table that includes users, process, and information (Table H-2). There is also a rules column, which later will be necessary for defining policy and user privileges; the information provided in this column may also save some work. There are multiple users, one process, and one information category.

**Table H-2. Simple Example of an IMM**

Users	Rules	Process	Information
CEO	Read, Write	Corporate Management	Policy
Employees	Read-		

In this example, corporate management informs employees about policy. In particular, the CEO manages corporate policy, but employees only see the policy. (The rules can be much more complex than those in this example.)

An important part of building the IMM is to acquire the information needed. The two methods that work best are conducting interviews and reviewing documents. The IPOC can be relied on to locate the documents or set up the interviews with knowledgeable customer employees.

Several interview sessions may be necessary. The PNE practitioner should always be sensitive to—

- **The Effects on Customer Operations.** Minimizing the effect on the customer's operations requires being prepared, knowing what is wanted, and making clear requests. Meeting with employees requires understanding that time is being taken from their other responsibilities—many with deadlines.
- **The PNE Project Schedule.** Meeting with employees according to their availability is inefficient. Realizing that not all interviewees will take the time to provide useful data in a timely manner, the PNE practitioner should use pre-interview questionnaires. Pointing out ways of familiarizing customers with project needs and being prepared to answer project-related questions is beneficial.

The best way of constructing the IMM is to identify the major functions of an organization and to decompose them into subprocesses—not only for functions directly related to products and services but also for internal support functions that may be affected by the solution, such as human resources, finances, business management, and research and development (R&D).

Decomposition should continue until the subprocesses yield no new subsets of users and their information; consolidating unnecessary decompositions later would consume precious time and effort. Typically, two decompositions to a third level are sufficient. Decomposition leads to increased detail and complexity. The customer and the information systems security team must determine the adequacy of definition. The customer may decide that further separation of users

and their privileges is unproductive and may even be counterproductive in contingency situations.

## H.4.4 Other Models

The customer may have completed several other types of models such as those listed below<sup>I</sup>

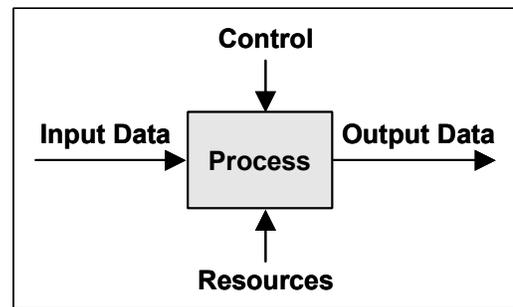
- Organization models.
- Data (information about operations, services, products) models.
- Process (describe flow of activities in business processes) models.
- Workflow (sequence of human activities) models.
- Financial (mostly spreadsheet) models.
- Simulation (detailed representation of activities) models.

These models can be a source of information for creating the IMM. The IMM models Organization, Data, and Process.

It is useful to compare the IMM with the IDEF model and the structured analysis model.

### H.4.4.1 IDEF

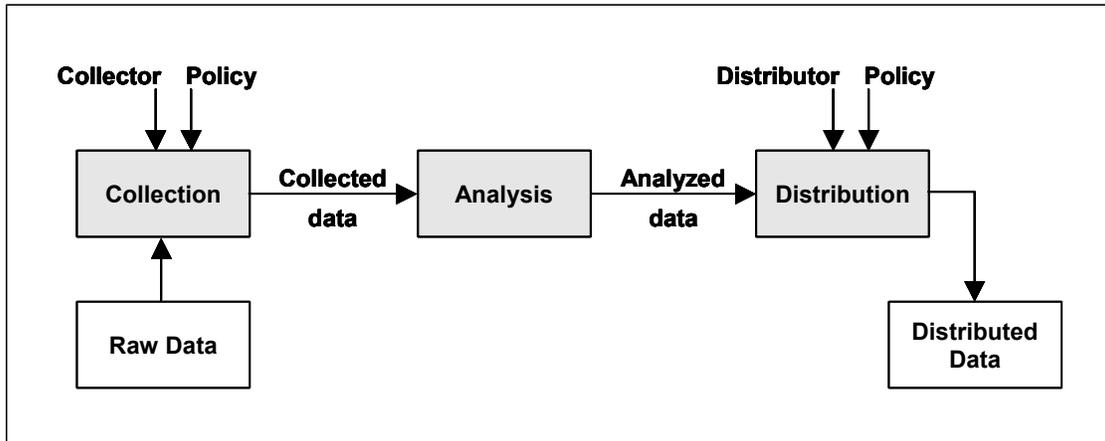
The IDEF model [IDEF] is one often used in information systems development. There are software tools that produce IDEF models. The model can be modified to become an IMM. The Input Data and Output Data arrows are typical dataflows. Resources arrows typically contain reference material or even system support data. Users and Policy/Rules are part of the Control arrow.



If the customer has used IDEF model, the PNE practitioner will need to modify it.

The example in Figure H-10 originated from an intrusion detection reporting system. This model, which emphasizes processes and the flows between them, consists of three processes, three sets of users, and possibly three policies.

<sup>I</sup> [Taylor] is the source for the bulleted items



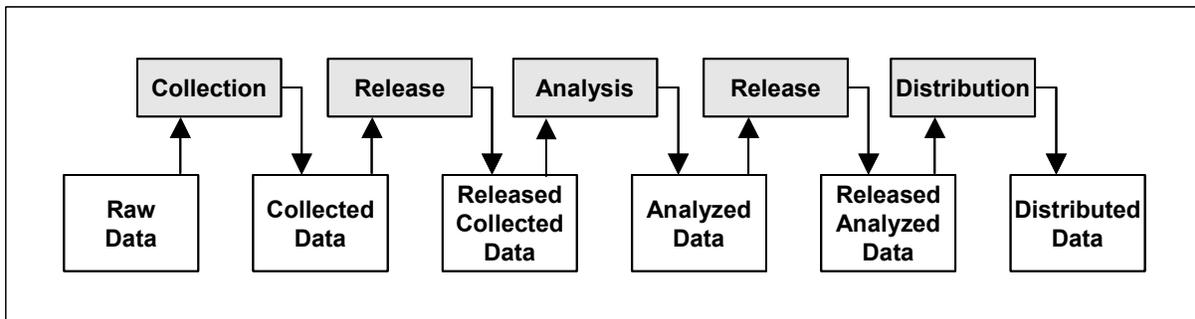
latf\_app\_h\_10\_0092

**Figure H-10. IDEF Model Example**

The three policies are not illustrated, but typically processing is partial—that is, only *some* of the—

- Raw data are forwarded as collected data for analysis.
- Processed collected data are analyzed for distribution.
- Processed analyzed data are distributed.

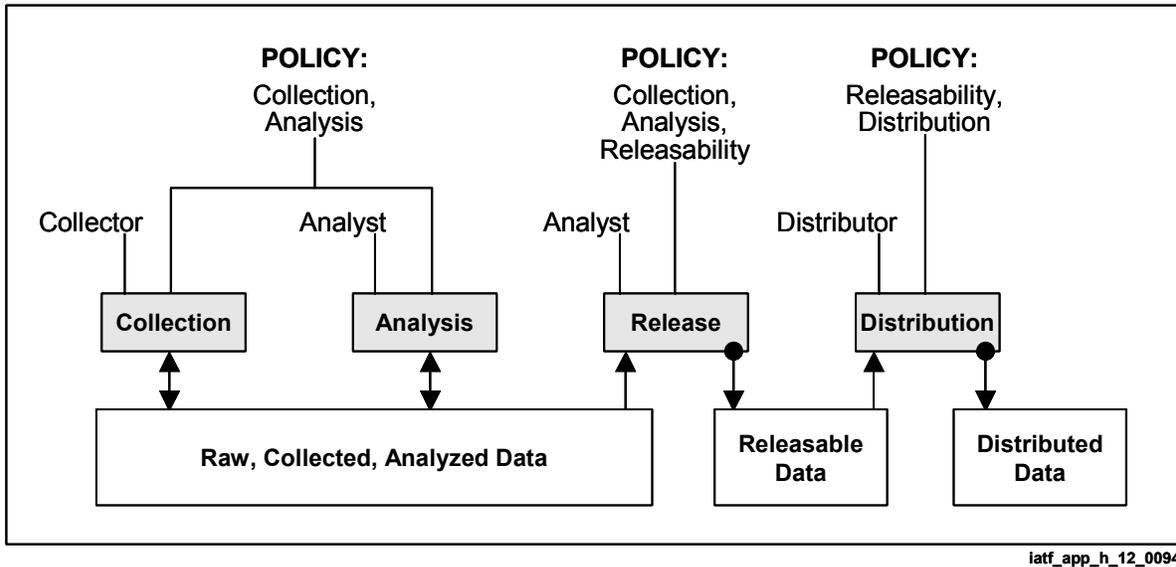
The movement of collected and analyzed data between processes is what is of interest from a security perspective. From a policy standpoint, it may be important to know what data are shared and who authorizes the sharing. This example needs better definition of policy and information sharing. One way to be explicit about policy is to show buffers—information stores—for each process and insert release processes, as shown in Figure H-11.



latf\_app\_h\_11\_0093

**Figure H-11. IDEF With Buffers and Release**

This initial modification, an excessive decomposition, remains consistent with IDEF but is a better representation for information management and protection. The arrow directions start to imply some flow or access definitions. The added data stores also raise questions about the allowable release, release controls, and sharing of data. At this point it is important for the customer to insert any rules and information about sharing and control. Figure H-12 shows the resulting fully modified model.



**Figure H-12. IDEF Modified**

The customer expresses no concern about whether the collector and analyst can manage the combined raw, collected, and analyzed information from a security perspective. In particular, although there may be a data-type separation, there is no need for a security separation. Also, the customer has decided that not all of the analyzed information can be released and relies on the analyst to decide what is releasable.

The arrow directions, important in both this and the next model, indicate the customer's rules. The dots replacing arrows at the ends of some lines indicate that the customer "doesn't care." The analyst uses the release process to make copies available to the distributor in a separate "releasable data" store. The distributor, using this access, distributes to the rest of the community, maintaining a record of what was distributed. The modified model makes explicit a policy of separation, user privileges, and data sharing; the arrowheads imply the rules.

## H.4.4.2 Structured Analysis

The model in Figure H-12 can be illustrated in the traditional structured analysis format: User—Process—Information seen in Figure H-13. This model contains the same information as the modified IDEF model.

## H.4.4.3 IMM Table

A third variation is tabular (see Table H-13), preserving all of the elements, users, rules, processes, and information. The same information management activity has been exhibited in the IDEF, structured analysis, and table models in Figures H-12 and H-13, and Table H-3. There is no "correct" way to model, but all the important elements must be present.

*Note:* The PNE practitioner should not attempt to use these often-complex models to brief a decision maker. They are tools only.

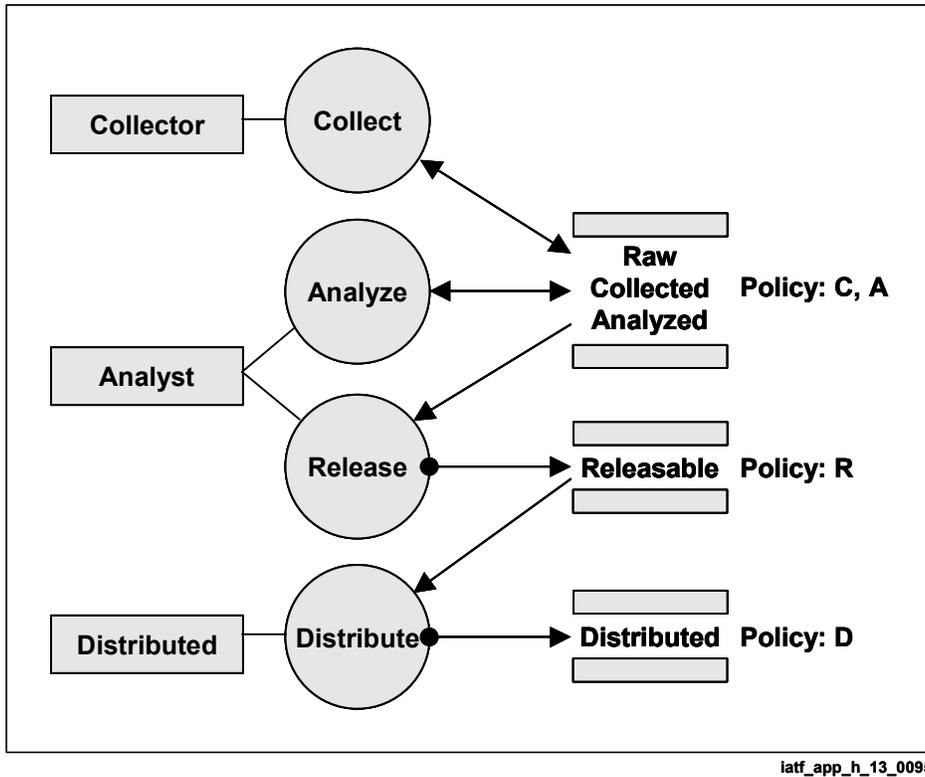


Figure H-13. Structured Analysis Model

Table H-3. Table Model of IMM

ID	Users	Rules	Process	Information
Policy CA	Collector	Read, Write	Collection	Raw Collected Analyzed
	Analyst	Read, Write	Analysis	
		Read	Release	
Policy R	Analyst	(Read), Write	Release	Releasable
	Distributor	Read	Distribution	
Policy D	Distributor	(Read) Write	Distribution	Distributed

( ) means: the action is permitted but not essential.

Annex A is an example of an IMM developed for a division of a corporation producing business forms. The content and depth of analysis of this IMM are valuable. That IMM also includes a

threat analysis (see Section H.6) and partially based on the same issues expressed in the corporate IPP (see Section H.8), as seen in Annex B.

## H.4.5 Why IMM Is Important

The finished product, the IMM, defines the information management to be accomplished by the solution in the desired detail:

- Who—Users, Rules.
- Does (or intends to do)—Rules, Process.
- With what information.

With a completed IMM, the information systems security team and the customer can begin to analyze what is and is not really necessary. It is the first stage in defining access control and privileges. The IMM is also a baseline for threat analysis, at the desired level of specificity, and for security services:

- Identification and authentication.
- Access control.
- Confidentiality.
- Integrity.
- Availability.
- Nonrepudiation.

In some cases the IMM will suggest to designers and customers simplifications that can be made by consolidating similar information categories or by relaxing the rules slightly to allow categories to be consolidated.

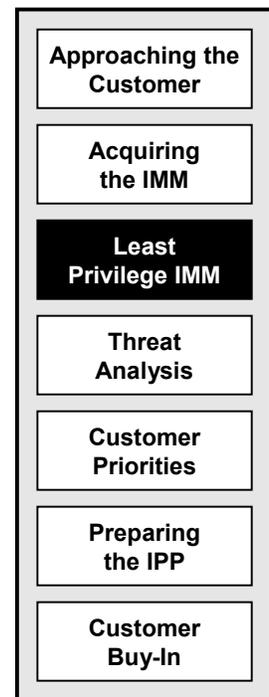
## H.5 The Least-Privilege IMM

“Least privilege” is a security-related concept that has practical value even without considering specific threats to information. A generic threat might be stated as “The more people who have access to information, the greater the probability of abuse.” This guidance document takes the following position:

Security protection is better when only those who need access to information are allowed access.

This section discusses aspects of modifying the IMM—

- **Least-Privilege Concept**—defines and explains it.
- **Consolidation**—demonstrates this IMM modification.
- **Information Domains**—explains how to set them up.
- **Revised IMM**—demonstrates completion.



iatf\_h\_8\_0090

This section also discusses two types of errors that may occur when an IMM is—

- Assigning unnecessary privileges.
- Creating unnecessary separations.

## H.5.1 Least-Privilege Concept

The decomposition process applied in developing the IMM accomplishes a major part of least-privilege control: The user-process-information segments were separated with the sense of “This set of users has some role in this process, and they manage this information.” Applying least-privilege also sets out—

- Services and activities limited to those who are essential to meeting responsibilities. Under least-privilege, roles are examined more carefully and any unnecessary privileges are removed.
- Justifiable complexity. The removal of privileges may lead to additional complexity in system design and ultimately to user frustration. Maintaining a close relationship with eventual users and obtaining their guidance and acceptance is very important.

Assignment of privileges stems from a Concept of Operation that associates people (users) with their jobs (processes). Users do the job; they need the information. Table H-4 depicts an accountant putting together financial records. The CEO, or even the CFO, probably will not have the time to manage the information directly, but from a management perspective they can see the big picture better. Notice that there may be an advantage to taking away the CEO’s “write” privileges.

**Table H-4. Least-Privilege Example**

Users	Rules	Process	Information
CEO	Read, Write	Corporate Finance	Investments, Customer accounts
Accountant	Read, Write		

## H.5.2 Consolidation

Examining the IMM will often reveal unnecessary separations of (user, process, information) categories. At this point the PNE practitioner should ask the customer to consider combining the categories. Table H-5 shows two sets of (users, process, information) categories with everything being equal except the information.

**Table H-5. Categories Before Consolidation**

Users	Rules	Process	Information
Group Manager	Read, Write	Corporate Management	Directives, Correspondence
Division Manager	Read, Write		

Users	Rules	Process	Information
Group Manager	Read, Write	Corporate Management	Progress Reports
Division Manager	Read, Write		

Information need not be separated for access control so these categories may be combined (Table H-6). Later, if it is discovered that the two information sets have different threats and security service requirements, they would be separated again.

**Table H-6. Categories After Consolidation**

Users	Rules	Process	Information
Group Manager	Read, Write	Corporate Management	Directives, Correspondence, Progress Reports
Division Manager	Read, Write		

### H.5.3 Information Domains

A unique set of [users, rules, processes, information] is an example of what DoD has defined as an “information domain” (DoD Goal Security Architecture [DGSA]). Though this is not a critical term, the PNE practitioner should understand the concept because it underlies the IPP. The concept is explained further in the DGSA (see References).

An information domain is a set of unique—

- Members of the domain—users.
- Information objects.
- Security policy identifying the relationships between members, information objects, and the security services required to protect the objects, such as least privilege.

Table H-7 displays an example of an information domain.

**Table H-7. Information Domain Example**

Domain	Users	Rules	Process	Information
Administration: Corporate	Group Manager	Read	Corporate Management	Directives, Correspondence, Progress Reports
	Division Manager	Read		

The PNE practitioner should watch for mistakes like read only or write only, meaning there are no writers or no readers in the domain. In the example, someone must prepare the information, so read only is not possible.

The rules are relatively simple; real-world policies on user privileges are more complicated. New rules are discovered with each new application of PNE.

The set of all information domains together forms the revised IMM.

## H.5.4 Revised IMM

The PNE practitioner should document and coordinate the revised IMM, also called the least-privilege IMM, with all interested parties. Because it collects all information domains, the revised IMM can be very detailed. The practitioner must identify the important reviewers and their availability. As many issues as possible should be flushed out—especially with operations personnel—before any remaining issues are sent to the decision makers.

When the revised IMM is completed, the PNE practitioner is ready for threat analysis.

## H.6 Threat Analysis

Once everything the solution is supposed to do is understood in significant detail, the information systems security team needs to investigate security, beginning with an information threat analysis. With the customer as the principal source for data, the PNE practitioner analyzes information threats in each domain in the following ways:

- **Identifying Harm to Information (HTI)**—The term **Harm To Information is shorthand for harm to the mission or business through attacks on the information.** Helping the customer identify the most to least valuable information and the types of harm that would result if it were exploited. Likely impacts to the customer's business or mission will establish priorities for protection. The PNE practitioner should ensure that all of the information domains are ranked.
- **Identifying Potentially Harmful Events (PHE)**—Helping the customer identify adversaries who might harm valuable information, the adversaries' motivations, the type of harm they might attempt, the sources of nonmalicious threats; and helping the customer to measure the likelihood of each type of adversarial attack (essentially, the adversary's motivation level) or nonmalicious harmful event.

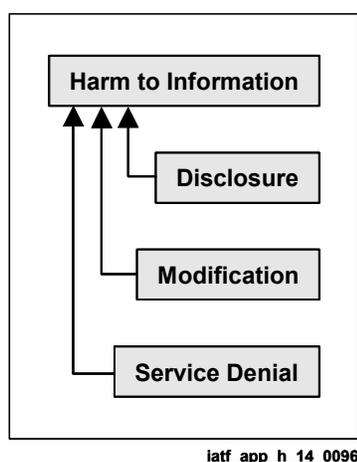


iatf\_h\_8\_0090

- **Combining HTI and PHE to Estimate Information Threat**—Analyzing and combining the HTI and PHE for each information domain listed in the IMM.

## H.6.1 Identifying Harm to Information

Examining each information domain begins with helping customers to assess its value. The value of information is viewed in many ways in the information protection community, but mainly it relates to the costs of replacing information or some other (typically non-information-system) asset if information is harmed. The PNE practitioner shows customers the types of possible harm to their information. Some are easily understood (see Figure H-14):



**Figure H-14. Types of Harm to Information**

- Disclosure, or loss of confidentiality.
- Modification, or loss of integrity.
- Nonavailability, or loss of access or service.

Other types of harm are more obscure—

- Repudiation, or loss of authenticity, leading to—
  - Denial of receipt of information.
  - Denial of sending information.

