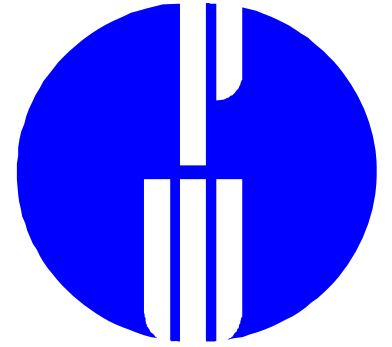
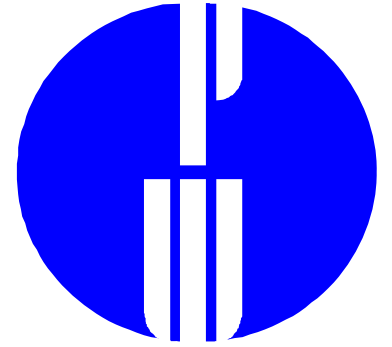


Security Through Process Management



"It's just the way we do things here."

POLICY



A POLICY PROCESS SHOULD:

- ▲ PROVIDE A SECURITY POLICY, to include:
 - scope
 - objectives
 - accountability
 - minimum requirements
 - consequences of non-compliance
- ▲ INVOLVE EXECUTIVE MANAGEMENT
- ▲ UPDATE POLICY FREQUENTLY

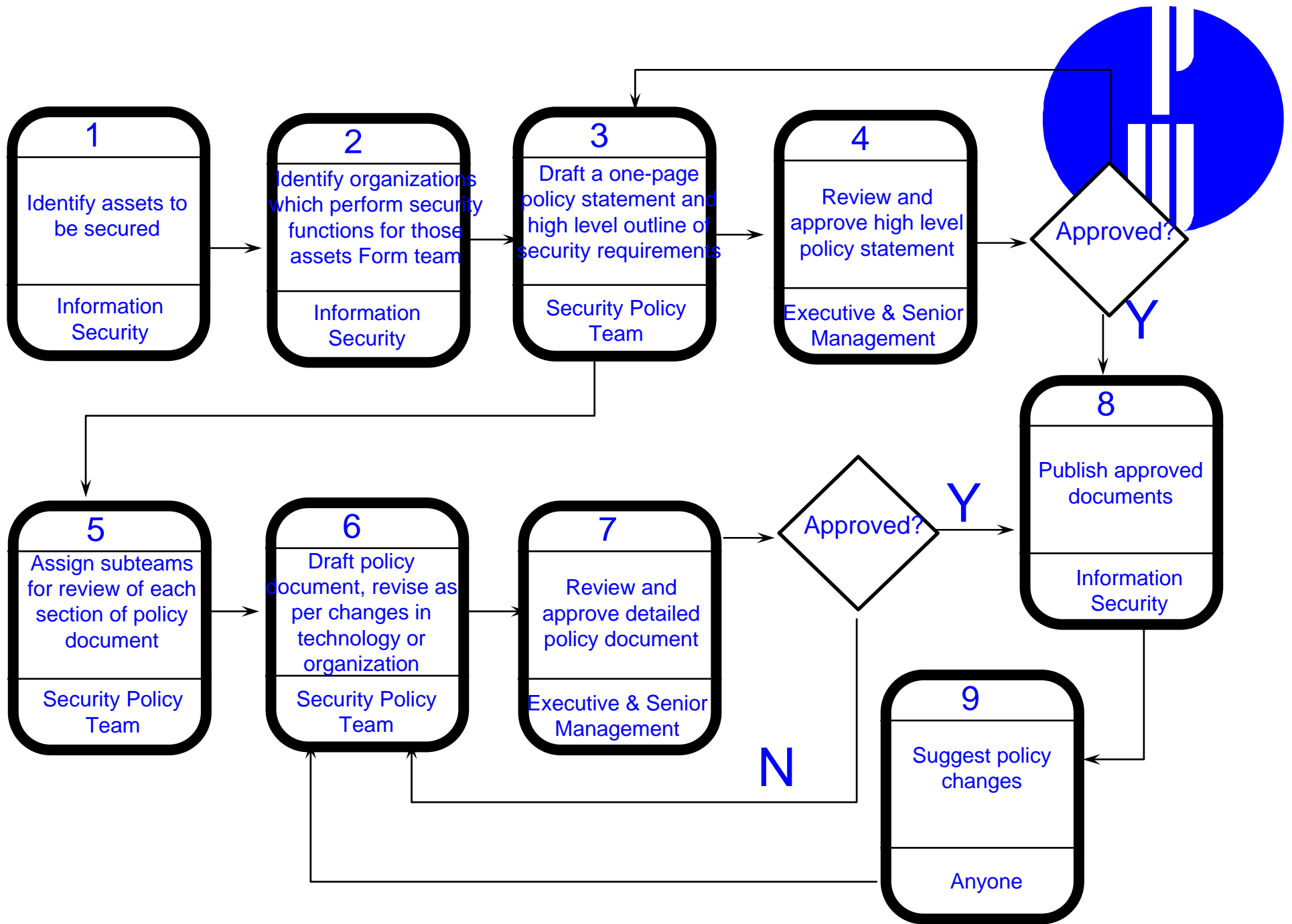
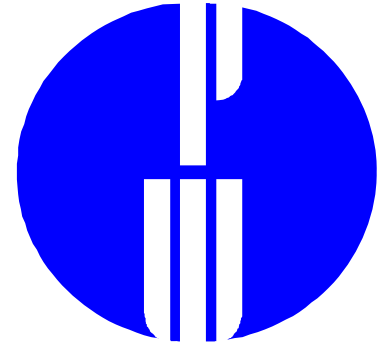
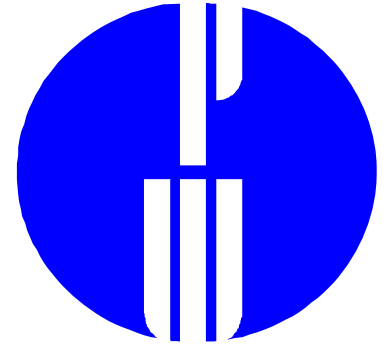


