

THIS PUBLICATION CONSISTS OF TWO PARTS  
In the following order:

- A) Report
- B) PowerPoint Presentation

# **Infrastructure Monitoring Challenges**

**J. L. Bayuk**

## **Overview**

When charged with monitoring the security of an enterprise, an information systems security professional must make choices. There are never enough resources to monitor everything that may be useful in detecting any type of security incident. But there must be enough to represent due diligence in protecting company assets. For example, where automated detection mechanisms do not make the risk/reward cut-off, audit trails must be accessible to investigators in the event of a known intrusion. This paper presents an approach to classifying types of security monitoring together with types of monitoring requirements. These classifications enable information systems security professionals to design monitoring architectures that are both cost and containment effective.

## **Monitoring Categories**

Comprehensive security monitoring requires a carefully designed monitoring package that includes:

Logs: User activity

Configuration: Variable settings

Service: Methods of system access

For example, an unauthorized addition of a new account to a system is generally accepted as something that security should detect. It could be detected through an activity monitor, a configuration monitor, or a service monitor.

To detect this activity with a log monitor, a security administrator would have to look at all logs of new account additions and compare them with the evidence from the authorization process that was eventually forwarded to the administrator assigned to add new accounts.

To detect this activity with a configuration monitor, a security administrator would have to detect changes in the snapshot of user lists on a periodic basis and compare these lists with the evidence from the authorization process that a new user was authorized.

To detect this activity with a service monitor, a security administrator would have to try to gain access to the systems using names of users who are not authorized to use the system.

All three categories of monitoring may be necessary to assure the security of a given information system. Within each category there are choices of type. Within each choice of type there are choices in granularity.

### ***Logs***

Logs are the most common form of security monitoring. Almost all access control mechanisms provide some level of logging to see that the access control mechanism at work. These logs can be used to track the activity of users on a system or network.

Security products invariably supply detailed logs of unauthorized access attempts. Failed access attempt logs are usually configurable with levels from “none” to “debug.” Setting such a flag to “none” will provide no logs and “debug” will provide the entry and exit for every subroutine in the vendor’s code. There will always be some activity in these logs as users forget their passwords or automated processes randomly fling themselves at them. As any intrusion detection literature will describe, one may use this “normal” or “baseline” activity to establish a pattern. Deviations from that pattern may then indicate an attempt to break the access control. It is commonly experienced that the deviation is a system administrator rather than an intruder. Human analysis must always accompany a response to incidents reported by these logs.

Failed attempt logs alone are not sufficient to monitor user activity. If an intruder breaches security, these types of logs are not helpful in establishing what access control mechanisms the intruder succeeded in breaking. Access control logs may also provide details of authorized access, with date and timestamps. However, this ability must not be taken for granted. Logging of authorized access attempts is not always a product feature, even in products that provide access control. If it is, it must be used judiciously. A system that must be protected is often a system that has many users performing many job functions. Logs of their authorized activities can easily fill all available disk space.

### ***Configuration***

Configuration monitoring is keeping track of what security prevention mechanisms are supposed to do and seeing that the tools chosen to enforce them are configured accordingly. This task is not trivial. Very rarely is a significant expenditure in security technology not accompanied by a significant effort in choosing the security tool that provides the richest set of security features to protect the targeted environment. But once

it is decided that those features will be used, the product must be installed and configured accordingly. And if that initial configuration changes, there go the desired security access controls. Even if configuration changes are recorded in a security log, their impact on the log itself may not be obvious to log monitors. Hence, monitoring the configuration per se (in and of itself) is key to an effective incident detection mechanism. The first thing a burglar will do is disable the alarm.

The configuration monitor depends on a snapshot that allows a security administrator to prescribe allowable sets of values for specific sets of configuration parameters and to flag exceptions. Files to be guarded by a configuration monitor include any and all vendor-provided configuration files that set the user-selectable options available upon installation. If this data is kept in a non-readable format, a periodic database query may be used to determine whether the information has been modified. If your system is not vendor supported, and you are unable to determine where the configuration parameters are stored, take a snap shot of the entire vendor installation with a modification detection tool (e.g. Tripwire), change a parameter, then run the tool again to identify what impact the change had on the file system.

There is no limit to the amount of information that may be included in a configuration parameter, but a good cut-off is at the point where the security administrator can easily distinguish between authorized and unauthorized changes to the configuration. Some configuration parameters are fairly static while others must necessarily change with system operation.

Static configuration parameters include automated startup and shutdown scripts, operating systems configurations. They include any configuration that, if changed, may allow a user to bypass the security product. Actual lists of users, or user adds and deletes, could also be included in configuration monitoring, but these only makes sense if the monitor can distinguish between authorized and unauthorized additions to the list. For example, security mechanisms designed for large sets of users will have two levels of user administration: administering users and administering administrators. In addition to lists of authorized users, there will be lists of authorized administrators. In some cases, it may make more sense to monitor the list of administrators and the templates for creating new users than to monitor than actual user profiles.