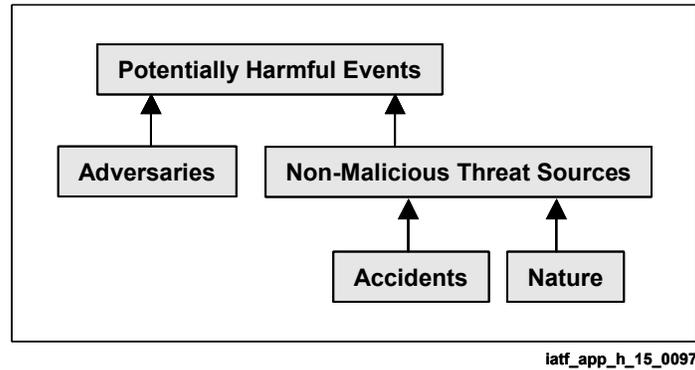
Customers can easily relate to the costs of replacing information that might be destroyed or corrupted or regaining the competitive edge lost by exposure of secrets. They will have difficulty evaluating possible loss of life. They can even assign a value to recovering from harm to their reputations. The PNE has four scales for defining harm: none, mild, significant, serious. The practitioner should use whatever metric scales the customer is comfortable with.

In helping the customer assign a metric value to information or to the effects of information exploitation for each information domain, some pertinent questions to be asked are—

- Is the harm none, mild, significant, or serious?
- If you [the customer] had to rebuild files, would that be no harm or serious harm?
  - How long would it take you to rebuild damaged files?
  - What would you not be doing while you were rebuilding damaged files?
  - Would this lost or delayed effort be significant or serious?
- If a discovery that you substantially invested in were stolen by your competitor, what would be lost?
  - How could you recover?
  - Is the cost of recovery significant or serious?
  - Is future lost revenue significant or serious?
- If a competitor acquired yesterday's stock values, would the impact be serious or not?

## H.6.2 Identifying Potentially Harmful Events

PHE may be caused by either nonmalicious or malicious threat sources or by adversaries. Nonmalicious threat sources (see Figure H-15) are natural disasters and accidents.



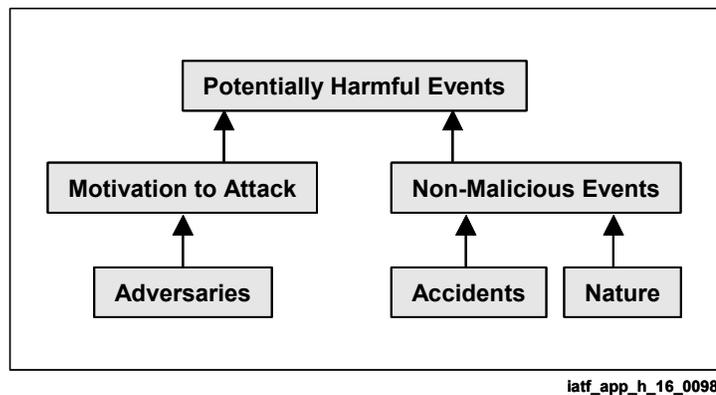
**Figure H-15. Sources of Potentially Harmful Events**

The PNE practitioner must also draw the customer's attention to a list of potential adversaries, such as those with past histories of attacks on others with a similar business or mission. Statistical reports of attacks will help with assigning probabilities. Types of adversaries that may attack information are—

- Competitors.
- Persons engaged in industrial espionage.
- Foreign governments.
- U.S. government employees and insiders.
- Hackers.
- Intruders.
- Criminals.

The PNE practitioner should present the customer with some examples of adversarial motives (see Figure H-16) for attacks—

- Sabotaging the business or mission by—
  - Destroying a capability.
  - Interfering with functions.
  - Destroying information.
  - Misleading or confusing a rival.
- Embarrassing or discrediting a rival.



**Figure H-16. Adversaries**

- Seeking monetary gain by—
  - Gaining knowledge.
  - Stealing ideas.
  - Stealing services.
  
- Acting out of curiosity or seeking notoriety.

The customer who understands adversaries and their motivations must then make a decision on the likelihood of adversaries, their motivation level, and finally PHEs (probabilities driven primarily by motivation). The four categories of PHE are none, low, medium, and high. To quantify these, the practitioner should use a metric scale the customer is comfortable with.

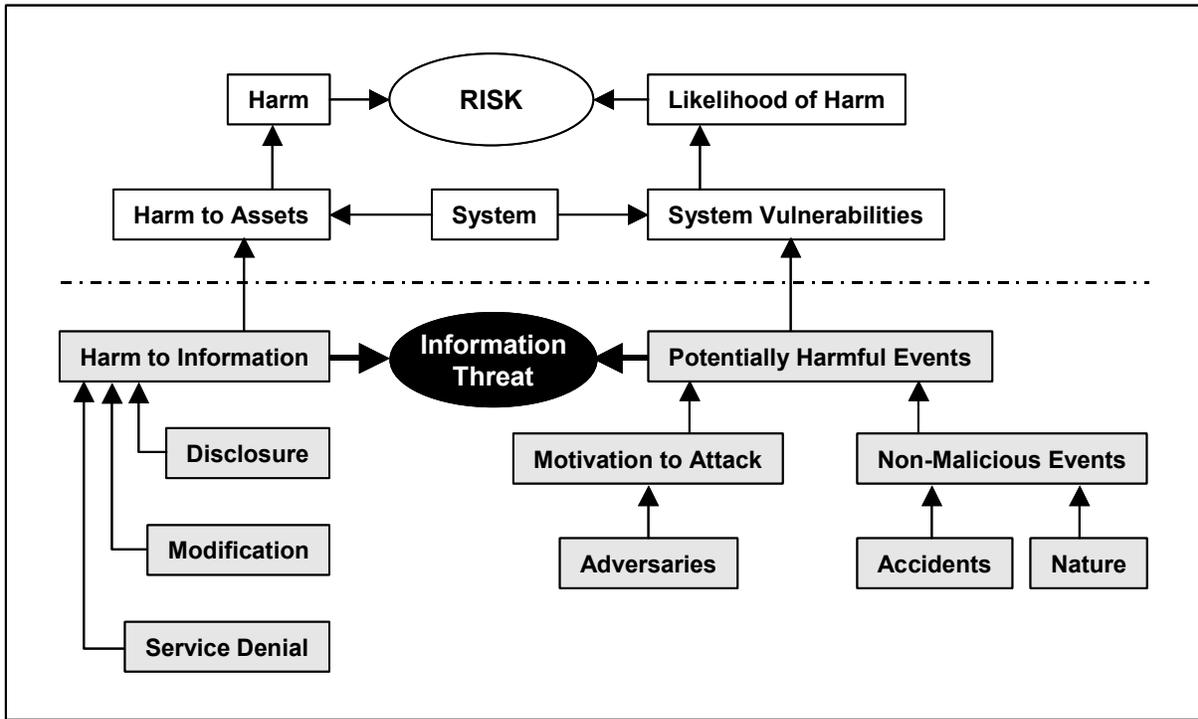
It is not realistic to assume that a solution will always provide protection. For example, one cannot assume that loss of data is not a problem because every system has backup capability. This protection-needs analysis may show the need for a backup capability. Two examples—

- An accountant at the telephone company is thinking of establishing a cost-free account for personal calls and calls by friends. What is the probability of a PHE—none, low, medium, or high?
  
- Files get corrupted by a power surge. What is the likelihood of this nonmalicious event—none, low, medium, or high?

At this stage (see top of Figure H-17), neither system nor security mechanisms have been defined. Hence, no notion of vulnerabilities exists, and a risk assessment cannot be performed.

### **H.6.3 Combining HTI and PHE to Estimate Information Threats**

The PNE practitioner uses previous analysis and estimates to prepare two tables similar to those (all data artificial) in Table H-8: one for PHE and one for HTI, both with headings for InfoDomain (domain name), Disclosure, Loss/Modification, Denial of Service, and Repudiation. The results of the estimation of PHE and HTI domain are then placed in the tables.



iatf\_app\_h\_17\_h017

Figure H-17. Information Threat

Table H-8. PHE and HTI Measures

Potentially Harmful Events				
InfoDomain	Disclosure	Loss/Modification	Denial of Service	Repudiation
Strategic planning	Medium	Medium	Low	None
Customer advocacy	High	Medium	Low	None

Harm To Information				
InfoDomain	Disclosure	Loss/Modification	Denial of Service	Repudiation
Strategic planning	Serious	Mild	Mild	None
Customer advocacy	Significant	Mild	Mild	None

The question then is, How can the measures of PHE and HTI be combined to express a combined information threat metric? The four types of quantitative data (the metrics) with measurement scales are shown in Table H-9.

**Table H-9. Information Threat Data**

Quantitative Data	Scale
Harm To Information—impact	None, Mild, Significant, or Serious
Potentially harmful event—a probability	None, Low, Medium, or High
Information threat—combining HTI and PHE	0, 1, 2, 3 (3 denotes highest information threat)
Strength of security service (described later)	None, Minimum, Moderate, or Strong

The PNE approach to combining PHE and HTI is the two-dimensional matrix shown in Table H-10—

- Row headings contain the HTI scale.
- Column headings contain the PHE scale.
- Matrix entries, combining PHE and HTI to produce information threat, are chosen from the scale {0, 1, 2, 3}.
  - 0 denotes lowest information threat.
  - 3 denotes highest information threat.

**Table H-10. Information Threat Combination Matrix**

		PHE			
		Measures	None	Low	Medium
HTI	Serious	0	2	3	3
	Significant	0	1	2	3
	Mild	0	1	1	2
	None	0	0	0	0

The numbers chosen should reflect commonsense situations (e.g., if there is no impact, any PHE results in no information threat). It is important to note that the matrix or other combining methodology is really an indication of the customer’s preference, guided, of course, by the PNE practitioner.

For each information domain and for each type of harm—

- Look up the value at the intersection of the PHE and HTI (see Table H-10).
- Record the results in a table (see Table H-11).

**Table H-11. Information Threat Table (ITT)**

Information Domain: Strategic Planning			
Disclosure	Loss/Modification	Denial of Service	Repudiation
3	1	1	0

The final results of the threat analysis are the detailed ITT tabulation by information domain of the importance of each type of harm to information. It is important to also record the rationale that supports the results and that justifies the selected PHE and HTI values. After completing the ITT, the PNE practitioner advises the customer of cooperatively developed findings and should be prepared to present the findings to decision makers for any adjustments.

The briefing to decision makers consists of—

- Summarizing the results when briefing.
- Illustrating unusual highs and lows.
- Explaining any other anomalies.
- Presenting any unresolved issues.
- Receiving the reactions and expressed priorities of the decision makers, who now begin to decide what is important.

## H.7 Customer Priorities

Analysis of threats to the customer’s information management must be presented to decision makers in a way that gives them the opportunity to know and accept or modify the results. The analysis results in coarse metrics that reflect the level of concern about attacks on each kind of information managed. The results desired from the briefings are to discover any changes in priorities and to achieve consensus.

The PNE practitioner achieves the desired consensus by—

- Presenting the threat analysis.
- Obtaining the customer’s view.
- Managing reactions.
- Setting priorities

### H.7.1 Presenting the Threat Analysis

Threat analysis results are typically presented to decision makers. Because the presentation is critical to the acceptance of the recommended method, the PNE practitioner



iatf\_h\_8\_0090

should—

- Present a coordinated result. The whole ISSE team and the decision makers' staffs should have had input.
- Present IMM and threats with minimal detail. The presentation should focus on the highest level of concerns and summarize the findings.
- Explain how to interpret any tables used.
- Increase depth as necessary. The full report should be available for any customer who desires to review it. The presentation should be structured so that backup material with finer detail and samples of the information are available.
- Present issues and recommendations. Any unsolvable issues that surfaced in working with operations or systems personnel should be presented to the decision makers for their judgment.

## H.7.2 Obtaining the Customer's View

The customer will want to know what the PNE team found to be the most important problems and will expect that the PNE team will have documented lesser problems as well. The threat matrix shown in the threat analysis section, if used, will rank the information threat for each domain as a 3, 2, 1, or 0. Present all the 3s and 2s and be prepared to at least categorize the 1s and 0s. Record customer reactions to each problem, and note whether the customer agreed or disagreed.

## H.7.3 Managing Reactions

Feedback on the threat analysis needs careful management. The ISSE team should assure the customer that the results will be amended to reflect their decisions. The ISSE team should—

- Advise and be open to the customer's views. The ISSE team advises and guides the customer, the customer's opinion is paramount. Minority opinions should be reported but not acted on unless the customer so directs.
- Be prepared for disagreements. If decision makers disagree with the results, they should be informed that the results reflect the findings of the customer's staff as well as the information systems security team. When there is disagreement, be ready to accept less than the information systems security team's judgment. Make a record of the disagreement.
- Remind the customers that the results will reflect their decisions. Inform the customer that changes will be made to reflect the decision maker reactions to the briefing.

## H.7.4 Setting Priorities

The goal of PNE is to capture the customer's priorities. The ISSE team should—

- Use the results of initial analysis. Make sure that the customer is aware of the documentation of the results.
- Amplify reasoning. Be ready to supply a rationale for the results from the threat analysis. Case histories are especially helpful.
- Encourage discussion. The highest priority items will probably receive the most reaction. Encourage the decision makers.

## H.7.5 Achieving Consensus

Full consensus may not be possible at the initial threat analysis presentation. The ISSE team should—

- Document the results and circulate them as often as necessary for review and comment at the highest levels of operation and decision making.
- Use meetings, if possible, to discuss and report progress.

## H.8 Preparing the IPP

The Information Protection Policy is the authoritative requirements document for the development and security life cycle of an information protection solution, whether it is called an IPP or some other name. What matters is that it contain the information necessary to help the security architect to satisfy protection needs. In preparing the IPP, the PNE practitioner should—

- Explain the Purpose and Type of IPP. “Policy” has many definitions.
- Identify existing policies, regulations, and procedures. In preparing the IPP, the PNE practitioner must be aware of all documents that pertain to security policy. The IPP should not conflict with, and indeed might be governed by, existing policy. Other security administrative needs can also be accomplished by including them in the IPP.
- Establish roles and responsibilities. The IPP can define how it should be revised and maintained and by whom.



iatf\_h\_8\_0090

- Identify decision makers. The signatures on the IPP identify which authorities or decision makers support the policies. The IPP can prescribe an administrative structure for assuring proper implementation.
- Define C&A procedures. The IPP can be the source for administering C&A procedures.
- Identify Security Service Requirements. The major purpose of the IPP is to document the security services required to counter identified threats to information.
- Document results.

## H.8.1 Explain the IPP Purpose and Type of IPP<sup>2</sup>

Security policies have a wide range of definitions and purposes. The purposes range from compliance with international treaties, to prescribed computer user behavior, to rules for a reference monitor in a trusted computer. Stating the purpose of a policy in the document is the only way to distinguish it from other policies.

Policy should not define how something is to be accomplished. Policy should document only what is to be accomplished—the requirements. The purpose of the IPP is to document the security services required to counter identified threats to information. Other potential sources of protection requirements, a mix of “what is required” and “how to do” types of documents—, are—

- International agreements and treaties.
- Government laws, statutes, and directives.
- Organizational directives.
- Operational agreements.
- IT system controls and procedures.
- Workstation controls.
- Doctrine.

Doctrine is often considered policy but is really part of the architecture and implementation. Doctrine includes all of the procedures, personnel administration, physical security specifications, and so forth needed to support the hardware and software design. Auditing, for example, is a doctrinal procedure used to detect compromises or violations of policy.

## H.8.2 Identify Existing Policies, Regulations, and Procedures

The PNE practitioner should—

---

<sup>2</sup> Section 1.1 in Annex B and Section 1.1 in Annex C are examples.

- Budget research time while building customer relations and before writing the IPP. In the IT business, most security policies are a mix of procedures, guidance, rules, and design specifications. Read and understand the structure and content of existing policy.
- Analyze procedures, guidance, and rules to discover the underlying policies. Procedures do have underlying policy. For example, the statement, “must use six-character passwords for login,” implements a requirement for a minimum-to-moderate strength I&A service.
- Retain and transfer any solutions to be used as possible design constraints. Solutions also have underlying policy. When a mechanism is identified in the existing documentation, record the fact for later analysis by the systems designer.

### **H.8.3 Establish Roles and Responsibilities<sup>3</sup>**

To ensure that the IPP is properly maintained, the PNE practitioner should—

- Identify existing security functions and resources and establish relationships. Organizations most likely have information or property protection rules in place, for example, assigned resources and organizational responsibilities for nightly lockup, paper file separations, financial auditing, or other safety requirements. The information management solution must coexist with these existing security measures. The information management solution may, in fact, be intended to augment or replace existing measures. Discover them and establish working relationships with those responsible for them.
- Identify resources for policy changes and enforcement. The IPP is useful as a vehicle for identifying its own maintenance and enforcement structure. A policy administrator will need to coordinate changes and manage the enforcement resources.
- Identify security evaluators, certifiers, and accreditors, and their responsibilities. An important issue for decision makers is choosing who will evaluate and certify that the solution provides adequate protection, and who will accredit any system as operationally acceptable.
- Suggest a security administration staff and define staff responsibilities. The IPP can be used to define a complete administrative staff for life-cycle support of itself and the IPP consistent with customer functions. Implementing the security management can be delayed until the system is designed, but the merit of placing it in the IPP is that resources can be authorized to help define the system. Typical staff roles are—
  - Chief Security Officer (CSO).
  - Office/unit/area security officers.
  - Network security administrators.
  - Security domain administrators.
  - Information domain administrators.

---

<sup>3</sup> Section 2.3 in Annexes B and C are examples.

## H.8.4 Identify Decision Makers

Identify decision makers, involve them and their staff members in the PNE process, and have them review the PNE at critical points. The IPP is the final documentation of the PNE. It must incorporate the results of the decision makers' previous decisions. Because the signatures on the IPP should be those of the authoritative decision makers, they must have the final review before signing. Typically, in a corporate structure, the CEO, CIO, COO, and CSO are the decision makers; in the DoD, the DAA is the decision maker.

## H.8.5 Define C&A Procedures<sup>4</sup>

Ultimately, someone must decide whether to accept and allow the use of new or modified information systems. The decision will be based partly on a determination that the solution adequately meets the information protection requirements stated in the IPP. The IPP can serve as the vehicle to force the decisions about who is the accreditor, the evaluator, and the certifier and to obtain their agreement to perform those roles. Many programs have been delayed or cancelled because these decisions were not made early enough, or at all. It is a good idea to recognize any specific certification & accreditation (C&A) process that is useful or organizationally dictated (e.g., DITSCAP). Documentation of procedures and decisions may be in the IPP itself or be included by reference.

## H.8.6 Identify Security Service Requirements<sup>5</sup>

There are some confusing overlaps between mechanisms that provide security services and the security services themselves. It may be helpful to consider a security service as a 'category of security mechanisms'. Security services include:

- Access control (in storage).
- Confidentiality (in transit).
- Integrity (in transit).
- Availability (of information and service).
- Nonrepudiation (proof of origin and delivery).
- Identification and authentication.
- Security management.

A mechanism for one security service may contribute to another security service. An access control mechanism can provide confidentiality and integrity services. Confidentiality mechanisms can provide access control and integrity services. One recommendation is to consider the access control mechanism as the security service for protecting information in storage, and confidentiality and integrity mechanisms as the security services for information in

---

<sup>4</sup> Section 2.4 in Annex B and Section 2.5 in Annex C are examples.

<sup>5</sup> Section 2.6 in Annex B and Section 3 in Annex C are examples.

UNCLASSIFIED

transit. Of course, I&A mechanisms support the other security services. Security management is considered a security service.

The main activity of the PNE is to identify specific information protection requirements in terms of—

- Each information domain.
- Each security service needed.
- The strength of each needed security service compared to each type of harm (copied from the Threat Analysis section)—
  - Disclosure, or loss of confidentiality.
  - Modification, or loss of integrity.
  - Nonavailability, or loss of access or service.
  - Repudiation, or loss of authenticity—
    - Denial of receipt of information.
    - Denial of sending information.

Table H-12 lists each of four types of harm with an information threat (rated as 0, 1, 2, or 3) specified for the strategic planning information domain.

**Table H-12. Information Threat Table**

**Information Domain: Strategic Planning**

Disclosure	Loss/Modification	Denial of Service	Repudiation
3	3	1	0

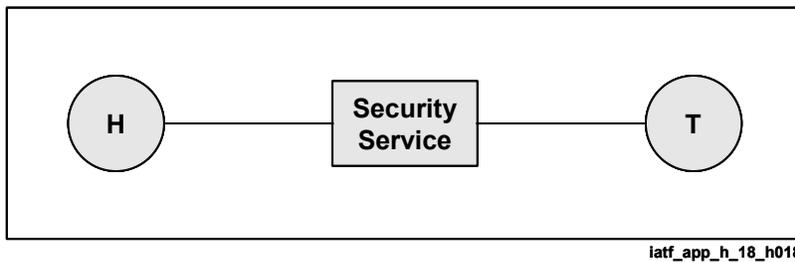
The activity is to assign a security-service strength combination to each type of harm, in which the scale for strength of the security service is none, minimum, moderate, or strong. The practitioner should use a metric scale that the customer is comfortable with. Table H-13 lists four types of quantitative data, or metrics, with measurement scales.