Figure 1: Example Policy Process



"That policy book? I think it's only for corporate. It doesn't apply here."



AWARENESS

AN AWARENESS PROCESS SHOULD:

- ▲ **PROVIDE AN AWARENESS PROGRAM, to:**
 - point out risks of non-compliance
 - teach security techniques
- ▲ **RECRUIT DEPARTMENT LIAISONS, to:**
 - distribute policy
 - facilitate awareness program activities
- ▲ **INVOLVE EXECUTIVE MANAGEMENT**

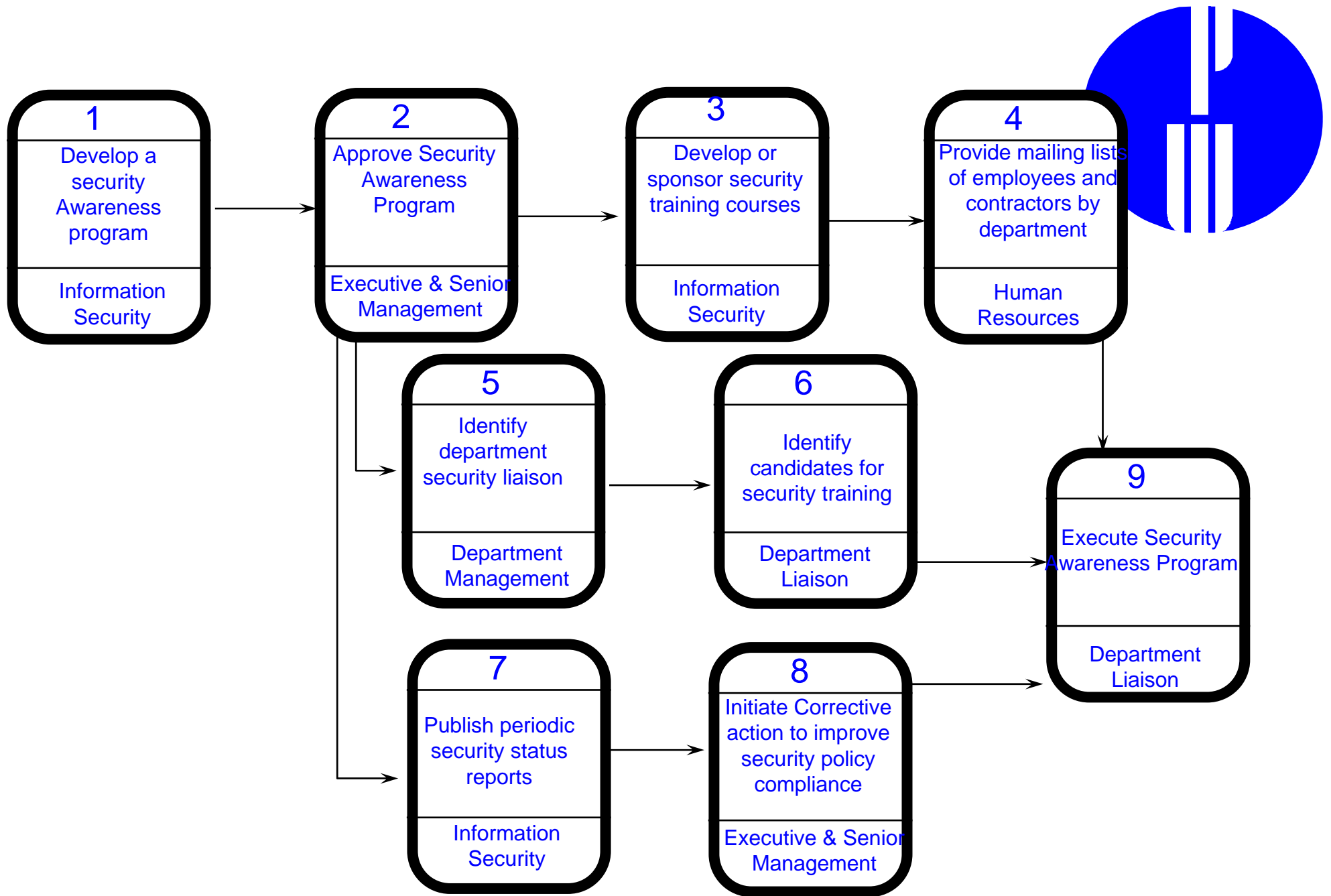
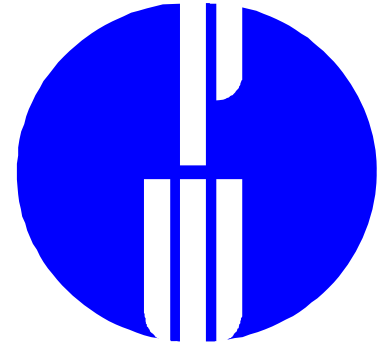