### *Service*

Lab tests on security products are usually designed to test whether access control mechanisms deny access to all except specifically authorized services. A test will configure a product to disallow a set of services, then try to 'break' the product to see if

the services can be accessed despite the best efforts of the vendor to keep them out. We refer to such testing as service testing. Though service testing is almost always performed in a product selection process, once a product has been ‘lab certified’ to perform denial of unauthorized access, that ability is often left unchallenged in the production environment.

However, there are sometimes global switches in product or backdoors in architectures that let unauthorized services slip through. These switches and backdoors are often provided by the vendor consultants once a product is in operation. An administrator will find it hard to perform a certain task and will receive advice that setting a global parameter will enable the task. Unfortunately, even in the most robust of products, security holes may surface in operation due to changes in the technology of a subsystem or changes in the environment. Hence, service monitoring is essential to a well-protected environment.

### **Monitoring Requirements**

Most companies will set minimum levels of security requirements that include monitoring. These are usually documented in policies and procedures. They are designed to ensure that the company can claim to be at “Industry standard” levels of security implementation. Yet rarely are they followed to the letter for every system in the company that falls under their jurisdiction. Some are peppered with vague language that allows for interpretation “based on the level of system risk,” or exceptions for “test” or “non-production” systems. Practical considerations often override security requirements, and exceptions are easily granted. Some requirements are just ruled not to apply to a given environment.

### ***Obligatory***

However, where security standards do exist at the obligatory level, they owe their implementation to the fact that ease of administration of multiple systems demands that administrators configure similar systems in similar ways. Large-scale systems and network administration tools may be in use for all systems and hence provide security monitoring for even non-critical systems. The level of security requirements that we call “obligatory” are those that get implemented in every system from sheer ease of administration. They may be designed to preserve integrity and accountability rather than security, but they have beneficial side benefits for security investigation.

Obligatory security requirements reflect the habits and administration tools of a company’s administration team. They often include failed logging attempts. In companies that have time-shared systems, they include success logs and accounting logs.

But rarely is configuration monitoring or service monitoring part of a company's baseline level of security monitoring requirements.

### ***Nominal***

As in the obligatory monitoring done for all systems, nominal monitoring requirements rely on the assumption that the configuration of the system upon install remains in place. But there is greater awareness of the types of user activity that may corrupt that configuration. In addition to failed user attempts, logs of administrative activity may be monitored. Written security policies are followed with minor exceptions, though they are interpreted in the loosest way possible to justify wide latitude given to administrators to decide what level of monitoring is appropriate for their unique systems.

For example, requirements for monitoring adds and deletes of user accounts in a nominal monitoring process will apply to operating system users, but not to web server administrators. Or requirements for monitoring configuration changes will apply to the operating system, but not to third party applications.

A system that is nominally monitored will maintain most if not all logs an investigator would need to trace actions following a security event. They just will not be easy to gather or interpret. It may sometimes be difficult to pinpoint activity to a single user. For example, it may be possible to tell that a given system configuration file was changed between the time of the previous night's backup and the time of the incident. But the person using this ID may only be identified as one of four users who were logged in at the time.

### ***Standard***

Standard monitoring comes with the recognition that security monitoring efforts must be designed to facilitate after-the-fact judgements concerning accountability. Advice on legal and regulatory compliance is sought. Security standards are interpreted to the letter, and frequently the policy author may be called upon to clarify the intention of a monitoring requirement. Standard security monitoring demands an independent audit trail, and thus introduces the requirement for a separate group to provide segregation of duties in the configuration and monitoring processes. The use of administrative accounts will be thoroughly monitored.

But of course it is evident that simply looking at scattered logs from a few thousand systems could not qualify as due diligence in monitoring. Thus standard monitoring requirements often call for automated identification of potential security incidents. Economies of scale may require that automated processes filter logs to preserve only

security-relevant information so it is easily retrievable in the event an investigation is required. Actual logs are only consulted in the event that an incident detection necessitates an investigation. Automated security detection mechanisms do not inherently provide accountability for file system changes, but they make it possible for security administrators to react faster and thus narrow the potential suspects.

### *Critical*

In every company, there are higher criteria set for protection of the ‘crown jewels.’ These are company assets vulnerable to computer system misuse. All sorts of checks and balances are built into application software to narrow the risk of system abuse, so monitoring the integrity of the application is the paramount activity in a critical security monitoring requirements. This of course includes standard monitoring requirements at the operating system level. In addition, it contains the configuration of the application, its inputs, and outputs.