**Table H-13. Information Threat Data**

Quantitative Data	Scale
Harm To Information (HTI)—impact	None, Mild, Significant, Serious
Potentially Harmful Event (PHE)—a probability	None, Low, Medium, High
Information Threat—combining HTI and PHE	0, 1, 2, 3 (3 denotes highest information threat)
Strength of Security Service	None, Minimum, Moderate, Strong

In this appendix we assign a security-service strength to a type of harm using the look-up tables in Figure H-18 and Table H-14:

Type of Harm	Security Service	Target <sup>6</sup>
Unauthorized access	Access control	Any data or system component
Disclosure	Confidentiality	Any data or process
Modification/damage	Integrity	Any data, process, or component
Denial of service/use	Availability	Any data, process, or component
Spoofing/Denial	Non-repudiation	Proof of origin or delivery of data
False authorization <sup>7</sup>	Authentication	Authentication data or decision
Unauthorized control	Security management	Security management data



iatf\_app\_h\_18\_h018

**Figure H-18. Map Type of Harm to Security Service**

**Table H-14. Map ‘Information Threat’ to ‘Strength’**

Information Threat	Strength of Security Service
0	None
1	Minimum
2	Moderate
3	Strong

For each information domain and for each type of harm, map the information threat to a security service strength.

Note two assumptions in this approach—

- Within an information domain, the strength of the security service needed to protect against a type of harm is proportional to the information threat to that type of harm.
- The strength of I&A and security management security services must be commensurate with the strongest of the other security services in the information domain.

Table H-15 contains the results for strategic planning.

<sup>6</sup> The Target column is provided for reference only.

<sup>7</sup> The False authorization and Unauthorized control rows are provided for reference only.

**Table H-15. Data for Information Protection Requirements**

Information Domain Strategic Planning	Disclosure	Loss/ Modification	Denial of Service	Repudiation
Information Threat	3	3	1	0
Security Service	Confidentiality	Integrity	Availability	Nonrepudiation
Strength	Strong	Strong	Minimum	None

The two special requirements for the example are that—

- All system components and data require a strong level of I&A protection.
- All security-management data require a strong level of security management protection.

## H.8.7 Document Results

The final product of PNE is an IPP, in whatever documented form, that defines—

- Information management.
- Threats to information management.
- Security services priorities.
- Authoritative direction.

The well-prepared IPP provides a wealth of information for design and for C&A, but it is a living document that must be periodically reviewed and updated.

## H.9 Customer Buy-In

The final step in the PNE process is achieving the customer’s agreement to maintain and enforce the IPP and to provide the resources and agents needed for its execution. Customer support of this agreement is crucial for—

- Defining a solution consistent with the IPP.
- Developing a system consistent with the system security requirements as allocated from the IPP and the security architectures.

To obtain buy-in, the PNE practitioner must—

- Explain ownership (again). The final product, the IPP, is an internal document owned by the customer. Make sure that the customer understands that the IPP is the customer’s policy, not the PNE practitioner’s policy.



iatf\_h\_8\_0090

- Explain the need for high-level endorsement. Management and leadership must be the driving force. An IPP that is not supported by management is a total waste of effort.
- Explain the need for maintenance. The IPP must be reviewed periodically because it must change as changes occur in the mission, the business, or the system.
- Explain the need for necessary resources. The customer must identify and apply resources to maintain the IPP effectively.

## **H.9.1 Explain Ownership (Again)**

If the correct procedures have been followed, the PNE practitioner should already have buy-in, with the customer participating by—

- Contributing information.
- Reviewing and commenting on documents.
- Making decisions that resolve issues.

The IPP, therefore, documents the customer's desires and decisions.

## **H.9.2 Explain the Need for High-Level Endorsement**

The customer must understand that the IPP represents the rules not according to the information systems security engineer but according to the customer. Without the power of the decision makers behind the IPP, no protection program exists. The decision makers' signatures are evidence of coordinated approval.

## **H.9.3 Explain the Need for Maintenance**

Changes will occur. The IPP should be self-sustaining by its own content. Therefore, the signed IPP should identify and approve the procedures necessary to keep it active and current.

## **H.9.4 Explain the Need for Necessary Resources**

The IPP should also be self-sustaining in terms of its resources. Therefore, the signed IPP should identify and approve the resources necessary to support the customer's mission.

## **H.10 Summary**

PNE provides a detailed description of the first and perhaps the most important activity of ISSE. It engages customers to become the source and the advocates for protecting their own information. The seven procedures from Approaching the Customer to Customer Buy-in provide a solid foundation for the next ISSE activity—Define System Requirements—where the systems context, concept, and requirements are defined.

# PNE Glossary and Acronym List

C&A	Certification and Accreditation
CEO	Chief Executive Officer
CIO	Chief Information Officer
COO	Chief Operating Officer
CSO	Chief Security Officer
DAA	Designating Approval Authority. One of the signatories of the System Security Authorization Agreement in the Department of Defense certification and accreditation process.
DGSA	Department of Defense Goal Security Architecture
DITSCAP	Department of Defense Information Technology Security Certification and Accreditation Process.
DoD	Department of Defense
HTI	Harm to Information
IA	Information Assurance
I&A	Identification and Authentication
IAS	Information Assurance Solutions. An NSA (security) process for finding security solutions.
IATF	Information Assurance Technical Framework
IDEF	Integrated DEFinition
IMM	Information Management Model. The IMM represents everything that an information system should accomplish. The IMM can be used to check consistency and to evaluate the actual system. A comprehensive developed IMM is the starting point for information protection, but very often the PNE practitioner must develop the IMM, which defines “who does what with which information objects.”

## UNCLASSIFIED

Appendix H  
IATF Release 3.1—September 2002

INFOSEC	Information Systems Security. This acronym also breaks out to “Information Security” and means classification management within that community, although not in this document.
IPOC	Initial Point of Contact
IPP	Information Protection Policy. The PNE practitioner produces the IPP (a form of security policy) as the final result of PNE. The IPP represents the latest requirements and decisions of the customer concerning information protection. It belongs to the customer, not to the PNE practitioner.
IS	Information Systems
ISSE	Information Security Systems Engineering. The primary skill needed in PNE is systems engineering with a specialty in information security.
IT	Information Technology
ITSEC	Information Technology Security
ITT	Information Threat Table
ND186	Network Defend 186. A National Cryptologic School course.
NSA	National Security Agency
PHE	Potentially Harmful Events
PNE	Protection Needs Elicitation
PP	Protection Profile. Part of the Common Criteria language.
R&D	Research and Development
SE	System Engineering
SSAA	System Security Authorization Agreement. The document capturing a system’s certification details and accreditation status in DITSCAP.
TOE	Target of Evaluation. Part of the Common Criteria language.

# References

[DGSA] DoD Goal Security Architecture, Version 1.0 ,Defense Information Systems Agency, October 1993.

[IDEF] IDEF modeling, <[www.edef.com](http://www.edef.com)>.

[Taylor] Taylor, David A. Business Engineering with Object Technology, John Wiley and Sons, 1995.

[Yourdan] Yourdan, Edward. Modern Structured Analysis Yourdan Press, 1989.

**UNCLASSIFIED**

Appendix H  
IATF Release 3.1—September 2002

**This page intentionally left blank**

# **PNE Annex A: IMM Example**

---

[This annex to this document is an unedited (except for company name) example of an actual IMM.]

**XYZ Corporation**

**Business Forms Division**

## **INFORMATION MANAGEMENT MODEL**

*A composite understanding of XYZ, Business Forms Division's information, and information management, with threats analyzed and information domains determined.*

**UNCLASSIFIED**

Appendix H, Annex A  
IATF Release 3.1—September 2002

**This page intentionally left blank**

# Executive Summary

## XYZ Business Forms Division

### Information Management Model (IMM)

The XYZ Corporation Information Protection Policy (IPP) (draft: dated ..... ) provides the policy on information protection and provides guidance for the preparation of policies by divisions of the corporation. This Information Management Model (IMM) has been prepared in accordance with the procedures defined in the XYZ IPP for the XYZ Business Forms Division (BFD). It is a source document for XYZ BFD's Information Protection Policy (IPP).

This document, XYZ BFD's IMM, is the result of—

- 1) Modeling the division's information management functions.
- 2) Considering corporate policy.
- 3) Analyzing more specific threats.
- 4) Revising the model to meet existing policy and to partially counter any specific threats.

The IMM is a logical description of information management which depicts the users, processes, information, and information flows which support the business. The threat analysis from the examination of the IMM by information category of its potential for harm, the impact of harm to business, and the selection of needed security services. The XYZ IPP had defined relevant threats, impacts, and security services applicable to all XYZ divisions. The information categories of the IMM were reorganized into information domains (refer to definitions) wherein security services were applied to the users, processes, and information categories. Each information domain contains an element of policy. The IMM was used as the basis for the XYZ BFD Information Protection Policy (IPP). That IPP is the composite of the defined information domain protection policies and forms the basis for subsequent security architecture recommendations.

The development of this IMM resulted in the formation of 47 information domains. This included 44 user types/roles 48 types of processes, and 124 information categories. The choices made for XYZ BFD were influenced heavily by the following set of priorities:

- customer service.
- protection of customer information.
- protection of XYZ's proprietary information.
- protection of XYZ's financial information.
- separation of customer accounts information.

With a few exceptions, the threat of disclosure is not significant to XYZ BFD. The threat of unauthorized modification is significant. Most domains were formed with this threat being the most prominent from both a potential harm and impact perspective. The denial of

service/availability threat is relevant to various XYZ BFD processes and information, but only has a serious impact upon the customer ordering. The authentication of users is essential in supporting all security services.

## 1.0 Introduction

Before any information systems engineering process begins an Information Management Model (IMM) must exist or be developed. The IMM provides the basis for all future analysis and is necessary to understand the information systems requirements. This IMM provides an understanding of XYZ's information; what information is managed, who manages it, what processes utilize and modify it, and what transfers occur.

IMMs are developed in one of two contexts: the as-is or the to-be. In the as-is, the IMM is derived from existing systems and applications and correlated with business functions as they are currently organized and implemented. This is useful in documenting the as-built system's IMM. In the to-be, the IMM is derived from re-engineered or new business processes and business flow. Information description, structure, categorization, flow, and management controls are derived from the newly engineered, or existing re-engineered business functions. The to-be IMM is the target IMM.

This document presents the target IMM for XYZ's XYZ Business Forms (XYZ BF) and Systems Division (SD). The focus is on the XYZ BFD re-engineered business processes. However, both the as-is and the to-be have been used, because the target IMM is a composite of old and new XYZ BFD processes and information.

This IMM documents the information in terms of users-processes-information and information flow. Using the XYZ Corporation Information Protection Policy a threat analysis is performed upon the IMM resulting in a revised IMM with information domains. An information domain is a set of unique users-processes-information, where the privileges associated with any user on any information object in that domain are the same for all information objects. Information domain security policies and a composite security policy are presented in the XYZ BFD's Information Protection Policy.

## 1.1 Background

XYZ's XYZ BFD is re-engineering its core business areas for improved performance and reduced cost. This re-engineering will result in new information, revised business processes, and new information technologies with distributed computing.

This document is one in a series of documents that XYZ's XYZ BFD will receive under the management consulting arrangement with our firm. This document has been developed under a consulting engagement task entitled XYZ Security Policies and Standards.

The XYZ Security Policy and Standards consulting task will develop and deliver:

- The XYZ Corporation Information Protection Policy;
- XYZ BFD's Information Management Model;
- XYZ BFD's Information Protection Policy;
- System Security Architecture recommendations for the XYZ BFD division.

The XYZ Corporation Information Protection Policy provides the guidelines for information protection services for all of XYZ's divisions. The XYZ BFD's specific information protection documents follow these guidelines. XYZ BFD's information protection standards documentation is a useful model for other XYZ divisions.

## 1.2 IMM Development Approach

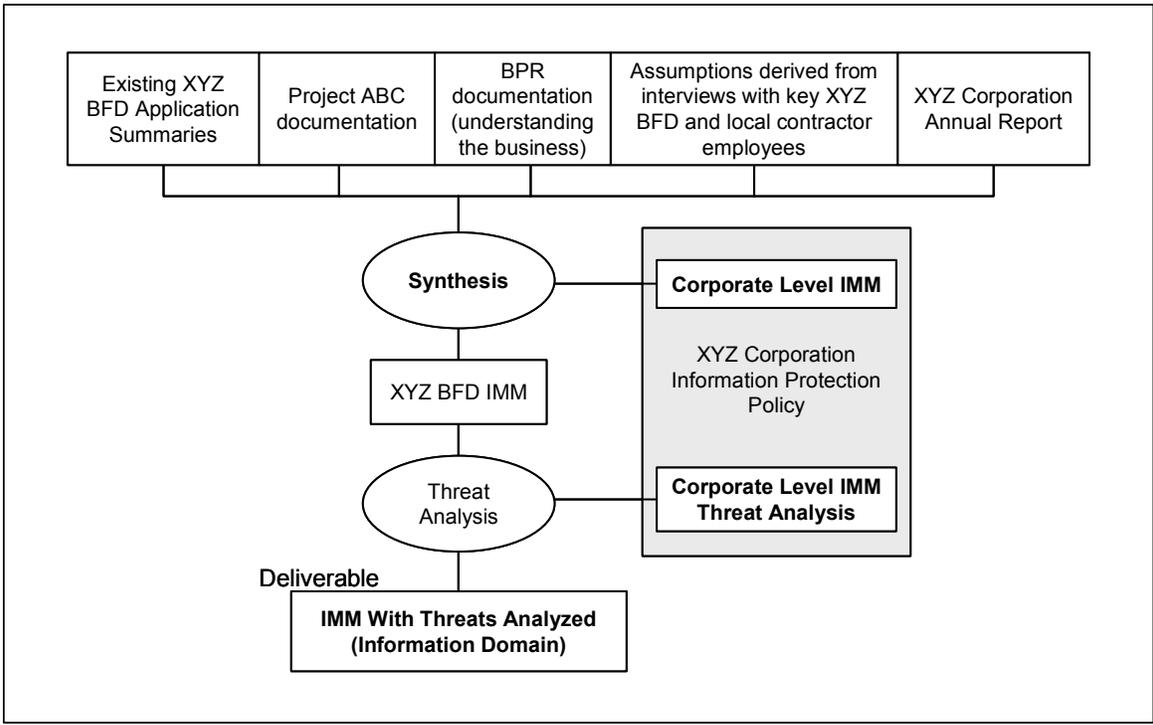
The IMM is developed by decomposing users-processes-information, and logical information flows to where the set of users and their roles are uniquely different. Using the XYZ Corporation Information Protection Policy a threat analysis performed upon this set *users-processes-information* resulting in a revised IMM with information domains. This document will form the basis of the XYZ BFD's Information Protection Policy.

## 1.3 Sources Of Information About XYZ BFD IMM

The sources of information for developing the IMM came from existing documentation and from interviews with XYZ employees and XYZ-local Data Center contractor employees. Documentation includes summary information of existing applications, project ABC report, the XYZ Corporation Annual Report, and XYZ Business Process Re-engineering project (understanding the business). Figure 1.3.1 highlights the IMM development approach and information.

## 2.0 XYZ BFD IMM Decomposition

XYZ BFD top level information management model is illustrated in Table 2.0.1. The top level processes include both core business processes and infrastructure (or resource management) processes which support the core business processes.



latf\_ann\_a\_001

**Figure 1.3.1. IMM Information Sources & Development Approach**

The XYZ BFD core business processes include:

- Customer Ordering
- Information Inquiry
- Manufacturing
- Warehousing

The XYZ BFD infrastructure processes include:

- Business Planning
- Marketing
- Finance and Accounting
- Personnel Management
- Information Systems and Communications Management
- Facilities Management
- Corporate Relations
- Security Management

**Table 2.0.1. Top Level XYZ BFD IMM**

<b>USERS</b>	<b>PROCESS</b>	<b>INFORMATION</b>
Customers, XYZ Employees	Customer Ordering	Customer Profile and order entry/order process info
Potential Customers, Customers, XYZ Employees	Inquiry	General catalog, customer profile, oe/op info
XYZ Employees, Suppliers, Customers	Manufacturing	Manufacturing Process Management Info Customer New Forms Design Info
XYZ Employees, Customers	Warehousing	Shipping, Receiving, and Inventory Control Info
XYZ BFD Executives & Staff	Business Planning	Planning Info
Sales/Marketing Staff & Executives	Marketing	Marketing Info and General Catalog Updates
Finance/Accounting Staff & Certain Executives	Finance & Accounting	AR/AP/GL Info
Personnel Staff	Personnel Management	Personnel Files, Policies & Procedures, Payroll Info
IS/Comm Management & Operations Staff	Is/Comm Management	IS/Comm Planning, System & Network Management, and Ops Info
Office Managers Admin Staff	Facilities Management	Office Supplies Accounting Facilities Maintenance. Monitoring Info
XYZ BFD and Corp. Executives	Corporate Relations	Reporting Information
XYZ BFD Security Managers/Administrators	Security Management	Security Management Information

The XYZ BFD IMM decomposition begins from this level of abstraction, preceding downward until the logical groupings no longer have any unique user and user role variations. For this reason, some process classes and information categories must be decomposed to a finer resolution than others. For example, both the business planning and corporate relations infrastructure processes, users, and information end at level 1. There is no refinement necessary beyond level 1 because there are no clarification of the users and user roles at a finer granularity than level 1, at least none that we uncovered during our analysis of these two XYZ BFD processes.

## 2.1 Customer Ordering Process Decomposition

The order process described is based on the XYZ BPR project “Understanding the Business” Document, because it is the most current description of the future. The level 2 decomposition is summarized in Table 2.1.1. The level 3 decomposition is summarized in Table 2.1.2.

**Table 2.1.1. Customer Ordering Process Level 2 Decomposition**

USERS	PROCESS	INFORMATION
Potential Customers, Customers, Sales Reps, Sales Center Reps	Identification	Customer Profile
Potential Customers, Customers, Sales Reps, Sales Center Reps	Profile Management	Customer Profile
Potential Customers, customers, sales reps, sales center reps, xyz manufacturing, warehouse, and finance employees	Order Entry Order Processing	Customer Profile, New Forms Design, POs/Releases, Read- only Price Quotes
Potential Customers, Customers, Sales Reps, Sales Center Reps	Order Adjustment	POs/Releases and Customer Order File
Potential Customers, Customers, Account Managers, Account Representatives	Inquiry Process Link	Customer Profile, New Forms Design, POs/Releases, Order File, Price Quotes

The identification process identifies the customer by name, account number, or phone number. The information is contained in the customer profile. If the customer is new, they will be deferred to the profile management process to develop a new customer profile. Input to the identification process comes from interactive customers or EDI transactions. EDI transaction input is for existing customers only, and must include adequate identification information and order process request information to process the EDI transaction. Existing customers, after identification, are prompted for the particular ordering process sub-process they wish to use, if

the user is interactively connected to the identification process. This is described in the XYZ Direct ordering process. The identification process does not have a level 3 decomposition.

**Table 2.1.2. Order Entry and Order Process Level 3 Decomposition**

USERS	PROCESS	INFORMATION
Customer, Sales Rep, Sales Center Rep, Manufacturing Forms Designer	New Forms Design	Customer catalog, general catalog, new forms image
Sales Rep, sale center rep, no users	Price Quote	Price ranges file, freight/shipping price file, customer concessions info and po (complete or partial)
Customer, sales rep, sales center rep	Activate Order or Release	Trigger/Status Info and Orders File

The profile management process allows a new customer to build a customer profile, and allows an existing customer to modify information in the customer profile. The content of the customer profile information is defined in XYZ Direct documentation. Some of the information in the customer account is controlled by the customer, other information may be read but not modified by the customer, and other information (i.e., credit approval/disapproval information) may not be viewed by the customer, but is necessary to activate an order.

The order entry and order processing processes allow the user to order XYZ BFD products, design new forms products, get price quotes prior to activating an order, set an automatic reorder cycle, and release inventory stored in a warehouse to be shipped to the customer. The customer interface to this process is by way of the Triage concept, or via EDI transaction, after passing through the identification process.

The order adjustment process allows the customer to change or cancel an activated purchase order or release instruction. The customer interface to this process is by way of the Triage concept or EDI transaction, after passing through the identification process.

The inquiry process is a level 1 process, with linkage from the customer order process. This link is by way of the Triage concept or via EDI transaction, after passing through the identification process. Users may also engage the inquiry process without entering the ordering process, but are to general inquiries that do not relate to a specific customer account. The inquiry process is detailed in section 2.2.

The level 3 decomposed processes of the order process are all associated with order entry and order processing.

The new forms design sub-process of the order entry and order processing processes allow a customer, customer surrogate, or interactive customer/manufacturing forms designer to develop

new forms. The price quote sub-process provides the user with a quoted price affiliated with a particular order. The activate order/release sub-process allows a trigger to send the order or release to manufacturing or warehousing for completion.

## 2.1.1 Customer Ordering Process Threat Analysis and Information Domains

The customer ordering processes and information have two needs. The first is to verify the identity of users for controlling access. The second is to control accessibility and privileges to certain order processing information for confidentiality and integrity reasons. Three guidelines are used to determine ordering process information domains. The guidelines are as follows.