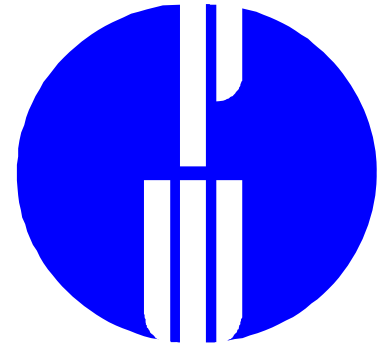
Figure 2: Example Awareness Process



"They are supposed to tell us when people quit, but they never do."

"We send a memo to their secretary. We have all the copies!"

ACCESS



AN ACCESS PROCESS SHOULD ADDRESS:

- ▲ IDENTIFICATION OF THOSE REQUIRING ACCESS
- ▲ AUTHORIZATION PROCEDURES FOR ACCESS
- ▲ AUTOMATIC AUTHORIZATION OF THOSE IDENTIFIED & AUTHORIZED FOR ACCESS
- ▲ SEPARATION OF DUTIES BETWEEN AUTHORIZATION & AUTHENTICATION
- ▲ SEPARATION OF ACCESS ENVIRONMENTS FOR KEY USER COMMUNITIES

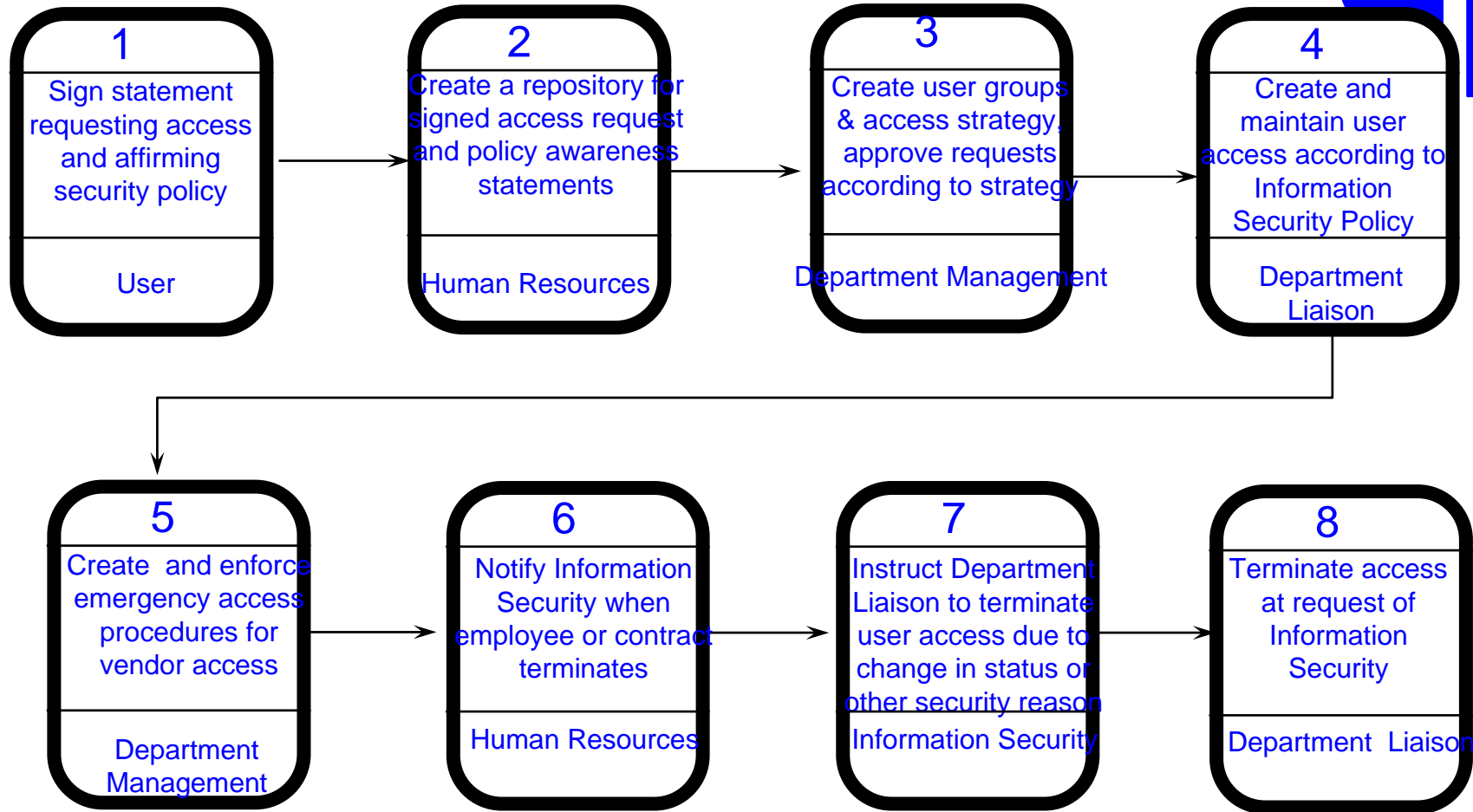
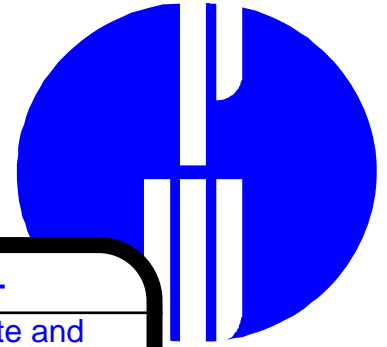
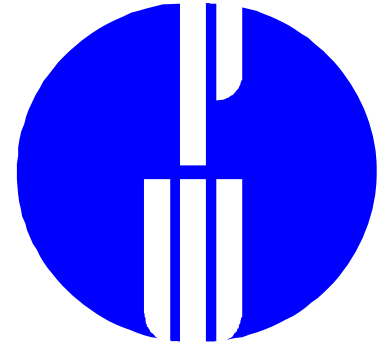
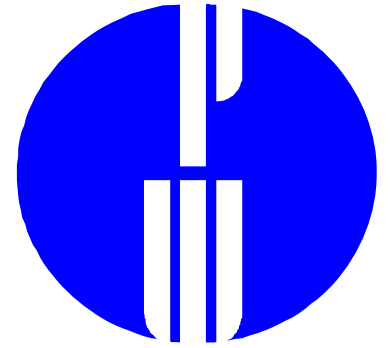


Figure 3: Example Access Process



"We log everything, but we only look at it if there's a problem."

MONITORING



A MONITORING PROCESS SHOULD:

- ▲ CONFIGURE SYSTEM SECURITY PROFILES
- ▲ FREQUENTLY REVIEW SECURITY LOGS
- ▲ IDENTIFY THE ROOT CAUSE OF SECURITY ALERTS
- ▲ FREQUENTLY UPDATE SECURITY PROFILES

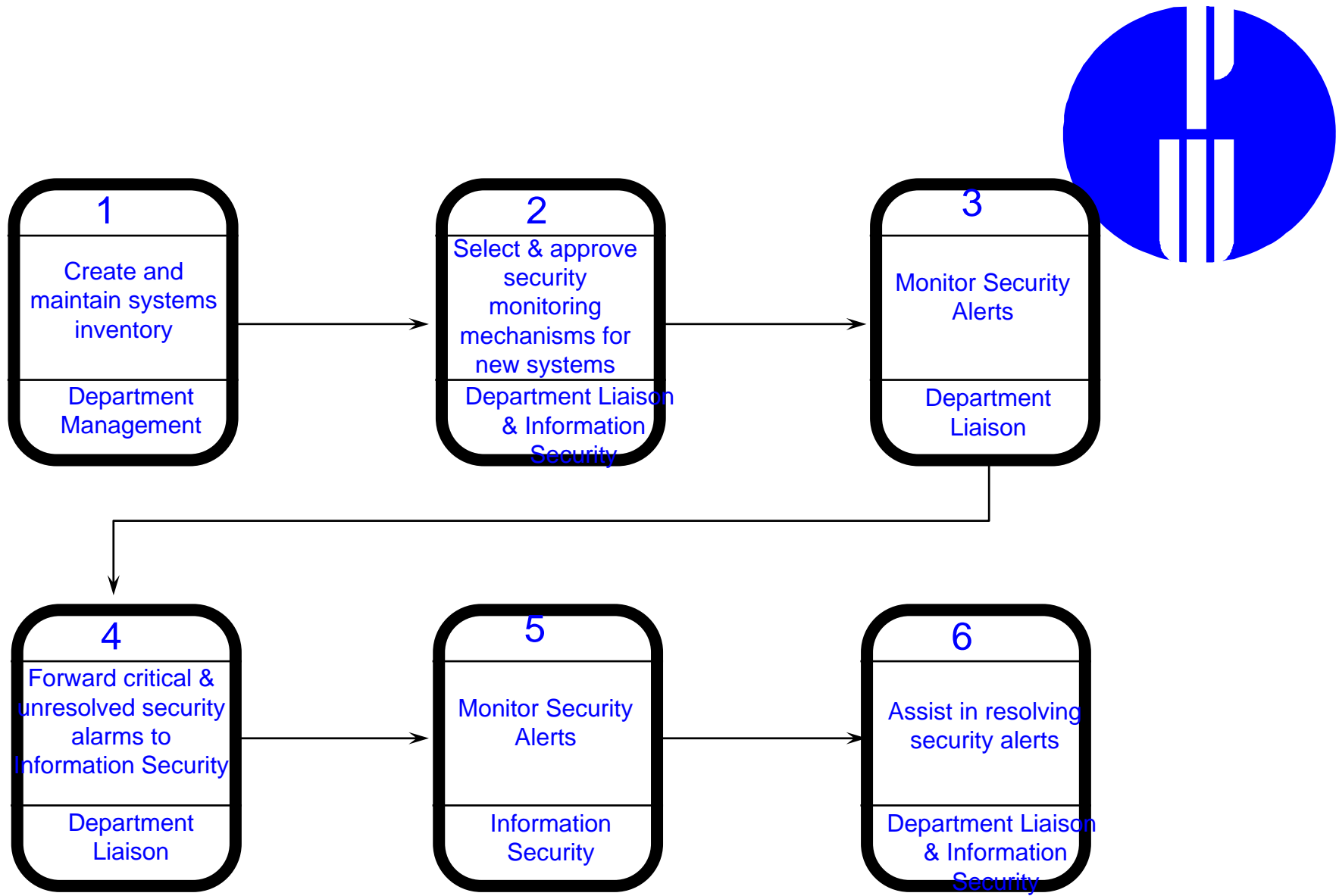
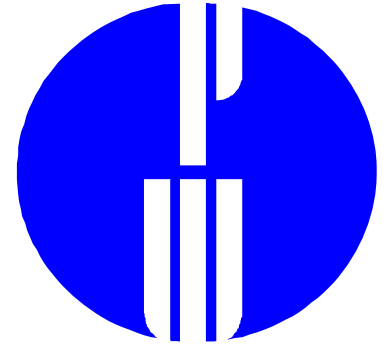
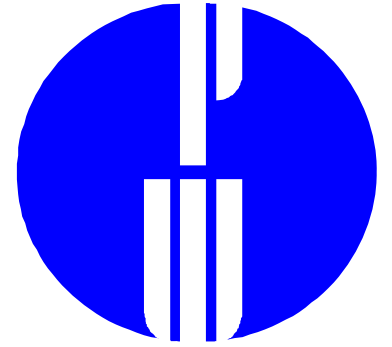