- With the exception of the identification process, all other sub-processes of the customer ordering process require that the user's identity and/or EDI transaction content origin be authenticated. The other guidelines cannot be enforced without user identification and authentication and/or EDI transaction data origin authentication.
- Keep each customer's information separate from other customers' information to minimize the threats of disclosure to unauthorized users and modification by unauthorized users.
- Identify read and write privileges associated with all customer ordering processes and information to minimize the threats of unauthorized disclosure to the customer representative or unauthorized modification by the customer representative.

From the XYZ Corporation Information Protection Policy:

### Sales

**Threats:** Sales information about non-standard pricing arrangements offered to specific customers, or planning for special sales or agreements is threatened by disclosure (medium) and loss or damage (medium). The impact of disclosure or loss is (mild)

**Security Services:** This sales information requires confidentiality (minimum) and integrity (minimum) in both storage and transfer. Access control (minimum) must limit information entry and disclosure to XYZ sales personnel and information disclosure to only the specific customers involved. I&A (minimum) is required to support the other security services.

### Customers

**Threats:** Information about customers wherein accounts, customer profiles, ordering histories, and customer proprietary information is unique to that customer are threatened by disclosure (medium) and loss or damage (medium). The impact of disclosure of customer proprietary information is (serious) and the disclosure of other customer information is (significant)

**Security Services:** This customer information requires confidentiality (moderate) and integrity (moderate) in both storage and transfer. Access control (moderate) must limit information entry and disclosure to XYZ specific sales personnel and information disclosure to only the specific customers involved. I&A (moderate) is required to support the other security services.

## Orders

**Threats:** Information about orders may contain unique pricing arrangements with (medium) threat of disclosure and (medium) threat of loss or damage. The impact of disclosure is (significant) and of loss or damage is (mild).

**Security Services:** This ordering information requires confidentiality (moderate) and integrity (minimum) in storage and transfer. Access control (moderate) should limit access to specific customers, specific salespersons, specific sales managers, and any financial information users.”

The three extractions relate to the XYZ BFD ordering process. From this analysis, five information domain types are concluded. These five information domain types are summarized in Table 2.1.3.

**Table 2.1.3. Order Process Information Domains**

DOMAIN	USERS	RULES	PROCESS	INFORMATION
ORDER Identification	Anyone		Identification	
ORDER Profile Management [1 per account]	New customer	Write	Profile Management Create profile	Customer profile - Customer's info
	Sales representatives	Auth: read/write		
	Account mangers	Auth: read/write		
	Account representatives	Auth: read/write	Profile management Modify profile	
	Customer	Auth: read/write		
	Sales representatives	Auth: read/write		
	Account mangers	Auth: read/write		
	Account representatives	Auth: read/write		
	Warehouse employees	Auth: read		
	Manufacturing employees	Auth: read		
Finance employees	Auth: read			
ORDER Pricing [1 per account]	Customer rep	Auth: read	Profile Management Price quote	Customer Profile - Pricing info
	Account/sales reps	Auth: read		
	Account mangers	Auth: read		
	Warehouse employees	Auth: read		
	Manufacturing employees	Auth: read		
	Finance employees	Auth: read/write		

**UNCLASSIFIED**

Appendix H, Annex A  
IATF Release 3.1—September 2002

<b>DOMAIN</b>	<b>USERS</b>	<b>RULES</b>	<b>PROCESS</b>	<b>INFORMATION</b>
ORDER Credit Checking [1 per account]	Account mangers	Auth: read	Profile Management - Credit check - Credit approval flag	Customer Profile - Credit info
	Account/sales rep	Auth: read		
	Finance employees	Auth: read/write		
	Finance managers	Auth: read/write		
	Marketing managers	Auth: read		
	Marketing representatives	Auth: read		
	XYZ BF executives	Auth: read		
ORDER Entry and Processing [1 per account]	Customers	Auth: read/write	Order Entry & Order Processing  (Linkage to inquiry)	Customer Profile orders releases new forms
	Account/sales rep	Auth: read/write		
	Account manager	Auth: read		
	Warehouse employees	Auth: read		
	Manufacturing employees	Auth: read		
	Finance manager	Auth: read		
	Finance employees	Auth: read		

## 2.2 Inquiry Process Decomposition

The inquiry process allows XYZ’s existing and potential customers and XYZ’s employees to gather information on XYZ’s products and services, inventories, and the status of existing orders. This information can be accessed through the XYZ Direct Triage, via EDI, direct connections, or through XYZ’s internal IS. The users and information associated with this process are shown in Table 2.2.1 which expands upon the Inquiry information shown in Table 2.0.1.

**Table 2.2.1. Inquiry Process Top-Level Decomposition**

<b>USERS</b>	<b>PROCESS</b>	<b>INFORMATION</b>
Potential Customers	Inquiry	Offering (Catalog)
Customers		Order Status
XYZ Employees		Quotes
		Inventory
		Financial
		Customer Profile

The information in Table 2.2.1 is further decomposed into groups of processes with common sets of users and data. This decomposition is shown in Table 2.2.2.

**Table 2.2.2. Inquiry Process Level 2 Decomposition**

USERS	PROCESS	INFORMATION
Potential Customers	Offering inquiry	Offering (catalog)
Customers	Request for quote	Order status
XYZ Sales reps	Inventory inquiry	Quotes
XYZ Account Manager		Inventory
XYZ Account Exec.		
XYZ Financial Employees		
XYZ Marketing Employees		
Customers	Order Status Inquiry	Order status
XYZ Sales reps		Customer profile
XYZ Account manager		
XYZ Account exec.		
XYZ Sales reps	Financial Requests	Payment history
XYZ Account manager		Customer profile
XYZ Account exec.		
XYZ Financial employee		

From the XYZ Corporation Information Protection Policy:

## Marketing

**Threats:** Marketing information wherein sales people promote products and service to customers and potential customers, assess markets, quote standard pricing, and acquire information about the competition is threatened (medium) by the possibility of information being lost or damaged. The impact of such loss is considered (mild) requiring an investment in the rebuilding of the information.

**Security Services:** Marketing information shall be protected for data integrity (minimum). Confidentiality is not required. Access controls (minimum) must limit information entry to XYZ personnel with some exceptions for customer inquiry records.

## Customers

**Threats:** Information about customers wherein accounts, customer profiles, ordering histories, and customer proprietary information is unique to that customer and threatened by disclosure (medium) and loss or damage (medium). The impact of disclosure of customer proprietary information is (serious) and the disclosure of other customer information is (significant)

**UNCLASSIFIED**

Appendix H, Annex A  
IATF Release 3.1—September 2002

**Security Services:** This customer information requires confidentiality (moderate) and integrity (moderate) in both storage and transfer. Access control (moderate) must limit information entry and disclosure to XYZ specific sales personnel and information disclosure to only the specific customers involved. I&A (moderate) is required to support the other security services.

**Orders**

**Threats:** Information about orders may contain unique pricing arrangements with (medium) threat of disclosure and (medium) threat of loss or damage. The impact of disclosure is (significant) and of loss or damage is (mild)

**Security Services:** This ordering information requires confidentiality (moderate) and integrity (minimum) in storage and transfer. Access control (moderate) should limit access to specific customers, specific salespersons, specific sales managers, and any financial information users.

**Warehousing/Distribution/Transport**

**Threats:** Information about inventories of products, shipping schedules, carriers, transfers and disposals is threatened by loss or damage (low) but has (significant) impact on service to customers.

**Security Services:** This information is in access (moderate) to authenticated (minimum) customers, and XYZ employees. Integrity (moderate) in storage and transfer and confidentiality (minimum) in transfer is required.

Analyzing Table 2.2.2 with the above threats applied shows that the information in the level two decomposition must be further decomposed to provide separation of general inventory information from customer-specific inventory information. The result of that decomposition is shown in Table 2.2.3.

**Table 2.2.3. Inquiry Process Level 3 Decomposition**

<b>USERS</b>	<b>PROCESS</b>	<b>INFORMATION</b>
Potential customers	Offering inquiry	General XYZ inventory
Customers	Request for quote	Catalog
XYZ Sales reps	Inventory Inquiry	
XYZ Account manager		
XYZ Account exec.		
XYZ Financial employees		
XYZ Marketing employees		
Customers	Inventory inquiry	Customer-specific inventory
XYZ Sales reps	Request for quote	
XYZ Account manager		
XYZ Account exec.		

## 2.2.1 Inquiry Process Threat Analysis and Information Domains

The decomposition of the inquiry process results in four sets of user-processes-data. These sets must to be examined for threats as described in Section 2.6 of the XYZ Corporation Information Protection Policy. These threats may not represent all of the threats to the XYZ BFD Division; therefore, the four sets must also be examined for other potential threats. Also, the XYZ Corporation Information Protection Policy provides for the minimum set of probabilities of attack, degrees of impact, and security strength ratings, which in some cases may be higher for the XYZ BFD Division. A general determination is that all customer-specific information must be in separate information domains.

The first domain is order status & inventory. The information in this domain is associated with inquiries into the status of a customer's order. Part of that inquiry process interacts with the customer's profile to get information necessary to display the order status. The XYZ Corporate Policy states that the threat to the disclosure and/or loss of customer information, including ordering information, is medium and the impact of disclosure of a customer's information is serious. The policy also states that access to customer information must be to that customer and to specific XYZ sales personnel who are associated with that customer. Also, as this is an inquiry process, all users are to only reading the information and therefore cannot alter or damage the information. Table 2.2.4 shows this information domain.

The second domain is Financial Requests. This domain is associated with financial inquiries into payment history and the customer profile. The XYZ Corporate Policy shows that the disclosure of customer information is considered serious. Further, the policy states that access to financial information must be even within XYZ. The users associated with this domain are XYZ personnel. In addition, those with the ability to write or generate this information must be restricted. The privileges reflect this restriction. This domain is shown in Table 2.2.4.

The third domain is Inventory and Quotes. This domain is associated with inquiries into catalogs and requests for standard quotes. The information in this set is restricted to XYZ. The XYZ Corporate Policy expresses the concern with the loss, damage, and integrity of this information. The policy further requires that entry of this information be restricted to XYZ personnel only. XYZ's marketing personnel are the only users who can write into this information domain; all others have read-only privileges which meets this requirement. The information domain is shown in Table 2.2.4.

**Table 2.2.4. Inquiry Process Information Domains**

DOMAIN	USERS	RULES	PROCESS	INFORMATION
INQUIRY Order Status & Inventory (1 per order)	Customers (specific)	auth: read	Order Status Inquiry	Order-Specific
	Account Rep (specific)	auth: read	Inventory Inquiry	Customer Inventory
	Account Manager (specific)	auth: read		
	Account Exec.	auth: read		
INQUIRY Financial Requests	Account Reps (specific)	auth: read	Financial Requests	Payment History
	Account Manager. (spec)	auth: read		Customer Profile
	Account Exec. (specific)	auth: read		
INQUIRY Inventory & Quotes	Potential Customers (any)	read	Inventory Inquiry	General XYZ Inventory
	Customers (any)	read	Request for Quote	Quote
	Account Reps (any)	read		Catalog
	Account Manager (any)	read		
	Account Exec. (any)	read		

## 2.3 Manufacturing Process Decomposition

The manufacturing process from Table 2.0.1 is decomposed into forms design, production control, operations management, engineering, and distribution as shown in Table 2.3.1. There are three major aspects of manufacturing supported by information management; the customer's view of the status of his orders, the management's view of business performance, and the management of production.

**Table 2.3.1. Manufacturing Process Level 2 Decomposition**

<b>USERS</b>	<b>PROCESS</b>	<b>INFORMATION</b>
Customers Sales representatives Sales managers Managers Design engineers	Forms Design	Forms catalog, new forms customer orders
Customers Sales representatives Sales managers Operations staff	Operations	Customer orders schedules business plans manufacturing plans product inventories
Managers Production control staff	Production Control	Customer orders, Schedules Providers
Managers Suppliers	Raw materials management	Material inventories, Material orders, Suppliers invoices
Managers Maintenance staff	Engineering	Equipment data, Engineering notes Maintenance schedules
Customers Sales representatives Sales managers Managers	Distribution	Schedules, carriers, Invoices, inventories, Warehousing data

## 2.3.1 Manufacturing Process Threat Analysis and Information Domains

From the XYZ Corporation Information Protection Policy:

### Manufacturing/Vendors/Supplies

**Threats:** Information about products, inventories, requisitions, vendor and supplier contracts, production schedules, is threatened by disclosure (low) and loss or damage (medium). The impact of disclosure is (mild) and of loss or damage is (significant).

## UNCLASSIFIED

Appendix H, Annex A  
IATF Release 3.1—September 2002

**Security Services:** This information is in access (moderate) to authenticated customers (minimum) and XYZ employees. Confidentiality in transfer (minimum), and integrity in storage (moderate) is required.

Although a third level decomposition of the manufacturing process would be useful for information management modeling, the analysis for information protection purposes resulted in satisfactory definition at the second level. The results are shown in Table 2.3.2.

The manufacturing-catalog items information domain addresses the need for inquiry into the manufacturing status of catalog items by nearly anyone and allows for information update and monitoring by operations and production control personnel.

The manufacturing-customer orders information domains are established to provide the inquiry by customer order of any needed manufacturing response and permits the update and monitoring of that status information by manufacturing personnel.

The manufacturing-raw materials domain is information of concern only to manufacturing personnel with the exception of financial accounting which is dealt with in that process.

The manufacturing-distribution domain records information about carriers and warehouses. The actual shipping and invoicing are accomplished under manufacturing-catalog items and manufacturing-customer orders updates.

Manufacturing-design supplements the forms design activities which can be accomplished under the customer ordering process. Completed designs are placed in the catalog.

The manufacturing-operations information domain is used to prepare the manufacturing planning and reporting to XYZ BFD management in association with business planning. Manufacturing operations personnel have many responsibilities in the other manufacturing information domains.

The manufacturing-production control information domain controls the internal scheduling of personnel and equipment for production, including maintenance of equipment. Production control also acquires the services of external manufacturing and service providers herein referred to as “providers.”

**Table 2.3.2. Manufacturing Process Information Domains**

DOMAIN	USERS	RULES	PROCESS	INFORMATION
MANUFACTURING Catalog Items	Potential Customers	read	Inquiry	Catalog Item Inventories, Production schedules, Shipping Schedules Invoices
	Customers	read		
	Sales Representatives	read		
	Sales Managers	read		
	Operations Managers	read	Mfg. Std. Items Update	
	Production Managers	read		
	Operations Staff	read, write		
	Production Control Staff	read, write		
MANUFACTURING Customer Orders  (one/cust)	Customers (specific)	auth: read	Inquiry	Customer Orders Inventories, Production Schedules Invoices  Shipping Schedules New Forms Requests
	Sales Representatives (customer's)	auth: read		
	Finance & Accounting	auth: read		
	Sales Managers	auth: read		
	Operations Managers	auth: read	Mfg. Customer Orders Update	
	Production Managers	auth: read		
	Operations Staff	read, write		
	Production Control Staff	read, write		
	Design Engineers	auth: read		
MANUFACTURING Raw Materials	Managers	auth: read	Raw Materials Management	Material Inventories Material Orders Suppliers Info
	Operations Staff	read, write		
	Production Staff	read, write		
	Finance & Accounting	auth: read		
MANUFACTURING Distribution	Operations Managers	auth: read	Distribution	Carriers Info Warehouse Info
	Production Managers	auth: read		
	Production Control Staff	read, write		
MANUFACTURING Design	Design Engineers	read, write	Forms Design	Forms Catalog
MANUFACTURING Operations	Operations Managers	read, write	Operations	Manufacturing Plans
	Operations Staff	read, write		
	XYZ BFD Executives	auth: read		
MANUFACTURING Product Control	Production Managers	read, write	Production Control	Equipment Data Maintenance Schedule Providers Engineering Notes
	Production Control Staff	read, write		
	Operations Managers	auth: read		
	Finance & Accounting	auth: read		

## 2.4 Warehousing Process Decomposition

Warehouse management involves inventory storage and distribution of XYZ BFD procured and produced products. It includes three level 2 processes, summarized in Table 2.4.1.<sup>8</sup>

Warehousing/distribution processes are partially described in the XYZ BPR changes documentation, and detailed in the project ABC documentation.

**Table 2.4.1. Warehousing Process Level 2 Decomposition**

USERS	PROCESS	INFORMATION
Warehouse manager Warehouse staff Customers Other XYZ employees	Inventory Control	XYZ-owned and non-owned warehouse inventory databases and inventory audit files
Warehouse manager Warehouse staff Customers Finance and accounting staff	Shipping	POs, releases, returns, and transfer transactions Invoices XYZ-owned warehouse inventory databases
Warehouse manager Warehouse staff Customers Other XYZ employees Finance and accounting staff	Receiving	Invoices XYZ-owned warehouse inventory databases

The inventory control process maintains accurate type, location, and quantity of products stored in both XYZ-owned and non-owned databases, and responds to inquiries about inventory. For inventory stored in non-owned warehouses, XYZ may inquire about its inventory, but may not update the information in that database; update privilege is reserved to the owner of the database. The inventory control process has two level 3 processes, as summarized in Table 2.4.2.

**Table 2.4.2. Inventory Control Process Level 3 Decomposition**

USERS	PROCESS	INFORMATION
Warehouse manager Shipping & receiving staff	Inventory update process	XYZ-owned inventory databases
Warehouse manager Warehouse staff Customers Authorized XYZ employees	Inventory inquiry (linkage of inquiry process), XYZ internal use product inquiries Shipping/receiving location finding inquiries	XYZ-owned and non-owned inventory databases

<sup>8</sup> It is assumed that some XYZ-internal-use products are stored in warehouses as well as other XYZ facilities where these products (e.g., manufacturing raw materials, facilities management office supplies, and IS/Comm management operations supplies and backup/transition hardware) to be used are stored.

The inventory update process is used to maintain accurate type/location/quantity of warehouse-stored products. There are two related but different sub-processes associated with the inventory update process, summarized in Table 2.4.3.

**Table 2.4.3. Inventory Update Process Level 4 Decomposition**

USERS	PROCESS	INFORMATION
Warehouse manager Warehouse staff	Normal Operations Inventory Update	XYZ-owned inventory databases
Outside independent inventory audit team and/or Inside assigned inventory audit team	Inventory Audit	XYZ-owned inventory databases and inventory audit count and discrepancies database

The normal operations inventory update sub-process is utilized by the shipping and receiving processes which routinely “pick and put” warehouse inventory. This accomplishes their distribution and storage functions.

The inventory audit sub-process provides the checks and balances oversight function for warehouse inventory control. The inventory audit sub-process is used to maintain the integrity of the inventory control process. Inconsistencies found between the inventory control database and manual counting results are reviewed and reconciled. The database is then adjusted.

The inventory inquiry process decomposes to two different types of inquiry handling sub-processes. The first is a link from the Level 1 Inquiry process, described in Section 2.2. The second type of inquiry sub-process is specific to internal XYZ and XYZ BFD employee inventory database queries. The inventory inquiry sub-process decomposition is summarized in Table 2.4.4.

**Table 2.4.4. Inventory Inquiry Process Level 4 Decomposition**

USERS	PROCESS	INFORMATION
Potential Customers, Customers, XYZ Employees	Inquiry Process Linkage	Sold & to-sell product inventory databases in two major partitions.
Authorized XYZ Employees	XYZ-Employee-Only Inventory Inquiry process	All XYZ-owned inventory databases

The inquiry process linkage relates to two distinctly different inquiry sub-processes, as discussed in Section 2.2, and summarized in Table 2.2.3. The sub-processes are distinguished by inventory inquiry to the general products inventory, and inventory inquiry to a specific customer’s products inventory.

The XYZ-employee-only inquiry process is a separate sub-process of the warehouse inventory control process; it is not associated with the inquiry process described in Section 2.2. The

**UNCLASSIFIED**

purpose of this sub-process is to allow authorized XYZ employees to view inventory information related to XYZ BFD internal-use products stored in XYZ owned/managed warehouses. Authorized XYZ employees include staff from the manufacturing, facilities management, and IS/Comm management organizations.

The shipping process distributes products from warehouses to XYZ customers, XYZ internal organizations, and returns to suppliers. The shipping process is driven by four types of activities: customer purchase orders, customer releases, internal XYZ transfers, and supplier return orders. From these four driving activities, the shipping process collects the identified products from the warehouse inventory, packages the collected bundles for shipping, selects the appropriate carrier method, creates a shipping invoice, and ships the product bundles. The shipping process also includes notification messages to Finance & Accounting, other internal XYZ organizations, suppliers, and customers, as necessary, and updates the inventory databases via the inventory control update process. Table 2.4.5 summarizes the level 3 shipping process decomposition.

**Table 2.4.5. Shipping Process Level 3 Decomposition**

<b>USERS</b>	<b>PROCESS</b>	<b>INFORMATION</b>
Warehouse shipping staff, customers, authorized XYZ employees	Shipping Request Handling Process	Order files, supplier return messages from internal organizations, transfer messages from internal organizations, and pick/bundle files
Warehouse stock staff	Picking & Bundling Process	Pick/bundle files
Warehouse shipping staff	Invoice & Ship Process	Invoices, customer profiles, preferred freight carriers, notification messages

The shipping request handling process is activated by inputs from order processing, and XYZ internal transfer and supplier product return messages. This process creates stock pick & bundle files that direct warehousing stock handling personnel to fetch and package the appropriate product bundles for shipping.