Figure 4: Example Monitoring Process



"We know we have security problems, we just don't have the resources to fix them."

COMPLIANCE



A COMPLIANCE PROCESS SHOULD ENSURE THAT INSTANCES OF NON-COMPLIANCE WITH SECURITY POLICY ARE:

- ▲ REPORTED TO INFORMATION SECURITY
- ▲ ASSIGNED TO APPROPRIATE MANAGEMENT
- ▲ SUPPORTED BY RISK ACCEPTANCE UNTIL RESOLVED

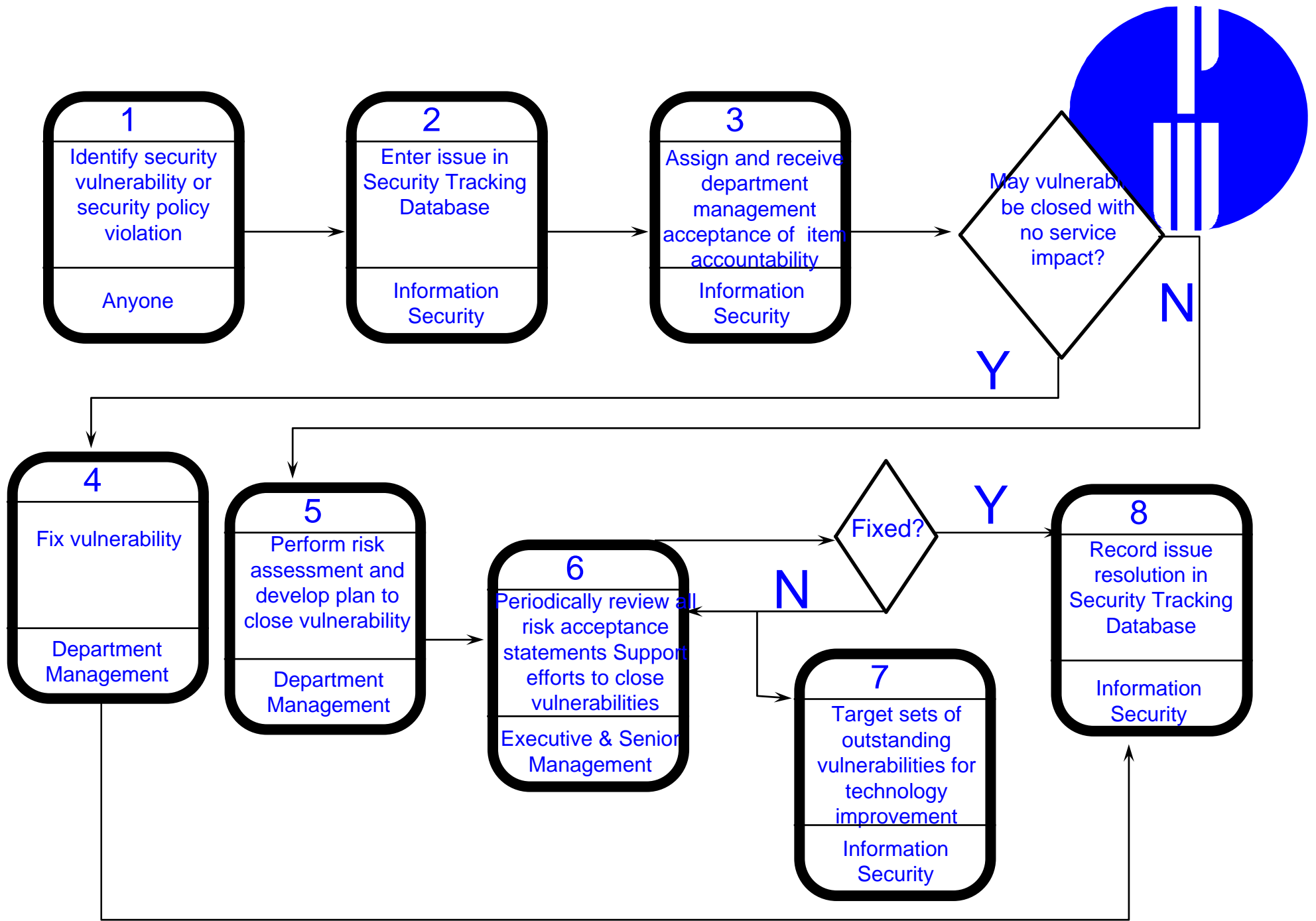
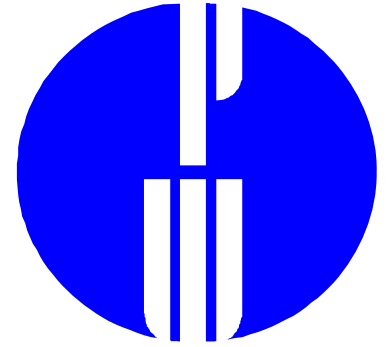
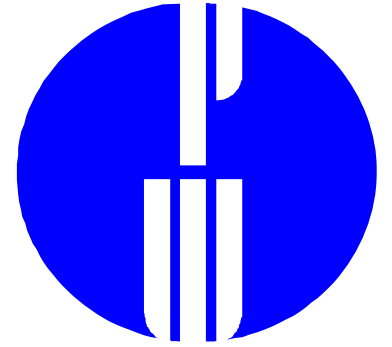