The picking and bundling manual process fetches the stock items directed in a pick/bundle file and packages/bundles the collection of items for shipping.

The invoice and ship process checks the bundle ready for shipment against the purchase order, release, or return, making any adjustments necessary to ensure the purchase order or release is filled correctly or the return to supplier is complete in accordance with the receiving invoice. This process also creates an invoice for the goods to be shipped, ensures the goods are shipped by the appropriate carrier, and notifies the proper XYZ BFD organizations of the shipment. Also, this process updates the warehouse inventory databases to reflect the stock used.

The receiving process takes in supplier shipments and customer-returned goods to XYZ warehouses, and handles transfers between XYZ and non-XYZ controlled warehouses. This

process is essentially the reverse of the shipping process. Table 2.4.6 summarizes the level 3 decomposition of the receiving process.

**Table 2.4.6. Receiving Process Level 3 Decomposition**

USERS	PROCESS	INFORMATION
Warehouse receiving staff	Received Products Handling process	Supplier invoices, customer return goods invoices, XYZ internal transfer transactions
Stock movement staff	Stock Products Received	Inventory database(s)
Warehouse receiving staff	Received Goods Invoice Processing	Accounts payable invoice database, accounts receivable database adjustments (returned customer goods)

The received products handling process deals with deliveries to the warehouse. The process is responsible for checking the invoice against goods received, and logging the supplier invoice, customer returned goods invoice, or internal transfer transaction for processing. The stock products received process deals with storing the delivered goods in the warehouse and updating the inventory database(s). The received goods invoice processing process deals with archiving the receiving invoices and internal transfer transactions. It is also responsible for forwarding a copy of the invoice along with date received to the finance and accounting accounts payable process for supplier receiving goods, and accounts receivable process for customer returned goods. There are no level 4 receiving process decompositions.

## 2.4.1 Warehousing Process Threat Analysis & Information Domains

In analyzing the warehousing processes and information from a threat perspective, three general controlling functions are examined: inventory management, shipping and receiving transaction management, and warehousing oversight management.

From the XYZ Corporation Information Protection Policy:

### Warehousing/Distribution/Transport

**Threats:** Information about inventories of products, shipping schedules, carriers, transfers and disposals is threatened by loss or damage (low) but has (significant) impact on service to customers.

**Security Services:** This information is in access (moderate) to authenticated (minimum) customers, and XYZ employees. Integrity (moderate) in storage and transfer and confidentiality (minimum) in transfer is required.

The threat analysis conclusions of XYZ BFD's warehousing information varies somewhat from the corporate-level IPP threat conclusions, as follows.

**UNCLASSIFIED**

1. Inventory management includes managing privileges to update the inventory database(s) by particular users. The threat of unauthorized modification (loss or damage) is *medium* and has a *significant* impact potential on service to customers, but only a *minimum* impact potential of product/property theft. The non-availability threat to inventory information is *low* but has a *significant* impact potential on service to customers.<sup>9</sup>
2. Shipping and receiving transaction management includes pulling/picking and putting stock distribution operations, and managing invoices, releases, and transfer transaction handling and notification processes and procedures. The threat of unauthorized disclosure is *low* and has a *minimum* impact. The threat of unauthorized modification is *medium* and could have a *significant* impact.
3. Warehousing oversight management is fulfilled with the Inventory Audit process. The audit process includes independent physical stock counts to match against the inventory database, discrepancies records, and investigative results information. The threat of unauthorized disclosure is *low* and has a *minimum* impact. The threat of unauthorized modification is *medium* and could have a *serious* impact.

Considering the above threat conclusions to warehousing information, seven information domains for the XYZ BFD warehousing process are determined. Two of the seven have been defined in Section 2.2 - the status and inventory and inventory and quotes inquiry process domains. The remaining five information domains are summarized in Table 2.4.7.

**Table 2.4.7. Warehousing Process Information Domains**

<b>DOMAIN</b>	<b>USERS</b>	<b>RULES</b>	<b>PROCESS</b>	<b>INFORMATION</b>
WRHS Internal Products Inv. Management	Manufacturing staff	Auth: read	Internal-Use- Products Inventory Inquiry	Internal-use- products inventory
	Facilities mgt staff	Auth: read		
	IS/ Comm mgt staff	Auth: read		
	Warehouse employees	Auth: read/write	Inventory Update proc	
WRHS Customer- Specific Prod Inventory Management [1per cust acct]	Customer rep(s)	Auth: read	Inquiry process	Customer- specific inventory
	Account manager	Auth: read		
	Account/Sales rep	Auth: read		
	Warehouse employees	Auth: read/write	Inventory Update process	
WRHS General Prod Inventory Management	Anyone	Auth: read	Inquiry process	General products inventory
	Warehouse employees	Auth: read/write	Inventory Update process	

<sup>9</sup> The non-availability threat correlation to the unauthorized modification threat (i.e., destruction of inventory information) carries the same potential and impact to customer service as defined by the unauthorized modification threat.

DOMAIN	USERS	RULES	PROCESS	INFORMATION
WRHS Accounting Management	Warehouse employees	Auth: read & write	Warehouse Management	Invoice logs & archive, transfer & return transactions notification info
WRHS Inventory Audit Management	Independent audit personnel and authorized warehouse employees	Auth: read & write	Inventory Audit process	Inventory audit count, discrepancies, and investigative files

## 2.5 Business Planning Process Decomposition

The business planning process focuses upon the plans and strategies to support U.S. Business Form’s missions. The Business Planning Process develops the business directives, objectives, and goals and determines the critical success factors for the corporation. Information is retrieved from sales, budgeting, marketing, and manufacturing. The business planning process in Table 2.0.1 does not decompose below level 1. Table 2.5.1 shows level 1 with a detailed breakout of the users and information. This analysis was guided by the NorthStar documentation and interviews with XYZ executives.

**Table 2.5.1. Business Planning Process Level 1 Decomposition**

Users	Process	Information
XYZ BFD executives and staff	Business planning	Strategic targets, policies, directives, objectives, goals
Sales managers		
Manufacturing managers		
Finance managers		

### 2.5.1 Business Planning Process Threat Analysis and Information Domains

From the XYZ Corporation Information Protection Policy—

## Planning

**Threats:** Information about planning for new products, new business areas, facility and equipment additions or modification, price changes, strategic account management, research, marketing initiatives is threatened by disclosure (low) but can have (significant) impacts through competitor knowledge.

**Security Services:** Access (moderate) to such information is to specifically involved XYZ personnel with confidentiality (moderate) and integrity (minimum) in storage and transfer. Sales personnel are permitted to release information to customers at planned release dates or events. This represents a change in policy for that information which is to be effected by the designated security administrators.

The business planning process has a single information domain. XYZ is concerned both with the integrity and confidentiality of this information. Access to this information is to managers and executives and their staffs. To protect the integrity of this information only the executives and their staffs can enter or write the information. To generate this information the executives and their staffs must be members of other domains to read whatever information they need. This information includes competitors prices, sales planning, sale budgets, market research, manufacturing plans, etc. The Business Planning domain is shown in Table 2.5.2.

**Table 2.5.2. Business Planning Process Information Domains**

DOMAIN	USERS	RULES	PROCESS	INFORMATION
BUSINESS PLANNING	XYZ BFD executives and staff	Read/write	Business Planning	Strategic targets, policies, directives, objectives, goals
	Sales managers	Read		
	Manufacturing managers	Auth: read		
	Finance managers	Auth: read		

## 2.6 Marketing Process Decomposition

The marketing process from Table 2.0.1 is decomposed into product promotion, targeting/projections management, and sales analysis as shown in Table 2.6.1. The decomposition was guided by existing mainframe applications, the NorthStar Project documentation, and XYZ BPR changes concepts.

**Table 2.6.1. Marketing Process Level 2 Decomposition**

<b>USERS</b>	<b>PROCESS</b>	<b>INFORMATION</b>
Potential customers, customers, sales managers, sales representatives	Product Promotion	Catalog, brochures, advertisements, standard prices
Sales managers sales representatives XYZ BFD executives	Targeting/ Projections Management	Customer histories, customer pricing strategic targets, monthly/yearly projections, market research, competitor prices, sales planning
Sales managers sales representatives XYZ BFD executives	Sales Analysis	Sales performance monitoring scorecards

## 2.6.1 Marketing Process Threat Analysis and Information Domains

From the XYZ Corporation Information Protection Policy:

### Marketing

**Threats:** Marketing information wherein sales people promote products and service to customers and potential customers, assess markets, quote standard pricing, and acquire information about the competition is threatened (medium) by the possibility of information being lost or damaged. The impact of such loss is considered (mild) requiring an investment in the rebuilding of the information.

**Security Services:** Marketing information shall be protected for data integrity (minimum). Confidentiality is not required. Access controls (minimum) must limit information entry to XYZ personnel with some exceptions for customer inquiry records.

### Sales

**Threats:** Sales information wherein non-standard pricing arrangements are afforded to specific customers, or planning for special sales or agreements is threatened by disclosure (medium) and loss or damage (medium). The impact of disclosure is (significant) and of loss or damage is (mild)

## UNCLASSIFIED

Appendix H, Annex A  
IATF Release 3.1—September 2002

**Security Services:** This sales information requires confidentiality (minimum) and integrity (minimum) in both storage and transfer. Access control (minimum) must limit information entry and disclosure to XYZ sales personnel and information disclosure to only the specific customers involved. I&A (minimum) is required to support the other security services.

Analysis of the information and users of marketing at the second level of decomposition resulted in a perceived need to separate customer unique information into marketing-customers domains. This limits access to a customer's history and any special pricing to those with specific customer responsibilities or oversight positions. The customer's sales representative is therefore granted read and write access in this domain. The sales analyst here is considered an oversight role with equal privileges. The specific customer is granted read access. Other customers and sales representatives are excluded. The process called upon in this domain, profile management, is drawn from the customer ordering process. The separation of customer history from customer pricing was considered as a possible need but is not recommended as necessary. Sales Managers are authorized read access for administrative oversight of marketing.

The marketing-promotion domain allows practically anyone to view all the products and services available from XYZ BFD. This domain is for advertising and must be widely viewable. The content however must be generated and controlled by XYZ BFD marketing. The preparation of this information is accomplished by Sales Managers and Sales Analysts.

The Marketing-Strategy domain is viewable by XYZ BFD management and marketing personnel. Customers and other users are excluded to protect the timing and objectives of major sales events until available to the public. At the appropriate time, sales managers and analysts may transfer information from the marketing-strategy to the marketing-promotion domain. This domain also includes information gathered about competitors and any marketing plans. The documentation of marketing-strategy information is accomplished by Sales Analysts.

The marketing-sales domains (one per customer) permits the customer's sales representative to see performance data for his or her accounts but excludes other sales representatives. Managers and XYZ BFD executives can monitor this activity but only Sales Analysts may prepare the information.

Any of the privileges identified within these Marketing information domains must be enabled by the authentication of the identities claimed.

**Table 2.6.2. Marketing Process Information Domains**

DOMAIN	USERS	RULES	PROCESS	INFORMATION
MKTNG Promotion	Potential customers	Read	Product Promotion	Catalog, brochures, advertisements, standard prices
	Customers (any)	Read		
	Sales managers (any)	Read, Auth: write		
	Sales analysts (any)	Read, Auth: write		
	Sales representatives (any)	Read		
	XYZ BFD executives	Read		
MKTNG Customer  (one per customer)	Customers (specific)	Auth: read	Profile Management	Customer histories Customer pricing
	Sales managers (any)	Auth: read		
	Sales analyst (any)	Auth: read, Auth: write		
	Sales representatives (Customer's)	Auth: read, Auth: write		
MKTNG Strategy	Sales managers (any)	Auth: read, Auth: write	Targeting/ Projections Management	Strategic targets, Competitor prices, sales planning Monthly/yearly projections, market research
	Sales analysts (any)	Auth: read, Auth: write		
	Sales representatives (any)	Auth: read		
	XYZ BFD executives	Auth: read		
MKTNG Sales  (one per customer)	Sales managers (any)	Auth: read	Sales analysis	Sales performance monitoring scorecards
	Sales analysts (any)	Auth: read, Auth: write		
	XYZ BFD executives	Auth: read		
	Sales representatives (specific customer)	Auth: read		

## 2.7 Finance and Accounting Process Decomposition

The finance and accounting process from Table 2.0.1 is decomposed into Accounts Receivable, Accounts Payable, and General Ledger as shown in Table 2.7.1.

**Table 2.7.1. Finance and Accounting Process Level 2 Decomposition**

USERS	PROCESS	INFORMATION
Finance managers Accounts receivable staff	Accounts receivable	Customer information customer orders warehouse, manufacturing info credit info prices collections general ledger
Finance managers Accounts payable staff	Accounts payable	Warehouse, manufacturing info facilities info, invoices customer orders payments, on-hold payments contracts general ledger payroll
Finance managers Plans staff	Financial planning	Pricing general ledger investment records tax records, payroll records customer profiles reports assets budgets capital expenditures

## 2.7.1 Finance and Accounting Process Threat Analysis and Information Domains

From the XYZ Corporation Information Protection Policy—

### Finance and Accounting

**Threats:** Financial information such as customer accounts receivable, accounts payable, general ledgers, financial reports, purchase orders, banking, payroll, commissions and bonuses, capital expenditures, and capital assets are considered to be threatened by disclosure (high) and loss or damage (medium). The impact of disclosure is (serious) and of loss or damage is (significant).

**Security Services:** This information is in access (strong) to specific finance personnel by information domain, to all auditors and XYZ business area and corporate officers as needed. Confidentiality (strong) and integrity (moderate) in storage and transfer is required. I&A required is (strong)

The information domains shown in Table 2.7.2 were chosen to separate planning from transactional information, and internal transactions from external transactions. This separation allows information to be entered by XYZ employees other than finance and accounting. This is in variance to the limitations imposed by XYZ Corporate policy but is necessary for business flow. The domain structure chosen would require accounts receivable and accounts payable to be transferred into the general ledger by financial personnel.

Similarly, warehouse, manufacturing, and facilities transactions can be recorded by those staffs with finance controlling posting to the ledger.

**Table 2.7.2. Finance and Accounting Process Information Domains**

DOMAIN	USERS	RULES	PROCESS	INFORMATION
FINANCE Management	Finance managers	Read, write	Financial Planning	Assets, budgets tax records general ledger capital expenditures reports investments banking
	Finance staff	Read, write		
	XYZ BFD executives	Auth: read		
	Auditors	Auth: read		
			Accounts payable	
			Accounts receivable	
FINANCE Customer  (one/customer)	Accounts receivable staff	Read, write	Accounts receivable	Customer credit customer orders special pricing collections
	Finance managers	Auth: read		
	Sales managers	Auth: read		
	Sales representatives (specific customer)	Auth: read		
FINANCE Deliveries	Accounts receivable staff	Read, write	Accounts receivable	Warehouse invoices manufacturing invoices Contract deliveries
	Finance managers	Read, write		
	Warehouse staff	Read, write		
	Manufacturing staff	Read, write		
FINANCE Expenditures	Accounts payable staff	Read, write	Accounts payable	Warehouse expen Mfg/facilities expen is/comm expen payments, On Hold contracts let
	Warehouse staff	Read, write		
	Manufacturing staff	Read, write		
	Facilities staff	Read, write		
	IS/Comm staff			
FINANCE Payroll	Accounts payable staff	Read, write	Payroll	Employee records EFT transfers commissions bonuses
	HR personnel	Auth: read		

## 2.8 Personnel Management Process Decomposition

The personnel management process manages all actions associated with XYZ employees, including payroll. The process from Table 2.0.1 is decomposed into H/R management, employee records management, and payroll management as shown in Table 2.8.1.

**Table 2.8.1. Personnel Management Process Level 2 Decomposition**

USERS	PROCESS	INFORMATION
Employees	Personnel Management	Organizational
H/R Personnel		Training Information
Finance Personnel		Recruiting
U.S. Business Form's Execs		Benefits & Compensation
		Division Policy & Procedures
Employees	Employee Records Management	Employee
H/R Personnel	Payroll Management	Time & Attendance
Finance Personnel		

### 2.8.1 Personnel Management Process Threat Analysis and Information Domains

From the XYZ Corporation Information Protection Policy:

#### Human Resources/Personnel Administration

**Threats:** Information about XYZ personnel which permits the administration of payroll and benefits, promotions, assignment of duties, and performance appraisals, is considered threatened by disclosure (medium) and by loss or damage. The impact of disclosure to anyone who does not specifically need to know is (serious). The impact of loss or damage is (significant).

**Security Services:** Access to this information must be (strong) to only those involved in personnel administration and to the specifically involved supervisory personnel. Confidentiality (strong) and integrity (strong) is required for storage and transfer of this information. I&A (strong) is necessary to support the other security.

#### Finance and Accounting

**Threats:** Financial information such as customer accounts receivable, accounts payable, general ledgers, financial reports, purchase orders, banking, payroll, commissions and bonuses, capital

expenditures, and capital assets are considered to be threatened by disclosure (high) and loss or damage (medium). The impact of disclosure is (serious) and of loss or damage is (significant).

**Security Services:** This information is in access (strong) to specific finance personnel by information domain, to all auditors and XYZ business area and corporate officers as needed. Confidentiality (strong) and integrity (moderate) in storage and transfer is required. I&A required is (strong).

Analysis of this information, which contains both human resources and financial information, results in the need to separate employee-unique information from general personnel information. Further access to and the ability to create or change employee-unique information must be tightly controlled. This leads controlled access to the information and to the separation of employee information into information that the employee can create or change and employee information that only an employee can read. Each of these domains have two processes that can act upon the information. Only employees and H/R personnel can use the Manage Employee records process. Only finance personnel can use the payroll process. These two domains are called employee managed records/payroll and employee-h/r managed domains, respectively. Analysis of the general personnel information leads to the need to protect the integrity of the information. This leads to the separation of this information into domains were only the H/R personnel and the Division executives can create or change the information. These domains are the h/r management and division policy domains. These domains are shown in Table 2.8.2.

**Table 2.8.2. Personnel Management Process Information Domains**

DOMAIN	USERS	RULES	PROCESS	INFORMATION
PERSONNEL Employee- Managed Records/Payroll	Employee (specific)	Read/write	Manage Employee Records	Employee managed
	H/R personnel	Read/write	Payroll processing	Time & attendance
	Finance personnel	Auth: read		
PERSONNEL Employee-H/R Managed	Employee (specific)	Auth: read	Manage Employee Records	H/R managed
	H/R personnel	Auth: read/write	Payroll processing	
	Finance personnel	Auth: read		
PERSONNEL H/R management	Employees (any)	Auth: read	H/R Management	Organizational
	H/R personnel	Read/write		Training programs
	Finance personnel	Auth: read		Recruiting
PERSONNEL Division Policy	XYZ BFD execs	Read/write	Policy Management	Division policy & procedures
	Employees (any)	Auth: read		

## 2.9 Information Systems & Communications Management Process Decomposition

The IS/Communications management process operates, monitors, and maintains XYZ BFD electronic information management technologies and applications. It is also responsible for planning, transitioning, integrating, testing, and administering new information systems and applications to maintain a technologically competitive work flow environment for XYZ BFD's business processes, customers, and employees. This process decomposes to four level 2 sub-processes, summarized in Table 2.9.1.

**Table 2.9.1. IS/Comm Management Process Level 2 Decomposition**

<b>USERS</b>	<b>PROCESS</b>	<b>INFORMATION</b>
IS/Comm operations staff	Operations	System management Information network management information
IS/Comm management & planning staff, outside contractors and consultants	Planning	Planning information
Integration contractors, IS/Comm management staff	Integration & Test	Integration information, test and evaluation information
Outsourcing contract manager IS/Comm management staff	Outsource contractor oversight	Contract information, performance information, financial information, adjustments information

The operations process decomposes to two level 3 sub-processes, summarized in Table 2.9.2.

**Table 2.9.2. Operations Process Level 3 Decomposition**

<b>USERS</b>	<b>PROCESS</b>	<b>INFORMATION</b>
IS/Comm managers end-system system operators end-system users capital equipment administrators IS Help desk personnel system hardware/software maintenance personnel application server O&M staff	System management	Capital Equipment inventory configuration information accounting information performance information trouble reporting/resolution information scheduling information outage & status information application management info
IS/Comm managers tech controllers end-system users capital equipment administrators Comm help desk personnel Comm hardware/software maintenance personnel	Network management	Capital Equipment inventory configuration information accounting information performance information trouble reporting/resolution information status & outage information

The system management process deals with the operations and maintenance of all XYZ BFD end systems. End systems include all workstations, laptops/notebooks, terminals, mainframes, mini and micro servers, telephones, facsimile equipment, and video conferencing cameras, computers, etc. used for information processing and information exchange in XYZ BFD'S area of IS/Comm management. It also includes all applications, system software, and utilities used on those end systems, as applicable. It does not include manufacturing equipment; manufacturing equipment used to produce XYZ BFD products is the responsibility of the manufacturing management process. The system management process decomposes to seven level 4 sub-processes, summarized in Table 2.9.3.

**Table 2.9.3. System Management Process Level 4 Decomposition**

<b>USERS</b>	<b>PROCESS</b>	<b>INFORMATION</b>
IS/Comm managers capital equipment administrator	Capital Equipment Inventory Management	Capital equipment inventory
IS/Comm managers system operators	Configuration Management	Configuration information
IS/Comm managers system operators end system users	Accounting Management	Accounting information
IS/Comm managers system operators	Performance Management	Performance monitoring information

**UNCLASSIFIED**

Appendix H, Annex A  
IATF Release 3.1—September 2002

<b>USERS</b>	<b>PROCESS</b>	<b>INFORMATION</b>
IS/Comm managers system operators	Job/scheduling Management	Job/scheduling information
IS/Comm managers IS help desk personnel system operators system hardware/software maintenance personnel end system users	Trouble Reporting & Resolution Management	Trouble reports/resolution information
IS/Comm managers system operators	Outage Collection Management	System outage & recovery information
IS/Comm managers application server O&M staff	Application Management	Application configuration & utilization information

The network management process deals with the operations and maintenance of all XYZ BFD’s communications systems, which includes: local area network media, hubs, bridges, and routers/gateways and configuration and addressing tables; local plant telephone wiring and switching components, and wide area communications leased line services and value added network interfaces from XYZ BFD facilities. The network management process decomposes to eight level 4 sub-processes, summarized in Table 2.9.4.

**Table 2.9.4. Network Management Process Level 4 Decomposition**

<b>USERS</b>	<b>PROCESS</b>	<b>INFORMATION</b>
IS/Comm managers capital equipment administrator	Capital Equipment Inventory Management	Capital equipment inventory
IS/Comm managers comm operators	Configuration Management	Configuration information
IS/Comm managers comm operators end system users	Accounting Management	Accounting/utilization information
IS/Comm managers comm operators	Performance Management	Performance monitoring information
IS/Comm managers Comm help desk personnel Comm operators Comm system hardware/software maintenance personnel end system users	Trouble Reporting & Resolution Management	Trouble reports/resolution information
IS/Comm managers comm operators	Outage Collection Management	Comm outage, recovery, & status information

Based on design and personnel allocation considerations, the system and network processes could be combined, but with clear delineation of roles and responsibilities. Common sub-processes, such as capital equipment inventory management, trouble reporting and resolution management, and to some extent configuration management, are logical candidates of overlapping functions where certain personnel may play both the system and network management roles.

Power, air conditioning, etc. required for IS/Comm is the responsibility of the facilities management process. Security management required for IS/Comm and facilities is the responsibility of the security management process.<sup>10</sup> Although it is necessary to delineate these processes in this way, it is possible that personnel roles and responsibilities may overlap organizational structure delineations. The latter is both a system design and personnel allocation consideration. In the case of security management, it is also a crucial security consideration—internal XYZ personnel should always be the security managers and administrators.

The IS/Comm planning process includes change management, system transitions, and the analysis of its information management model, new standards, technologies, and applications that XYZ BFD could utilize to maintain a competitive information management posture in the forms marketplace. This process does not decompose further, unless IS/Comm management chooses to detail it to a finer granularity, depending on the scope of its planning activities.

The integration and testing process includes system design, integration planning, and operational test and evaluation activities necessary to fulfill the results of planning process activities. This process also includes ordering hardware and software components from chosen vendors, and managing warehouse transfer requests to move warehouse-stored products for integration and testing. This process does not decompose further, unless IS/Comm management decides to detail it to a finer granularity, depending on the scope of any integration and testing activities. There is close coordination between the operations, planning, and integration and testing processes to ensure continuing operational performance objectives.

The outsource contracting management process includes managing the outsource contracts, providing outsource contractor direction and guidance, and rating the outsource contractor performance. This process does not decompose further, unless IS/Comm management determines that each of the functions need to be delineated to a finer granularity. There is obvious need for coordination between system, network, and integration/test performance monitoring functions and the outsource contracting management process.

---

<sup>10</sup> Security management architectural constructs typically spread across facilities management (the environment protection allocations), end systems (the information system protection portion of IS/Comm), and communication systems (the transfer system portion of IS/Comm). Although an autonomous and independent level 1 process, security management blankets integral portions of all core and infrastructure business processes.

## 2.9.1 IS/Comm Process Threat Analysis & Information Domains

Threat analysis of XYZ BFD IS/Comm process and sub-processes concludes no variance from the threat analysis results of this infrastructural area described in the XYZ Corporate-level Information Protection Policy.

From the XYZ Corporation Information Protection Policy:

XYZ sets high standards in service and product availability to its customers. Information systems are threatened by:

- Processing system failures: malfunctions, errors, deliberate destruction, inadequate performance
- Communications system failures: malfunction, errors, deliberate destruction, inadequate performance
- Application failures: errors, loss, corruption
- Information failure: errors, loss, corruption, spoofing

The probability of one or more of these events occurring is (high) and will result in the disclosure, loss, or damage to information. The impacts are (serious).

As a result of these threats, their potential, and impact, eleven information domains have been generated. These information domains are summarized in Table 2.9.5.

**Table 2.9.5. IS/Comm Management Process Information Domains**

DOMAIN	USERS	RULES	PROCESS	INFORMATION
IS/COMM Management	Managers	Auth: read/write	Configuration mgmt Performance mgmt Outage Collect mgmt Accounting mgmt Scheduling mgmt	Configuration performance system outage, recovery & status accounting scheduling
	Operators	Auth: read/write		
	Users	Auth: read		
IS/COMM Maintenance	Managers	Auth: read	Trouble Reporting/Resolution mgmt	Trouble reports/resolution database
	Help desk staff	Auth: read/write		
	Operators	Auth: read/write		
	Maintenance staff	Auth: read/write		
	Users	Auth: read		
	Application staff	Auth: read/write		

**UNCLASSIFIED**

<b>DOMAIN</b>	<b>USERS</b>	<b>RULES</b>	<b>PROCESS</b>	<b>INFORMATION</b>
IS/COMM Trouble reporting	Help desk staff	Auth: read/ write	Trouble Report Submission	Trouble report entries
	Operators	Write		
	Users	Write		
	Application staff	Write		
IS/COMM Applications	Managers	Auth: read	Application mgmt	Application configuration/utilization
	Application staff	Auth: read/write		
IS/COMM Management	Managers	Auth: read/write	Configuration mgmt Performance mgmt Outage Collection mgmt Accounting mgmt	Configuration performance system outage, recovery/status accounting
	Operators	Auth: read/write		
	Users	Auth: read		
IS/COMM Maintenance	Managers	Auth: read	Trouble Reporting & Resolution mgmt	Trouble reports/ resolution database
	Help desk staff	Auth: read/write		
	Operators	Auth: read/write		
	Maint. personnel	Auth: read/write		
	End system users	Auth: read		
	Appl O&M staff	Auth: read/write		
IS/COMM Trouble reporting	Help desk staff	Auth: read/ write	Trouble Report Submission	Trouble Report Entry Information
	Operators	Write		
	Users	Write		
	Application staff	Write		
IS/COMM Inventory	Managers	Auth: read	Capital Equipment Inventory mgmt.	Capital Equipment Inventory
	Capital equipment administrator	Auth: read/write		
IS/COMM Planning	Managers	Auth: read/write	Planning	Plans
	Planning staff	Auth: read/write		
	Contractors	Auth: read/write		
	Consultants	Auth: read		
	Employees	Auth: read		
IS/COMM Integration	Contractors	Auth: read/write	Integration/Test	Integration Test/Evaluation
	Management	Auth: read/write		
IS/COMM Contracts	Outsource Management	Auth: read/write	Outsource Contract Oversight	Contract, performance, financial, and adjustments
	Management	Auth: read/write		

## 2.10 Facilities Management Process Decomposition

Facilities management deals with two major infrastructure support elements of XYZ BFD: office supplies management, and physical facilities and utilities management and maintenance.

**Table 2.10.1. Facilities Management Process Level 2 Decomposition**

USERS	PROCESS	INFORMATION
Office managers, admin staff	Office Supplies Management	Ordering Information (POs) delivery Information (Invoice) transfer Information inventory Information utilization statistical Info
Facility managers, maintenance staff	Physical Facilities & Utilities Management	Facility incident reports personnel locator list utilities utilization & outage logs utilities maintenance reports ordering information (POs) delivery Information (Invoice) billing (AP) Information transfer information inventory information

Although it is possible to decompose each of the two processes to lower levels of resolution, it is not necessary from a security perspective.

### 2.10.1 Facilities Management Process Threat Analysis and Information Domains

From the XYZ Corporation Information Protection Policy:

#### Facilities Management

**Threats:** Facilities management information when associated with the security management function is threatened by loss or damage (medium). The reliability of electrical power systems, air conditioning, communications channels is a security issue. Information about power systems service providers and product repair services are examples of relevant data.

**Security Services:** Data integrity (minimum) of facilities management data must be maintained.

Two information domain types are determined to maintain the separation of office supplies and physical facilities management. The office supplies management domain type may be a single domain for the entire facility, or it may be separate domains by division. The physical facilities management domain type has at least one information domain type of this kind per XYZ BFD facility. Small satellite facilities may be under a single domain, or arranged by region and coupled with larger facilities in that region. The two domain types are summarized in Table 2.10.2.

**Table 2.10.2. Facilities Management Process Information Domains**

DOMAIN	USERS	RULES	PROCESS	INFORMATION
FACILITIES MGMT Office supplies	Office managers	Auth: read/write	Office Supplies mgmt	Ordering (POs) delivery (invoice) transfer inventory utilization statistics
	Administrative staff	Auth: read/write		
FACILITIES MGMT Facilities and Utilities	Facility managers	Auth: read/write	Physical Facilities/ Utilities mgmt	Facility incident reports personnel locator list utilities utilization/outage logs utilities maintenance reports ordering (POs) delivery (invoice) billing (AP) transfer inventory
	Maintenance staff	Auth: read/write		

## 2.11 Corporate Relations Process Decomposition

The corporate relations process is focused upon report information and does not decompose below the first level.

### 2.11.1 Corporate Relations Process Threat Analysis and Information Domains

From the XYZ Corporation information protection policy:

## XYZ Corporate Relations

**Threats:** Information exchange between corporate divisions of XYZ are threatened by loss or damage (low). The impact of such a loss is (mild).

**Security Services:** Access (minimum) to this information should be to XYZ Employees. Data integrity requirements are (minimum).

There are minimal requirements for protection on the corporate relations information. However, there is still a need to protect the integrity of the information which is reflected in the rules. The domain for this process is shown in Table 2.11.1.

**Table 2.11.1 Corporate Relations Process Information Domain**

DOMAINS	USERS	RULES	PROCESS	INFORMATION
Corporate Relations	XYZ BFD Execs	auth: read/write	Corporate Relations	Reporting Information
	Corporate Executives	auth: read		

## 2.12 Security Management Process Decomposition

Security management deals with the initialization and subsequent operational controls of security policy (or policies) and security mechanisms. It is a process which is interleaved throughout and supports all information domains, and, as part of a security architecture, is allocated across environmental, end system, and transfer system architectural elements. As a logical process portion of the information management model, it decomposes to two level 2 processes, summarized in Table 2.12.1.

**Table 2.12.1. Security Management Process Level 2 Decomposition**

USERS	PROCESS	INFORMATION
Security Mgrs, Admin information domain members	Security Policy Management	Domain registration information security management information base
Security managers admin	Security Mechanism Management	Security management information base

The security policy management process deals with information management in both written form and machinable form. The written form includes XYZ corporation policies. In machinable form, this process installs and maintains rules and attributes to support the rules defined by the

written XYZ division IPPs. This process also registers information domains into the system and deletes information domains from the system.

The security mechanisms management process deals with the management of the security mechanisms and the information used by the security mechanisms to provide their security decision and enforcement functions. The security mechanisms enforce the security policy rules installed and maintained by the security policy management process. Each and every security mechanism implemented into the information system needs to be managed. Security mechanisms can be doctrinal, such as physical and procedural security, or electronic. Electronic security mechanisms always require doctrinal security mechanisms to protect them from unauthorized tampering, bypass, or destruction. Electronic security mechanisms include such things as user authentication, access control decision and enforcement functions, communication confidentiality, data integrity, and non-repudiation mechanisms (cryptographic mechanisms, key management mechanisms, digital signature mechanisms), and pervasive security mechanisms. The management of security mechanisms is a very complex process.

## 2.12.1 Security Management Process Threat Analysis & Information Domains

From the XYZ Corporation Information Protection Policy:

### Security Management

**Threats:** Implementation of policies and information needed to support the security services are at the core of any possibilities for information protection. Threats of disclosure and loss or damage are (high) and the impacts are (serious). Security management also involves physical security, administrative security, personnel security as well as the technical aspects of information security.

**Security Services:** This information requires integrity (strong) and confidentiality (strong) in storage and in transfer. Access control (strong) and the supporting I&A (strong) for specific security managers is required.

Every internal XYZ BFD information system component must have at least one context of a security management process and a security management information base. The security management process may be an integral element of the information domain of the user, or it may be a separate security management domain which is used to maintain and enforce the security policy for each, or all, information domains in which a user is authorized.<sup>11</sup> The security management domains are summarized in Table 2.12.2.

---

<sup>11</sup> There is one information domain in XYZ BF that anyone (identity unknown) may operate in -- the I1 inquiry process domain. The only security management function which is affiliated with this domain is the access control function to

**Table 2.12.2. Security Management Process Information Domains**

DOMAIN	USERS	RULES	PROCESS	INFORMATION
SECURITY MGMT System	Division security Mgr	Auth: read	Security Mgt	System security data
	System security Mgr	Read: write		
	Domain security Mgrs	Auth: read		
	Domain members	Auth: read		
SECURITY MGMT Mechanisms	Division security Mgr	Auth: read	Security Mgt	Security mechanisms data
	System security Mgr	Read: write		
	Domain security Mgrs	Auth: read		
	Domain members	Auth: read		
SECURITY MGMT Domain	Division security Mgr	Auth: read	Security Mgt	Domain security data
	System security Mgr	Auth: read		
	Domain security Mgrs	Read: write		
	Domain members	Auth: read		

### 3.0 Other Information Domain Considerations

Although unconfirmed, it is assumed that other types of information domains might be needed within XYZ BFD information systems. These other types of domains are compelled by the notion of individual employee domains, groupware domains for sharing correspondence between offices which do not, for one reason or another, fit a particular core or infrastructure business process defined in section 2, and perhaps others, such as “web server” (unauthenticated read only) domains, and the public domain. Architectural experiments currently underway within XYZ BFD, such as those investigating Internet-Commerce, groupware applications, etc. will require examination for new information domain considerations on a case by case basis. This stresses the importance of making XYZ BFD’s IMM and protection policies “living documents” -- i.e., they need to be upgraded from time to time, and maintained in accordance with changes in the IMM, XYZ BFD information protection policy, and XYZ Corporate Level information protection policy and policy guidelines.

---

maintain separation from all other information domains. All users of the I1 domain have read (non-authenticated read) privilege only.

# **PNE Annex B: Corporate IPP**

---

[This annex to this document is an unedited (except for company name) example of an actual IPP.]

## **XYZ CORPORATION**

### **Corporate Information Protection Policy**

**UNCLASSIFIED**

Appendix H, Annex B  
IATF Release 3.1—September 2002

**This page intentionally left blank**

# 1.0 Introduction

## 1.1 Purpose

This document establishes the policy of XYZ Corporation for the protection of information which is generated, stored, or received in the process of conducting its business. It presents the corporate policy on information protection in general as well as individual policies for specifically identified categories of information. Protection is defined for each information category in terms of the specific security services and the strengths required.

This document also establishes the procedures for its own maintenance and for the preparation and maintenance of other derivative policies for individual information categories.

## 1.2 Definitions

**Information:** data elements or objects generated, transferred, stored, processed, and destroyed in the conduct of business functions.

**Users:** individuals or groups of people who are responsible for managing a portion of the business information. Users include those who employ or manage information systems.

**Processes:** the functions performed by users or users aided by information systems which generate, transform, modify, collect, organize, present, and destroy information.

**Information Management Model (IMM):** a logical description of information management which depicts the users, processes, databases, and information flows which support a business enterprise.

**Information Domain:** A security entity composed of three elements—

- 1) Identifiable information objects.
- 2) membership of identifiable users
- 3) a security policy which defines the relationships between each member and all of the information objects.

**Information Domain Member:** a user identified to have some responsibilities or privileges in the management of the objects of an information domain.

**Security Policy:** rules which govern and identify the relationships between members and the objects of an information domain.

**Security Services:** activities that assist in, or provide for, the protection of information. Security services are provided by security mechanisms. Security mechanisms are diverse and include such things as guards, fences, cryptographic software, badges, or labels. The security

## UNCLASSIFIED

Appendix H, Annex B  
IATF Release 3.1—September 2002

services defined here are mutually supporting and often overlapping in the services provided. Although the definitions are provided in terms of people as individuals, they apply to groups, processes, and other agents or objects.

**Identification and Authentication (I&A):** The service which protects against the claims of individuals to be someone they are not. Identification is the establishment of the unique identity of an individual, group, or information system component. Authentication is the means for verifying the claimed identity.

**Access Control:** The service which protects information through the control of authorizations of individuals for knowledge or rights of manipulation.

**Confidentiality:** The service that protects information from knowledge or disclosure.

**Integrity:** The service that protects information from modification or loss.

**Availability:** The service that protects the individual from accidental or deliberate denial of access to information and other services.

**Non-repudiation:** The service which provides protection from an individual denying sending information (non-repudiation with proof of origin), or protection from an individual denying receiving information (non-repudiation with proof of delivery). These services are closely related to signing and notarization.

## 2.0 Information Protection Policy

### 2.1 Overview

The protection of information which supports business has always been essential to the success of corporations. However, many of the mechanisms for protection in computer based systems are significantly different from that of paper based systems. Ready access to information is one of the chief benefits of computer networks but it is also a major source of vulnerabilities. We take for granted the protective effects of buildings, offices, doors, receptionists, file cabinets, sealed envelopes, etc. Computer networks are designed for the sharing of information; overcoming distances and physical barriers that separate. Achieving a satisfactory balance between needed access and adequate protection requires the attention and careful consideration of the entire corporation. Security policies are instruments for coordination and agreement on what information needs protection, who are the potential adversaries, and who are the owners and protectors. Security policies document the decisions on protection and guide the architectures and implementations of information management systems.

XYZ Corporation mandates high availability of services to its customers. The provision of these services involves the access to some corporate information by XYZ's customers and even joint

management of other information by XYZ and its customers. Like most corporations, information is at the core of XYZ's business. There are many categories of information with different kinds and sources of threats. It is important to recognize that information protection is a direct service to customers as well as to XYZ's resources to provide all services. This policy presents the decisions and guidance for the necessary safekeeping of XYZ information.

## 2.2 Applicability

This security policy applies to all divisions of XYZ Corporation. As a multinational business XYZ is subject to the laws of the individual government jurisdictions. Conflicts which may arise between this policy and national or local laws must be resolved in favor of adherence to laws. Local laws which govern fraud and abuse, privacy protection, copyright protection, and governments rights to information access must be addressed and adhered to in the derivative policies of businesses which fall under those jurisdictions. Security architects and other implementers of this policy must be aware of the pertinent laws, for example, those which govern the use of and exportation/importation of cryptographic mechanisms and related materials. Security policies entered into by XYZ with other corporations and outside organizations must become part of this policy by inclusion or by reference.

## 2.3 Responsibilities

The preparation, modification, coordination, and promulgation of this policy is the responsibility of XYZ Corporation. The principal security focus within XYZ for these responsibilities is the Corporate Information Security Officer (CISO). The CISO is appointed by (Executive Committee e.g.)\_\_\_\_. The CISO is responsible to the Corporation for the implementation of this security policy. The CISO is responsible for the coordination of information security activities with those of other corporate security administrators such as those responsible for security guards or police or security investigations. The CISO shall recommend individuals for appointment as XYZ divisional Business Information Security Officers (BISO). The CISO recommendations for BISOs will be approved by (Division Executive e.g.)\_.

BISOs shall prepare business security policies consistent with this policy that govern the information protection requirements of their individual businesses. The BISO is also responsible for modification and coordination of business security policies. The business security policies must define any needed policy governing the interactions with other XYZ businesses. BISOs shall define within their policies how information domains are formed and how security administrators are designated to manage those information domains.

Information systems which are intended to implement and satisfy security policies must be certified and accredited. Certification is the process of security evaluation and reporting on the adequacy of a system to meet the requirements of a security policy. Accreditation is the process of approval and operational acceptance of a system which includes security. Accreditors are chosen from XYZ management to evaluate the effectiveness of their information systems in

meeting business objectives and the adequacy of its system management. BISOs are responsible for defining and managing the certification and accreditation processes.

All XYZ employees have some responsibility in protecting business information. Users of information must be made aware of security policies and must be informed of their responsibilities in meeting the protection requirements for any information that they manage. BISOs shall insure that all employees are informed of the responsibilities that they assume by virtue of their employment and all specific assignments.