Figure 5: Example Compliance Process



"We had a very short time to get this into production."

STRATEGY



A STRATEGY PROCESS SHOULD:

- ▲ ENSURE SECURITY MECHANISMS ARE IN BUSINESS CASES & BUDGETS
- ▲ REVIEW & TEST NEW SECURITY TOOLS & TECHNIQUES
- ▲ DEVELOP METHODS TO QUANTIFY LEVELS OF RISK IN NEW DEPLOYMENTS

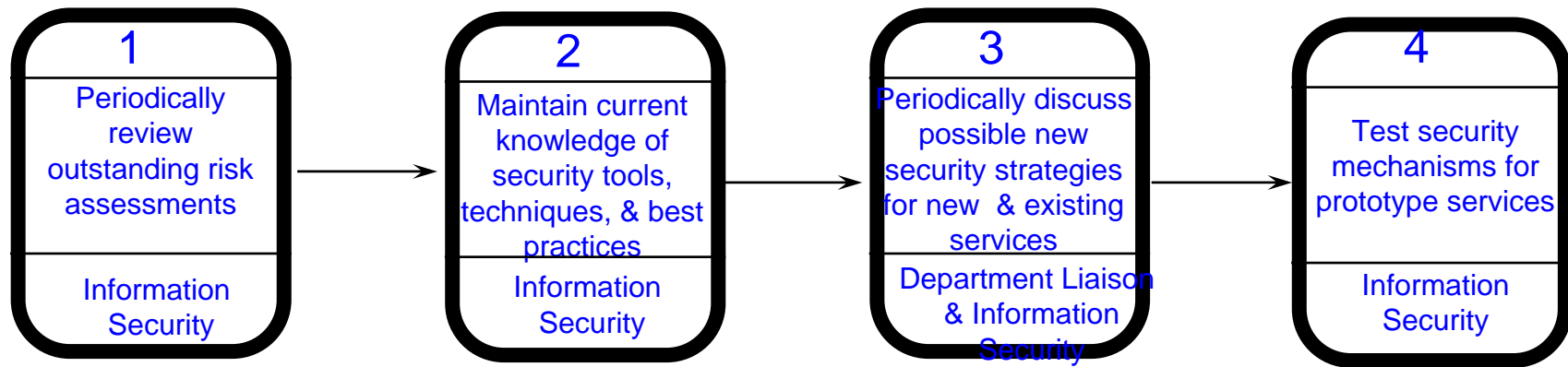
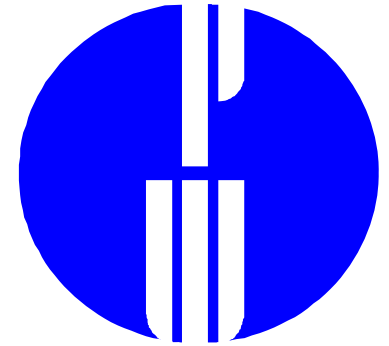


Figure 6: Example Strategy Process

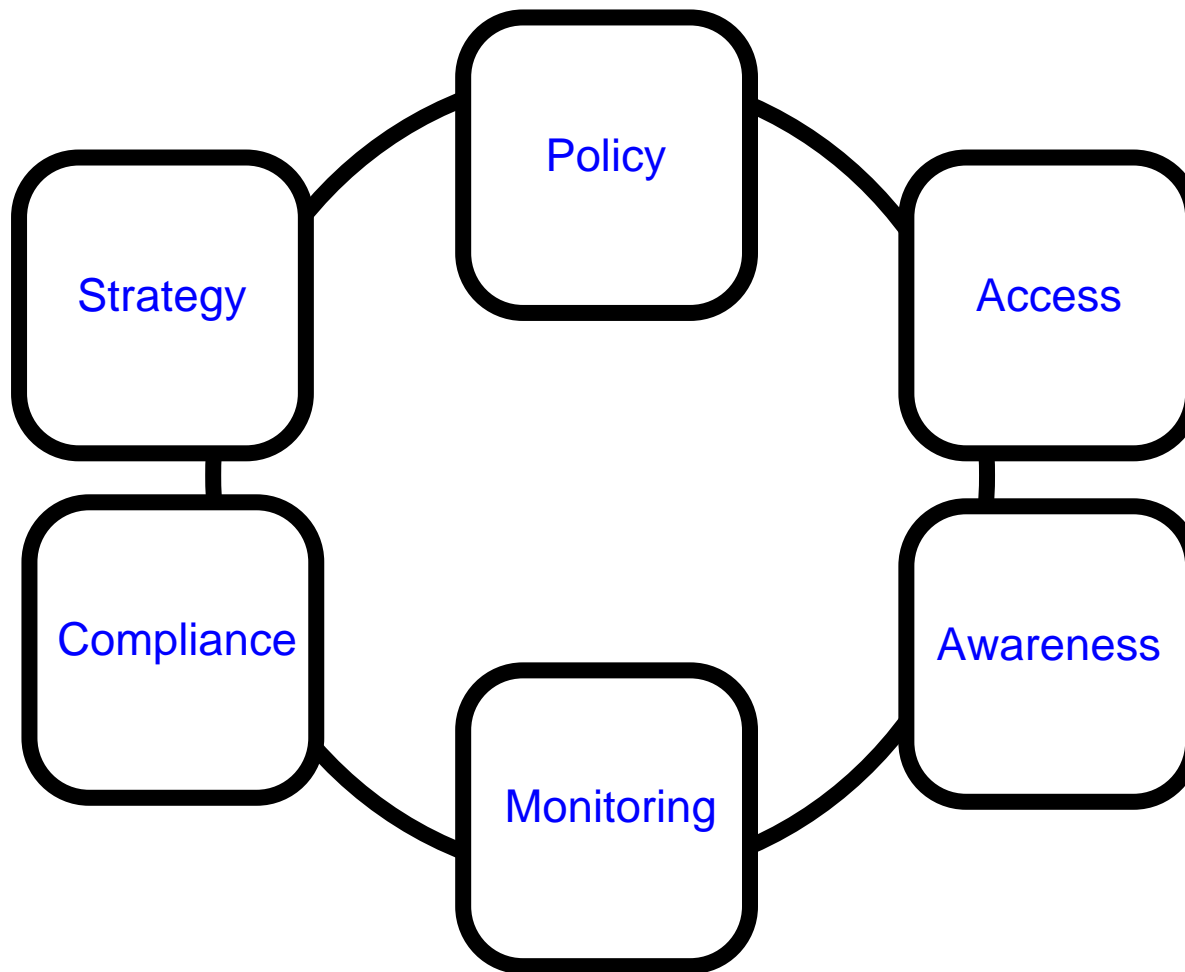
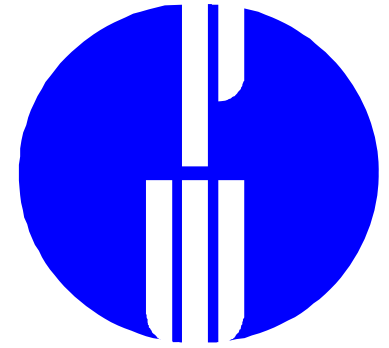
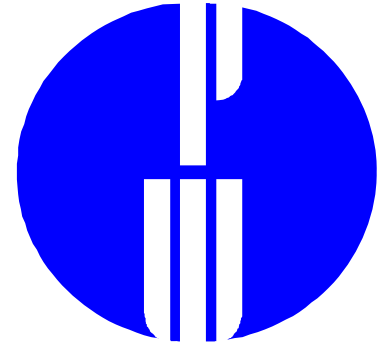
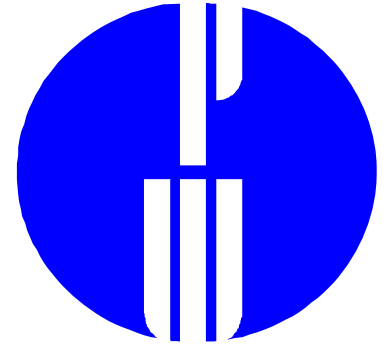


Figure 7: A Security Management Process

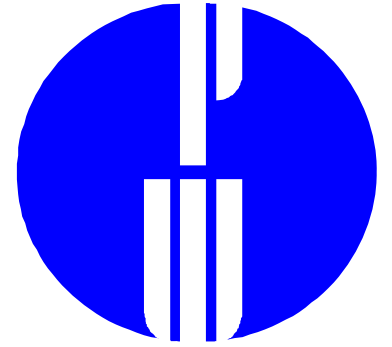


Questions?

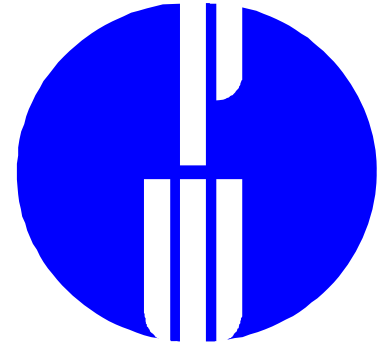


***"I can't get other departments
to buy in to my security
policy."***

Reply:

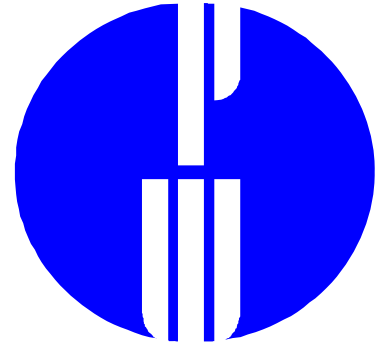


"An effective policy process requires representation from all affected organizations."