## 2.4 Procedures

Security policies vary in their formality depending upon the scope or the number of people involved. A corporate security policy, for example, needs wide dissemination and coordination with many individuals and with all business divisions. Changes require similar efforts to accomplish. Formal processing of such a policy is a necessity. Section III of this document provides guidance for the preparation of such policies. Perhaps the simplest form of policy is when an individual employee prepares information such as a drafted document which for a time is accessible only by the originator. This event is the formation of an information domain with a single member who accepts that the protection of the environment and the information system utilized is adequate. The employee is the certifier and accreditor of the system and this policy may be simply implied. All security policies should be reviewed periodically for continued need. Any changes in environment or systems should be evaluated by the certifiers and accreditors for adequacy of protection.

Information protection shall be considered in the planning, development, and use of all XYZ information systems. This applies to stand alone (including personal) computers as well as computer networks. Users of information systems must be made aware and must observe the requirements for the protection, i.e. security policy, for any information managed by them on such systems.

Information protection shall be considered as part of all contractual agreements. All parties to contracting with suppliers or customers, for example, must consider the necessity for preparing and including a security policy as part of the contract.

Circumstances will sometimes create the need to circumvent normal protection mechanisms. For example, the release of information to non-members of an information domain may be required in an emergency. The appropriate method for dealing with such contingencies is to decide who is permitted to override protection mechanisms and who will audit such activities. These are examples of the possible roles for security administrators. Such contingencies can and should be addressed in security policies.

Certification and Accreditation of information systems become increasingly important as the number of users, computers, and facilities implementing the system become larger. Formal certification is normally accomplished by expert security analysts. The certifier, with knowledge of the security policy, evaluates the total effectiveness of system security mechanisms and

prepares a certification report. The report may recommend system acceptance or it may cite deficiencies which must be mitigated or eliminated prior to acceptance. Formal accreditation is normally accomplished by those who prepared the original operational requirements. The accreditor makes the critical decision to accept or reject a system and to permit its operational use. Selection of certifiers and accreditors must be accomplished as part of the security policy preparation function.

## **2.5 The XYZ Corporate Information Management Model (C/IMM)**

The basis for developing the security policy for XYZ is the corporate information management model (C/IMM). An IMM defines who engages in what functions using what information. The XYZ C/IMM is the composite view of the corporation which must be further decomposed for each business area or division to a level of definition that is useful for the identification of information domains.

XYZ Corporation is engaged in four major business areas:

### 1) Business Forms

- Design and manufacture of custom business forms
- Print management
- Print outsourcing services

### 2) Business Systems

- Graphics services
- Business equipment
- Business products
- Research
- CRS

### 3) Labels and label systems

- Integrated label systems
- Software products
- Printers and applicators
- Pressure sensitive labels
- Proprietary label products

### 4) Customer Communications Services

- Personalized direct mail
- Direct marketing program development

## UNCLASSIFIED

Appendix H, Annex B  
IATF Release 3.1—September 2002

- Database management and segmentation services
- Mail production outsourcing services
- Bulk Communications Services

Each of the major business areas is composed of Core Business Functions and Infrastructure Functions:

- Core Business Functions
  - Marketing/Sales
  - Customers/Orders
  - Manufacturing/ Vendors/ Supplies
  - Warehousing
  - Distribution/ Transport
- Infrastructure Functions
  - Planning
  - Finance and Accounting
  - Human resources/personnel administration
  - Research
  - XYZ corporate relations
  - Information systems/communications
  - Facilities management
  - Security management

{With some generic assumptions about users and information records that might be found in all XYZ businesses there is sufficient information to analyze threats to corporate information.}

## 2.6 Threat Analysis

The threat analysis is keyed to the functions of the C/IMM. The degree of threat expressed is a relative scale used to express the probability of attack (high, medium, low, none) and the degree of impact (serious, significant, mild, insignificant). The security services are given strength ratings (strong, moderate, minimum, none) to establish relative priority in the provision of protection. The information management elements and the associated security services may not be relevant to a specific division but they are applicable to all occurrences in the XYZ corporation.

### Marketing

**Threats:** Marketing information wherein sales people promote products and service to customers and potential customers, assess markets, quote standard pricing, and acquire information about the competition is threatened (medium) by the possibility of information being lost or damaged. The impact of such loss is considered (mild) requiring an investment in the rebuilding of the information.

**Security Services:** Marketing information shall be protected for data integrity (minimum). Confidentiality is not required. Access controls (minimum) must limit information entry to XYZ personnel with some exceptions for customer inquiry records.

## Sales

**Threats:** Sales information wherein non-standard pricing arrangements are afforded to specific customers, or planning for special sales or agreements is threatened by disclosure (medium) and loss or damage (medium). The impact of disclosure is (significant) and of loss or damage is (mild)

**Security Services:** This sales information requires confidentiality (minimum) and integrity (minimum) in both storage and transfer. Access control (minimum) must limit information entry and disclosure to XYZ sales personnel and information disclosure to only the specific customers involved. I&A (minimum) is required to support the other security services.

## Customers

**Threats:** Information about customers wherein accounts, customer profiles, ordering histories, and customer proprietary information is unique to that customer and threatened by disclosure (medium) and loss or damage (medium). The impact of disclosure of customer proprietary information is (serious) and the disclosure of other customer information is (significant)

**Security Services:** This customer information requires confidentiality (moderate) and integrity (moderate) in both storage and transfer. Access control (moderate) must limit information entry and disclosure to XYZ specific sales personnel and information disclosure to only the specific customers involved. I&A (moderate) is required to support the other security services.

## Orders

**Threats:** Information about orders may contain unique pricing arrangements with (medium) threat of disclosure and (medium) threat of loss or damage. The impact of disclosure is (significant) and of loss or damage is (mild)

**Security Services:** This ordering information requires confidentiality (moderate) and integrity (minimum) in storage and transfer. Access control (moderate) should limit access to specific customers, specific salespersons, specific sales managers, and any financial information users.

## Manufacturing/Vendors/Supplies

**Threats:** Information about products, inventories, requisitions, vendor and supplier contracts, production schedules, is threatened by disclosure (low) and loss or damage (medium). The impact of disclosure is (mild) and of loss or damage is (significant).

## UNCLASSIFIED

Appendix H, Annex B  
IATF Release 3.1—September 2002

**Security Services:** This information is in access (moderate) to authenticated customers (minimum) and XYZ employees. Confidentiality in transfer (minimum), and integrity in storage (moderate) is required.

### **Warehousing/Distribution/Transport**

**Threats:** Information about inventories of products, shipping schedules, carriers, transfers and disposals is threatened by loss or damage (low) but has (significant) impact on service to customers.

**Security Services:** This information is in access (moderate) to authenticated (minimum) customers, and XYZ employees. Integrity (moderate) in storage and transfer and confidentiality (minimum) in transfer is required.

### **Planning**

**Threats:** Information about planning for new products, new business areas, facility and equipment additions or modification, price changes, strategic account management, research, marketing initiatives is threatened by disclosure (low) but can have (significant) impacts through competitor knowledge.

**Security Services:** Access (moderate) to such information is to specifically involved XYZ personnel with confidentiality (moderate) and integrity (minimum) in storage and transfer. Sales personnel are permitted to release information to customers at planned release dates or events. This represents a change in policy for that information which is to be effected by the designated security administrators.

### **Finance and Accounting**

**Threats:** Financial information such as customer accounts receivable, accounts payable, general ledgers, financial reports, purchase orders, banking, payroll, commissions and bonuses, capital expenditures, and capital assets are considered to be threatened by disclosure (high) and loss or damage (medium). The impact of disclosure is (serious) and of loss or damage is (significant).

**Security Services:** This information is in access (strong) to specific finance personnel by information domain, to all auditors and XYZ business area and corporate officers as needed. Confidentiality (strong) and integrity (moderate) in storage and transfer is required. I&A required is (strong).

### **Human Resources/Personnel Administration**

**Threats:** Information about XYZ personnel which permits the administration of payroll and benefits, promotions, assignment of duties, and performance appraisals, is considered threatened by disclosure (medium) and by loss or damage. The impact of disclosure to anyone who does not specifically need to know is (serious). The impact of loss or damage is (significant).

**Security Services:** Access to this information must be (strong) to only those involved in personnel administration and to the specifically involved supervisory personnel. Confidentiality (strong) and integrity (strong) is required for storage and transfer of this information. I&A (strong) is necessary to support the other security services.

## Research

**Threats:** Information pertaining to new products, processes, capabilities, newly applied technologies, patents pending, and trade secrets are considered threatened by disclosure (medium) and by loss or damage (low).

**Security Services:** Access to this information should be (moderate) to the specific research personnel involved, business area managers, and financial budget managers. This information requires confidentiality (moderate) in storage and transfer.

## XYZ Corporate Relations

**Threats:** Information exchanged between corporate divisions of XYZ are threatened by loss or damage (low). The impact of such loss is (mild)

**Security Services:** Access (minimum) to this information should be to XYZ employees. Data integrity requirements are (minimum).

## Information Systems/Communications

**Threats:** XYZ sets high standards in service and product availability to its customers. Information systems are threatened by:

- Processing system failures: malfunctions, errors, deliberate destruction, inadequate performance
- Communications system failures: malfunction, errors, deliberate destruction, inadequate performance
- Application failures: errors, loss, corruption
- Information failure: errors, loss, corruption, spoofing

The probability of one or more of these events occurring is (high) and will result in the disclosure, loss, or damage to information. The impacts are (serious).

**Security Services:** The general application of measures for system integrity (moderate) and communications availability (moderate) including security management auditing, and preventive maintenance is required.

## Facilities Management

**Threats:** Facilities management information when associated with the security management function is threatened by loss or damage (medium). The reliability of electrical power systems, air conditioning, communications channels is a security issue. Information about power systems service providers and product repair services are examples of relevant data.

**Security Services:** Data integrity (minimum) of facilities management data must be maintained.

## Security Management

**Threats:** Implementation of policies and information needed to support the security services are at the core of any possibilities for information protection. Threats of disclosure and loss or damage are (high) and the impacts are (serious). Security management also involves physical security, administrative security, personnel security as well as the technical aspects of information security.

**Security Services:** This information requires integrity (strong) and confidentiality (strong) in storage and in transfer. Access control (strong) and the supporting I&A (strong) for specific security managers is required.

## 2.7 Security Management

Security management is a set of pervasive security mechanisms which support the security services by direct and supervisory administration, automated processes, and by the activities of all information users. CISOs and BISOs were identified and required in section 2.3. These security managers are to appoint other security managers as needed to support the implementation of XYZ information systems. Security managers are also responsible for informing all users of their responsibilities and requirements.

## 3.0 Policy Preparation Guidance

### 3.1 Overview

This section of the document provides guidance for the development of security policies for the major business areas and divisions of XYZ. All policies are to be derived from the XYZ Information Protection Policy found in Section II. The form of security policies varies with the purpose intended. The corporate level policy of Section II provides general rules for all elements of XYZ and directs the development of more specific policies as needed. Business area policies should be based on the specific functions and information management of each business. Business area policies are expected to apply the security services to the more definitive Business

IMMs. Policies installed in information systems tend to address the needs of smaller groups of users and to cover more categories of information. The concept of an information domain provides a means to implement a security policy that applies to specific users and specific information. The information domain is indivisible in policy, membership, and information objects. The information domain policy then is the ultimate objective in the preparation and implementation of formally and informally adopted policies.

## 3.2 Purpose

This guide describes the process that was used to develop the XYZ corporate policy and is to be used in the development of derivative policies.

## 3.3 Process

The major steps in policy development are:

- Determination of the major functions from a business analysis
- Preparation of an information management model (IMM) from the information management functions used to support the major business functions.
- Performance of a threat analysis based upon the intentions of adversaries to harm the business
- Revision of the IMM to enable the improved allocation of security services
- Allocation of security services to users, processes, databases, and information flows

Each of these steps are described in the following paragraphs assuming the XYZ Information Protection Policy as a baseline.

## 3.4 Business Analysis

Each business area is assumed to have the functions presented in section 2.7 and repeated here. They are:

- Core Business Functions
  - Marketing/sales
  - Customers/orders
  - Manufacturing/ Vendors/ supplies
  - Warehousing
  - Distribution/ transport
- Infrastructure Functions
  - Planning

- Finance and accounting
- Human resources/personnel administration
- Research
- XYZ Corporate relations
- Information systems/communications
- Facilities management
- [Security management]

It is worth repeating that the emphasis is on functions not organizations. It is unlikely that the two are well aligned. It is likely however that individual business areas may differ functionally from those given as the core and infrastructure sets. Any additions or deletions should be made at this step. The functions are the framework for modeling the information management and it is therefore important that the set is as complete as possible.

## 3.5 IMM preparation

For each of the functions it must now be determined if and how information management is used to support them. This part of the process begins with the identification of any **information** being recorded and stored on any kind of media including paper forms and logs, video, audio, as well as the typical computer storage media. Next, any **processes** which generate, transfer, transform, edit, or destroy the information records are identified. **Then the roles of any users** who manage other users, the processes, or the information records directly must be identified. Finally, the IMM is completed by identifying all **information flows** between users, processes, and information stores. In the C/IMM it was assumed, for example, that each business would have marketing information and that all salespersons, sales managers, and customers would have some form of access to that information. In any specific business area information, users, processes and flows can be identified more clearly.

## 3.6 Threat Analysis

In the C/IMM threats were postulated in section 2.8 for each of the core and infrastructure functions and their associated information management model elements. Threats must be traced from the causes for harm. The causes may be deliberate, accidental, or natural as the examples that follow illustrate.

### Sources of threats

- Competitors
- Foreign companies and governments
- Computer hackers, viruses
- Employees (errors, incompetence, inexperience, fraud, abuse, disgruntled)
- Service providers (errors, negative priorities)
- Product vendors (exaggerations, hidden defects)
- Natural disturbances, disasters, accidents

- Customers (greed, fraud, abuse)
- Miscreants (criminals, saboteurs)

Threats are categorized according to the probability of an attack or the occurrence of a harmful event. The probability metrics of high, medium, low, or none are adequate for most analyses. In the C/IMM, under sales for example, it was assumed that some customers may attempt with medium probability to obtain information about special pricing arrangements for other customers. Threats are mapped to the IMM leading to notions of protection of information stores, processes, information flows, and desirable user activities. Once threats are mapped to the IMM the identification of needed security services can be straightforward. However, the threat analysis may suggest that the restructuring of the IMM may improve the possible allocation of security services. For example, the separation of special customer prices from standard prices in a database makes the rules for access control to prices less complex. In addition, a second metric is needed to assist in the selection of security services. The degree of impact on business or a business function should be decided from the metrics of serious, significant, mild, or insignificant.

## 3.7 Security Services

Security services were defined in Section I. Security services are assigned strength metrics in section 2.8 of strong, moderate, minimum, and none. The choice of metric should be commensurate with the probability and impact of the successful execution of a threat. For example, a highly probable attack on information of insignificant value warrants none to minimum protection. When applied to the IMM the security services can be very specifically identified such as, data confidentiality and data integrity are to be applied to special pricing information while being transferred from storage to the authentically identified customer. The complete set of security services so identified and composed form the core of the security policy.

## 3.8 Coordination

The true worth of a security policy is realized when full coordination with and agreement by the community of users is achieved. Architects and implementers of information systems can proceed with a high degree of confidence that changes will be well controlled

Although not technically policy in the sense of protection requirements, the identification of **certifiers** and **accreditors** in the policy is recommended. Their involvement during the development and coordination phase of policy making will shorten the process and improve the results.

**UNCLASSIFIED**

Appendix H, Annex B  
IATF Release 3.1—September 2002

**This page intentionally left blank**

# **PNE Annex C: Division IPP**

---

[This annex to this document is an unedited (except for company name) example of an actual IPP.]

**XYZ CORPORATION**  
**Business Forms Division**

**Information Protection Policy**

*Establishes the policy of the Business Forms Division for the protection of information that is managed in the process of conducting its business.*

**UNCLASSIFIED**

Appendix H, Annex C  
IATF Release 3.1—September 2002

**This page intentionally left blank**

# 1.0 Introduction

## 1.1 Purpose

This document establishes the policy of the Business Forms Division for protecting information that is managed in the process of conducting its business. An Information Protection Policy (IPP) is the record of agreement between all parties as to what protection is required. The IPP is also the basis for guiding the development of information system security architectures, their implementation, and their management during operation.

## 1.2 Background

Policy of the Business Forms Division, a division of XYZ Corporation, is guided by corporate policy (Reference A, Section 1.3) and the procedures it defines. This policy is derived from corporate policy and from the Information Management Model (IMM) for Business Forms Division (Reference B, Section 1.3). The IMM identifies the information domains that must be implemented to support protection of business functions. Information domains are formed by organizing information, processes, and users and selecting the security services to be applied based on threats to business functions. Information domains, security services, and strengths of service are presented in this IPP.

## 1.3 References

- A. XYZ Corporation. Information Protection Policy, <date>.
- B. Business Forms Division. Information Management Model, <date>.
- C. ISO 7498-2, Information Processing Systems-Open Systems Interconnection—Basic Reference Model—Part 2—Security Architecture, February 1989 (CCITT Recommendation X.800)

## 1.4 Definitions

The definitions provided in Reference A are repeated here, with others, for convenience.

**Information:** Data elements or objects generated, transferred, stored, processed, and destroyed in the conduct of business functions.

**Users:** individuals or groups of people who are responsible for managing a portion of the business information. Users include those who employ or manage information systems.

## UNCLASSIFIED

Appendix H, Annex C  
IATF Release 3.1—September 2002

**Processes:** the functions performed by users or users aided by information systems which generate, transform, modify, collect, organize, present, and destroy information.

**Information Management Model (IMM):** a logical description of information management which depicts the users, processes, databases, and information flows which support a business enterprise.

**Information Domain:** a security entity composed of three elements:

- 1) identifiable information objects
- 2) membership of identifiable users
- 3) a security policy which defines the relationships between each member and all of the information objects.

**Information Domain Member:** a user identified to have some responsibilities or privileges in the management of the objects of an information domain

**Security Policy:** rules which govern and identify the relationships between members and the objects of an information domain.

**Security Services:** activities that assist in, or provide for, the protection of information. Security services are provided by security mechanisms. Security mechanisms are diverse and include such things as guards, fences, cryptographic software, badges, or labels. The security services defined here are mutually supporting and often overlapping in the services provided. Although the definitions are provided in terms of people as individuals, they apply to groups, processes, and other agents or objects. These security service definitions are based on those defined by international standards (Ref. C)

**Identification and Authentication (I&A):** The service which protects against the claims of individuals to be someone they are not. Identification is the establishment of the unique identity of an individual, group, or information system component. Authentication is the means for verifying the claimed identity.

**Access Control:** The service which protects information through the control of authorizations of individuals for knowledge or rights of manipulation.

**Confidentiality:** The service that protects information from knowledge or disclosure.

**Integrity:** The service that protects information from modification, damage, or loss.

**Availability:** The service that protects the individual from accidental or deliberate denial of access to information and other services.

**Non-repudiation:** The service which provides protection from an individual denying sending information (non-repudiation with proof of origin), or protection from an individual denying

receiving information (non-repudiation with proof of delivery). These services are closely related to signing and notarization.

## **2.0 General Policy**

### **2.1 Overview**

This section of the IPP contains the general requirements for the protection of information by Business Forms Division and by those individuals and organizations involved in sharing information with the division. Specific requirements imposed by the security services of information domains are presented in section III and is summarized as a composite information domains database in Annex A. This type of policy is independent of implementation and its stated requirements may be satisfied by combinations of environmental, procedural, and technical (hardware, software, etc.) security mechanisms. The selection of mechanisms is accomplished by security architects and implementers of the information systems.

This IPP also defines the administrative procedures and responsibilities necessary to assure its implementation and to manage changes and additions.

The development of the IMM and this IPP were accomplished with the knowledge of several important business policies of the XYZ Corporation and Business Forms Division. Service to customers is the paramount objective and that demands high availability of information systems and the information needed to serve. This involves access to information about the status of some processes internal to the division. Protection of customer and Business Forms Division proprietary information from disclosure is a serious concern. Finance and accounting and personnel information are fundamentally protected with high priority.

### **2.2 Applicability**

The interests of Business Forms Division extend beyond its own employees and assets to customers, vendors, suppliers, other XYZ divisions, financial institutions, and to XYZ Corporation. This IPP is applicable directly to users of information systems and assets of Business Forms Division and indirectly through other policies that are developed in accordance with its procedures. Agreements for information protection with entities external to the division, expressed or implied, must be consistent with the requirements of this IPP. Other Business Forms Division security or information protection policies existing prior to this IPP must be replaced or brought into agreement with this IPP.

### **2.3 Responsibilities**

The Business Information Security Officer (BISO) shall be responsible for the preparation, maintenance, administration, and implementation of this IPP. The (Division Executive e.g.) shall appoint the BISO considering the XYZ employees recommended by the Corporate

## UNCLASSIFIED

Appendix H, Annex C  
IATF Release 3.1—September 2002

Information Security Officer (CISO). The BISO shall insure that the Business Forms Division IPP is consistent with the XYZ Corporation IPP. The BISO shall appoint Information Security Officers (ISO), as needed, to manage the policies and implementations of the major information domains.

The ISOs are the security managers of information domains. They shall initialize and maintain users privileges and support the required security mechanisms. ISOs may manage more than one information domain but the BISO should isolate the management of the most sensitive domains for better security. The BISO and ISOs shall coordinate with other security administrators, e.g. security guards and personnel investigators, as part of their total security management implementation.