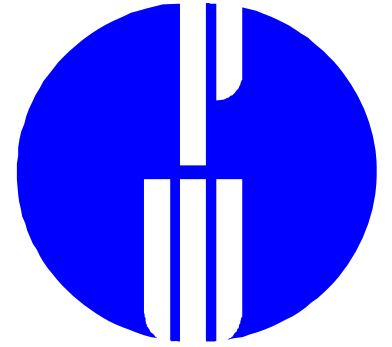


***"That is covered by our policy,
the users just didn't know
about it."***

Reply:

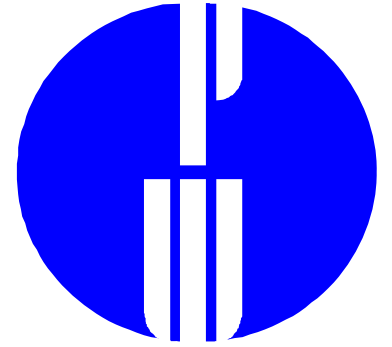


"An effective awareness process requires participation from all affected organizations."

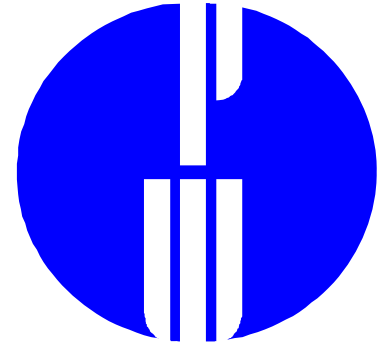


"We don't have responsibility for system access; it's performed at the department level."

Reply:

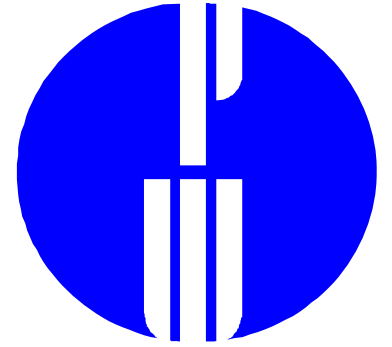


"An effective access process cuts across organizational boundaries."

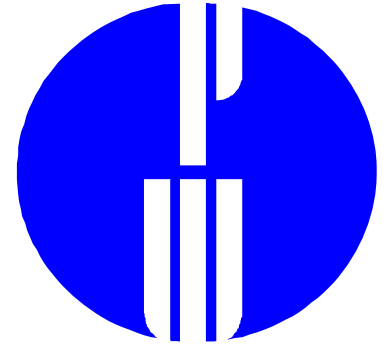


***"We don't have enough
people to monitor logs."***

Reply:

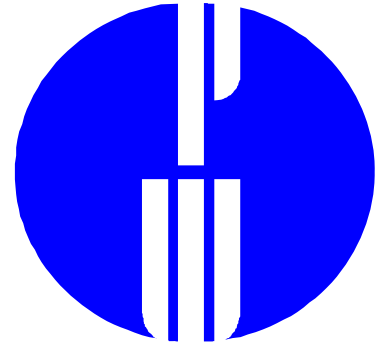


"An effective monitoring process starts with automation and ends with escalation."

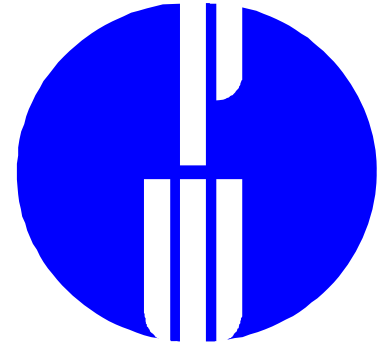


"We fixed this last year, and they put it back."

Reply:

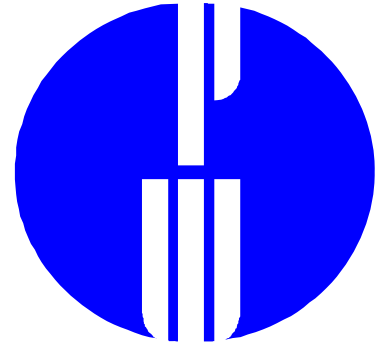


"An effective compliance process requires proof of lasting change."

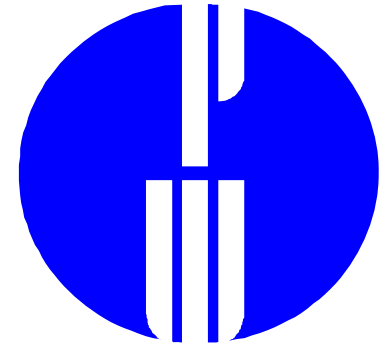


"Every time we get ahead of the game, they deploy some new kind of technology."

Reply:



"An effective strategy process makes security improvement part of the overall IT strategy."



An effective security management process comprises six subprocesses:

Policy:	to establish a framework for the development of organizational standards with respect to security
Awareness:	to educate those affected by security policy on their roles and responsibilities
Access:	to limit dissemination and modification of customer data and other sensitive information
Monitoring:	to detect policy violations and other security vulnerabilities
Compliance:	to track security issues and help ensure that resources facilitate the resolution of security issues
Strategy:	to meet the security challenges presented by new information technologies