All Business Forms Division employees have some responsibility in protecting business information. Users of information must be made aware of information protection policies and must be informed of their responsibilities in meeting the policy requirements for any information that they manage.

In establishing relationships with customers, vendors, suppliers, and other external organizations, policies for the entrusted sharing of information shall be applied or developed. The BISO shall approve all policies applied or developed for use involving external organizations. All such policies must become part of the IPP by inclusion or by reference.

## 2.4 Procedures

Security policies vary in their formality depending upon the scope or the number of people involved. A corporate security policy, for example, needs wide dissemination and coordination with many individuals and with all business divisions. Changes require similar efforts to accomplish. Formal processing of such a policy is a necessity. The XYZ Corporation IPP provides guidance for the preparation of such policies. Perhaps the simplest form of policy is when an individual employee prepares information such as a drafted document which for a time is accessible only by the preparer. This event is the formation of an information domain with a single member who accepts that the protection of the environment and the information system utilized is adequate. The employee is the certifier and accreditor of the system and this policy may be simply implied. All security policies should be reviewed periodically for continued need. Any changes in environment or systems should be evaluated by the certifiers and accreditors for adequacy of protection.

Information protection shall be considered in the planning, development, and use of all Business Forms Division information systems. This applies to stand alone (including personal) computers as well as computer networks. Users of information systems must be made aware and must observe the requirements for the protection, i.e. policy, for any information managed by them on such systems.

Information protection shall be considered as part of all contractual agreements. All parties to contracting with suppliers or customers, for example, must consider the necessity for preparing and including a security policy as part of the contract.

Circumstances will sometimes create the need to circumvent normal protection mechanisms. For example, the release of information to non-members of an information domain may be required in an emergency. The appropriate method for dealing with such contingencies is to decide who is permitted to override protection mechanisms and who will audit such activities. These are examples of the possible roles for security administrators. Such contingencies can and should be addressed in information protection policies.

## 2.5 Certification and Accreditation

Information systems which are intended to implement and satisfy information protection policies must be certified and accredited. Certification is the process of security evaluation and reporting on the adequacy of a system to meet the requirements of a policy. Accreditation is the process of approval and operational acceptance of a system which includes security. Accreditors evaluate the effectiveness of their information systems in meeting business objectives and the adequacy of its system management. Certification and Accreditation of information systems become increasingly important as the number of users, computers, and facilities implementing the system become larger. Formal certification is normally accomplished by expert security analysts. The certifier, with knowledge of the security policy, evaluates the total effectiveness of system security mechanisms and prepares a certification report. The report may recommend system acceptance or it may cite deficiencies which must be mitigated or eliminated prior to acceptance. Formal accreditation is normally accomplished by those who prepared the original operational requirements. The accreditor makes the critical decision to accept or reject a system and to permit its operational use.

The BISO shall select system evaluators and shall be responsible for defining and managing the certification and accreditation processes. Accreditation is the responsibility of the operational organization. The BISO shall certify all Business Forms Division information systems.

## 3.0 Information Domain Policies

### 3.1 General

All users of Business Forms Division must be made aware of their participation in any information domain for the purpose of understanding their responsibilities. Users who retain authentication information must be made aware of their responsibilities for its protection.

**Annex A** summarizes the information domains defined in the Business Forms Division IMM. The IMM specifies the rules for access and permissible processes for the various users. It also

summarizes the relevant threats, their potential and impact, as well as security services and strengths required by the information domains. Any other specific requirements or explanations are provided, by information domain, in the succeeding paragraphs.

The security services and strengths apply to information in use, storage, and in transfer. Security architects and security evaluators shall include mechanisms for availability, integrity, and non-disclosure for information in all of those states, as appropriate.

## 3.2 Systems Entry

### **INFORMATION DOMAIN: System Entry**

Unidentified users may choose between inquiring about products and services or entering the Order process with a customer identification (which includes, new customer). General Business Forms Division information about products, pricing, available inventory, and services is provided to “Potential Customers” through the Marketing and Warehousing processes.

## 3.3 Order Process

### **INFORMATION DOMAIN: Customer Identification**

Unidentified users, may enter customer identification information for the purpose of building a new customer profile, referencing an existing customer profile, placing orders, creating new forms design, reviewing or adjusting orders, or inquiring about products and services. Identification is by one of several submitted items including customer name or telephone number. The expected users are potential customers, customers, sales representatives, account managers, or sales managers, but the user’s identification is not required. This order process domain performs a context switch to the appropriate order process domain, based on the identification information provided.

### **INFORMATION DOMAIN: Customer Information and Order Management (one/customer)**

**New Profile:** Information from customer identification is used to determine if a customer profile exists or if a new profile needs to be generated. If a profile does not exist the unidentified user can create a profile by supplying the required customer information. Completion of the customer information part of the new profile will initialize the generation of authentication data for the customer and identify/assign the customer’s sales representative. The unidentified user is assigned the privileges of the identified new customer. All user activities are restricted to the new account of the identified customer. When the customer enters the order process on subsequent accesses, they will identify themselves with the appropriate customer account information, and be authenticated as a valid user of the existing profile.

**Existing Profile:** If a user wishes to review or adjust information in an existing profile or perform ordering functions, customer identification information must be provided first, followed

by the completion of user identification and authentication (I&A). This establishes the user's privileges in profile management and ordering within the customer account. Successful user I&A permits the customer, the assigned sales representative, and any account manager to modify the customer profile, enter orders, adjust orders, and activate orders. Warehouse, manufacturing, and finance employees can view this part of the customer profile and ordering data but cannot create or modify information in this information domain.

#### **INFORMATION DOMAIN: Customer Pricing**

**Pricing Agreements:** The customer's sales representatives, the specific account manager, and designated finance employees may establish unique pricing agreements between Business Forms Division and a customer. These pricing agreements are only disclosed to those users.

**Order Price Quotes:** The customer's sales representative, the specific account manager, and designated finance employees may establish prices for products and services requested in an order. The customer and designated warehouse and manufacturing employees may view this information. Order pricing is only disclosed to those users.

#### **INFORMATION DOMAIN: Customer Order Credit Approval**

Information about the approval for customer credit on each order is provided by designated finance employees. The customer may not access this credit information.

#### **INFORMATION DOMAIN: New Forms Design**

New forms may be designed by customers and others and be filed in customer specific files. This domain is separated from the customer information and order management domain because it allows a manufacturing design engineer read and write access to the new form information, to assist in its final fabrication, before entering the manufacturing order processing and production processes.

## **3.4 Manufacturing**

Manufacturing provides the production and distribution of Business Forms Division forms products. The manufacturing process is composed of six information domains.

#### **INFORMATION DOMAIN: Standard Items Update**

Operations and Production employees maintain records of general product catalog items produced and shipped to warehouses.

#### **INFORMATION DOMAIN: Customer Orders**

Operations and Production employees maintain records of production against customer orders. This includes requests to manufacturing for new forms design. Records are viewable by many

## UNCLASSIFIED

Appendix H, Annex C  
IATF Release 3.1—September 2002

who need to see them but the records are kept one per customer, to limit access to the account to which the order information belongs.

### **INFORMATION DOMAIN: Raw Materials**

Operations and Production employees maintain records about ordering, receiving, and inventory of raw materials used for forms production.

### **INFORMATION DOMAIN: Distribution**

Production employees maintain records about carriers and warehouses.

### **INFORMATION DOMAIN: Design**

Design engineers place new general product form designs into the general catalog.

### **INFORMATION DOMAIN: Production Control**

Users manage the manufacturing process runs.

## **3.5 Warehouse**

The warehousing process is divided into five information domains. Three of the domains are created to maintain separation of different types of inventories. The other two deal with warehouse accounting management (shipping, receiving invoice management, notifications, etc.) and independent inventory audits that provide accounting oversight of the Business Forms Division warehousing process.

### **INFORMATION DOMAIN: Internal Use Products Inventory**

The internal use products inventory is an ongoing storage record of manufacturing raw materials, facilities management office supplies and utilities parts and components, and IS/Comm management spare parts and system components, where such items are maintained in a Business Forms Division managed warehouse. Only valid and verified manufacturing, facilities management, IS/Comm management employees, and warehouse employees may read this information. Only warehouse stock movement employees may update this information.

### **INFORMATION DOMAIN: Customer Products Inventory**

The customer products inventory is maintained on a account basis (1 domain per customer) and provides the product items the customer has stocked in the warehouse at any point in time. Only the customer and those Business Forms Division employees representing the customer, and warehouse employees may read this information. Only warehouse stock movement employees may update this information.

### **INFORMATION DOMAIN: General Products Inventory**

The general products inventory is maintained on a general catalog products basis (no specific customer ownership) and provides the product items available to any customer or potential customer which is stored in the warehouse at any point in time. Anyone may read this information. Only warehouse stock movement employees may update this information. Inventory which is “earmarked” for outgoing customer shipment is not included in the available inventory quantities.

#### **INFORMATION DOMAIN: Warehouse Accounting**

The warehouse accounting domain processes all incoming and outgoing invoices and all incoming customer orders which get transformed and referenced in outgoing invoices, and warehouse status information about customer orders. This domain also issues notification to finance & accounting (AR) about customer order shipments, for billing and collection and for credit memo generation for customer returned products, and (AP) about the receiving of internal XYZ products shipped to the warehouse by suppliers. Any valid and verified XYZ employee may be granted authorization to read this information. Customers may read the information related to their account. Only authorized warehouse employees may write this information.

Where internal stock items are shipped directly to the Business Forms Division organization that ordered the items, vice going to warehouse inventory, then the ordering organization is responsible for the accounting management of such items, including notification of delivery to finance and accounting (AP). Where customer orders are filled, invoiced, and shipped directly to the customer by the manufacturing process, vice going to warehouse inventory for later shipping to customer, then the manufacturing organization is responsible for the accounting management of such items, including the notification of shipping to finance and account (AR).

#### **INFORMATION DOMAIN: Inventory Audit**

The inventory audit domain processes independent warehouse inventory counts and invoice reviews to ensure the integrity of warehouse management, and reconciles or instigates an investigation of unbalanced records and stock item counts. Only internal and/or external independent inventory audit personnel may read and write this information. Only warehouse management personnel, and Business Forms Division and corporate executives may read this information.

## **3.6 Business Planning**

#### **INFORMATION DOMAIN: Business Plans**

The users in this domain are Business Forms Division’s Executives, their staffs, and sales, manufacturing and financial managers. Only the executives and their staffs are allowed to create modify or destroy the information objects. Although the impact of loss of this strategic information is considered significant the threat to the loss or damage of the information is considered low. Moderate access control must be used to restrict the information to the

executives and senior managers. There are moderate confidentiality and minimal integrity requirements in both storage and transport of this information.

## 3.7 Marketing

### **INFORMATION DOMAIN: Promotion**

Sales managers and analysts maintain product catalogs and price information which are available to the general public as potential customers. This domain also includes promotional brochures and other forms of advertising (web pages?). The accessibility of this information is both desirable and threatening. Care must be taken to provide adequate separation for the protection of other domains. The access rules here indicate that unidentified users may view this information but any authenticated sales managers or analysts may prepare it.

### **INFORMATION DOMAIN: Customer (one/customer)**

The customer's sales representative or any sales analyst may record information about the customer's history or preferences as part of the customer profile. This domain also includes any unique pricing or buying agreements. The customer and any sales manager may view this record.

### **INFORMATION DOMAIN: Strategy**

Sales managers and analysts maintain marketing management and planning information to include establishing price ranges to be used in quoting prices for orders. This is a marketing user only domain except that division executives can view the information.

### **INFORMATION DOMAIN: Sales**

Sales analysts maintain statistics on a per customer basis which will indicate sales performance.

## 3.8 Finance and Accounting

### **INFORMATION DOMAIN: Management**

Financial managers and designated employees manage the division's finances. Posting to the general ledger involves transfers of information from the other finance domains. Inter-domain transfers require that transfer policies exist in each pair of domains involved in the transfer and that the user has the privilege to do it.

### **INFORMATION DOMAIN: Customer (one/ customer)**

Finance employees maintain credit and payment records, against accounts receivable, by customer. This information is available to the customer's sales representative and sales manager.

**INFORMATION DOMAIN: Deliveries**

Finance, warehouse, and manufacturing employees post accounts receivable by virtue of their deliveries.

**INFORMATION DOMAIN: Expenditures**

All employees who may obligate the division post expenditures.

**INFORMATION DOMAIN: Payroll**

Records of payroll disbursements, commissions and bonuses are kept by finance employees. This information is available to Human Resources personnel.

## 3.9 Personnel

**INFORMATION DOMAIN: Personnel: Employee-H/R Managed**

This is a set of domains; one per employee. The users of the domain are the specific employee, H/R personnel and financial personnel. The domain contains sensitive information about a specific employee. The domain requires strong identification and authentication and access control to insure that only the users of the domain have access to the information and to insure the integrity of the information by establishing and controlling the user's privileges. There are two processes that run in this domain; manage employee records and payroll processing. The payroll process is limited to financial personnel and can only read the information. Manage employee records is limited to the specific employee and H/R personnel where only H/R personnel can create, modify or destroy the information objects. There are strong confidentiality and integrity requirements for the information objects during storage and transportation.

**INFORMATION DOMAIN: Personnel: Employee Managed Records and Payroll**

This is a set of domains; one per employee. The users of the domain are the specific employee, H/R personnel and financial personnel. The domain contains sensitive information about a specific employee. The domain requires strong identification and authentication and access control to insure that only the users of the domain have access to the information and to insure the integrity of the information by establishing and controlling the user's privileges. There are two processes that run in this domain; manage employee records and payroll processing. The payroll processing is limited to financial personnel and can only read the information. Manage employee records is restricted to the specific employee and H/R personnel where both the specific employee and H/R personnel can create modify or destroy the information objects. There are strong confidentiality and integrity requirements for the information objects during storage and transportation.

## UNCLASSIFIED

Appendix H, Annex C  
IATF Release 3.1—September 2002

### **INFORMATION DOMAIN: Personnel: H/R Management**

The information in this domain is accessible to all XYZ employees. However the integrity of the information must be strongly protected. Therefore the domain requires strong identification and authentication of H/R personnel before they are allowed to create modify or destroy the information objects. There is a strong integrity requirement for the information objects during storage and transportation.

### **INFORMATION DOMAIN: Personnel: Division Policy**

The information in this domain is accessible to all XYZ employees. However, the integrity of the information must be strongly protected. Therefore the domain requires strong identification and authentication of Business Forms Division Executives before they are allowed to create modify or destroy the information objects. There is a strong integrity requirement for the information objects during storage and transportation.

## **3.10 Information Systems and Communications**

The information systems (IS) and communications management infrastructure process is composed of eleven information domains. Here, IS and communications management functions have been separated on purpose, to maintain integrity of these two major infrastructure processes, although in reality they may be managed as (or at least by) a single Business Forms Division entity. The IS process includes management, maintenance, trouble reporting, and applications management domains. The communications process includes management, maintenance, and trouble reporting domains. Jointly coupled IS/Comm domains include capital equipment inventory control, system planning, system integration activities and information, and contracts management.

### **INFORMATION DOMAIN: IS Management**

The IS management information domain is very broad based. It includes all major system management activities necessary to configure, account for and operate Business Forms Division end system components (workstations, servers, mainframes, telephones, fax machines, etc.). Users of this domain are IS managers and operators. Overall system administration is maintained and controlled by this domain.

### **INFORMATION DOMAIN: IS Maintenance**

The IS maintenance domain provides the information and processes to maintain and control routine and specific end system preventative maintenance functions. IS operators and maintenance personnel (including contract maintenance personnel) are the users of this domain.

**INFORMATION DOMAIN: IS Trouble Reporting**

The IS trouble reporting domain provides the process and information for users to reports problems and get those problems resolved. Users may report problems and request assistance via telephone, person to person, or electronic mail. User may read problem resolution information. Only IS help desk personnel may read and write the information in this domain.

**INFORMATION DOMAIN: Applications**

The applications management domain provides the process and information to initialize and modify application specific parameter information. This domain includes specific server data base maintenance functions. Only applications management and maintenance personnel may read and write application management information. They directly support the primary users of the specific applications (e.g., ABC and DEF Business Forms Division applications).

**INFORMATION DOMAIN: Communications Management**

The communications management domain includes all major local and wide area communications management activities necessary to monitor, configure, account for and trouble shoot problem origin for Business Forms Division communication relay system components. Users of this domain are IS/Comm managers and communication operators/tech controllers, who are allowed to both read and write information objects in this domain. Overall communications administration is maintained and controlled by this domain.

**INFORMATION DOMAIN: Communications Maintenance**

The communications maintenance domain provides the information and processes to maintain and control routine and specific communications component preventative maintenance functions. Communications operators/tech controllers and maintenance personnel (including contract maintenance personnel) are the users of this domain.

**INFORMATION DOMAIN: Communications Trouble Reporting**

The communications trouble reporting domain provides the process and information for users to report communication problems and get those problems resolved. Users may report problems and request assistance via telephone, person to person, or electronic mail. All users may read problem resolution information. Only communications help desk personnel may read and write the information in this domain.

**INFORMATION DOMAIN: Inventory**

The inventory domain is used to maintain an accurate IS/Comm record of hardware and software and spare parts capital equipment (owned) and leased equipment, which is managed by IS/Comm. It may or may not contain IS/Comm inventory maintained in the warehouse, if such equipment (e.g., spares and transition components) are to be stored in one or more XYZ warehouses. IS/Comm managers, optionally IS/Comm outsource contractors, and both Business Forms Division and corporate executives may read this information. One or more assigned

## UNCLASSIFIED

Appendix H, Annex C  
IATF Release 3.1—September 2002

capital equipment administrators are the only ones who may read and write (maintain) this information. This record is maintained for finance and accounting tax purposes and asset accounting purposes. This record is subject to periodic F&A audits.

### **INFORMATION DOMAIN: Planning**

The planning domain is used to maintain an accurate IS/Comm record of planning information. This domain may contain information such as engineering plans, concept of operations documents, transition plans, development schedules, procurement plans, etc. IS/Comm managers and their staff have read and write access to this information. All other users, defined by IS/Comm management, have read access to this information.

### **INFORMATION DOMAIN: Integration**

The integration domain is used by the IS/Comm management staff to coordinate and oversee all information system and communication integration efforts. It includes integration planning documents, schedules, testing documents, procured equipment invoices, etc. related to any ongoing, planned, or past/archived integration activity.

### **INFORMATION DOMAIN: Contracts**

The contracts domain is used to guide, direct, monitor, instill adjustments to, and maintain status information on all IS/Comm contracts to Business Forms Division and/or other XYZ divisions as may be appropriate from time to time. IS/Comm contract managers and an assigned finance and accounting representative and manager have read and write access to the contracts information in this domain. Others, authorized by the IS/Comm manager are allowed read access to this information. There is a separate contracts domain for each contractor utilized by Business Forms Division.

## **3.11 Facilities Management**

### **INFORMATION DOMAIN: Office Supplies**

The office supplies domain is used by either an office manager or an administrator assigned by an office manager to maintain an inventory of office supplies used by the office. The manager or designated administrator orders supplies, may maintain an inventory of supplies in the warehouse, or at the local facility where the office resides. The manager or administrator notifies finance and accounting about supplier purchase orders and invoice receipt of received goods from suppliers if the inventory is maintained by the office. If the inventory is maintained by the warehouse, then the warehouse notifies finance and accounting about received goods and the cost. Any office employee may read the inventory or order information. The manager and/or designated administrator is the only one(s) who may write this information.

**INFORMATION DOMAIN: Facilities and Utilities**

The facilities and utilities domain provides the processes and information to account for facilities maintenance, outages, improvements, and utility cost monitoring. The facility manager or one or more designated facilities management employees may write this information. Any Business Forms Division employee may read this information.

## 3.12 Corporate Relations

**INFORMATION DOMAIN: Corporate Reporting**

The users in this domain are Business Forms Division and XYZ Corporate Executives and their staffs. This is reporting information that can be created modified and destroyed by Business Forms Division and executives and their staffs. There are minimum protection requirements for this information in storage and transfer. And minimal access control, and identification and authentication to protect the integrity of the information.

## 3.13 Security Management

The security management process is comprised of three different domain types: systems, mechanisms, and information domains. The international standard terminology for such information is the Security Management Information Base (SMIB). The SMIB is divided into the three types of domains.

**INFORMATION DOMAIN: Systems**

Each information end system or relay system contains protected information objects which are initialized and maintained by either an ISO or a designated system security manager (SSM). These managed objects may be managed locally or remotely. They include information which establishes and maintains information domains users and policies which are allocated to system level management.

**INFORMATION DOMAIN: Mechanisms**

Some security mechanism require individual support information which must be separated from any other security management for high protection. This includes e.g. cryptographic key material or mechanism attributes. This part of the SMIB may be managed by ISOs or SSMs.

**INFORMATION DOMAIN: Domains**

Each information domain requires a security management domain which contains its membership and policy. This domain may be managed at the system level by the SSM or in a separate domain which is managed by individual members of the domain or by ISOs.

**UNCLASSIFIED**

Appendix H, Annex C  
IATF Release 3.1—September 2002

**This page intentionally left blank**