The application monitoring requirement may introduce a process that goes beyond the company security policy. Application software must be included in both log and configuration security monitoring. This complicates the automated processes used to detect tampering because it introduces application idiosyncrasies such as generic application users and proprietary log file formats. In addition, preservation of application integrity may introduce new legal or regulatory requirements. For example, the requirement to detect security incidents within the given minimum time interval for backing out of a transaction.

### **Monitoring Alternatives**

In the previous sections, we have been careful not to make judgements concerning what types of monitoring requirements apply to what systems. We have also been careful not to mix discussion of monitoring categories with monitoring requirements. Monitoring categories are tools that are available to meet requirements. Requirements should not be about monitoring categories, but about necessary detection capabilities.

Bearing this distinction in mind, and considering that no one has resources to fulfill critical monitoring requirements for all company-owned systems, the objective is to identify the minimum level of infrastructure monitoring that may be applied in what combinations to fulfill different types of monitoring requirements.

The systems monitored must be viewed from an environmental perspective and decisions must be made on whether to monitor some types of activities at a firewall or proxy level, while other kinds at a system or database level. The monitoring function may be split

among groups who are best able to detect different types of events. For example, an application administrative group may be responsible for fraud detection while a network administrative group may be responsible for network denial of service attack detection.

In the matrix below, the row headings identify monitoring categories available as tools for various administrative groups. The columns headings are system monitoring requirements. The cells in the intersection of the rows and columns identify the sets of administrative groups who, as part of their normal job function, may incorporate aspects of security monitoring identified in row headings that would meet the requirements in the column headings.

Monitoring Category:	Monitoring Requirements:			
	Critical	Standard	Nominal	Obligatory
Configuration	System, Network, Security, & Application Administrators	System & Security Administrators	System Administrators	System Administrators
Log	System, Network, Security, & Application Administrators	System, Network, & Security Administrators	System & Network Administrators	Network Administrators
Service	Network & Security Administrators	Network Administrators	None	None

Detailed analysis of each system environment is required to make informed trade-offs concerning each monitoring type and requirements combination. So here we will be content to provide scenarios that illustrate the monitoring processes available to meet each level of security monitoring requirement.

Where you have obligatory security monitoring requirements, security monitoring may be left to system and network administrators. Whatever checks they automatically establish to measure system integrity may also lead them to identify a security incident. The obligatory monitoring is achieved because system administrators need to check the configuration often enough to maintain service. Hacking attempts may be identified via network intrusion detection logs, which exist for the entire enterprise. The combination of the activities is enough to fulfill obligatory security requirements.

Where security requirements are nominal, system administrators in their attempt to satisfy policy will configure more logging at the host level, where security incident activity is prone to consume unusual amounts of disk space. The administrator identifies the disk space issue, thereby identifying the security incident. Appropriate responses include contacting the security administration team and implementing a predefined incident recovery procedure. Where systems have nominal monitoring requirements they would normally have nominal uptime requirements as well. So it is possible to take them off-line or temporarily issue replacements while the extent of the damage is being investigated.

When security requirements are standard, a detection mechanism must be formally identified. It is not enough to keep logs if no one is responsible for looking at them. Thus security administrators are given responsibility for detecting and reacting to specific anomalies in many types of logs. But not to the extent that they duplicate efforts covered by system and network administrators in the course of the system maintenance aspect of their job function. It also may be inefficient to have security administrators perform a task if it introduces an infrastructure element just for security testing that already exists in another administrative group. For example, service monitoring may require a point of presence at every logical subnet. Network administrators may already have access to network components in each subnet, so they may volunteer to do service testing rather than to share the access with the security administrators. Responsibility for incident detection is thus distributed among organizations, each focusing on the areas that apply to their domain of expertise.

Where security monitoring requirements are critical, configuration monitors are a requirement even if every individual configuration change is recorded in activity logs. It may be very difficult to determine in advance which entries in the activity logs of a few thousand production operations systems will indicate that configuration parameters have been modified in a way that adversely affects systems security. But it is straightforward to determine allowable sets of values for specific sets of configuration parameters and flag exceptions. Activity logs may then be used to determine accountability for changes.

Critical security monitoring requirements also take into account business functions that are normally beyond the scope of an infrastructure monitoring effort. Hence, application specialists must supplement the infrastructure administrators in responsibility for security incident detection. These efforts are not necessarily limited to information security tools and techniques, but may include statistical transaction analysis, account reconciliation, and spot checks on inventory.

## **Summary**

Even if an organization has unlimited resources for security monitoring, an information systems security professional must still make choices as to which type of security monitoring best fulfills requirements for incident detection. This paper has presented an approach to classifying the types of security monitoring available to meet those requirements. These classifications enable information systems security professionals to design monitoring architectures that are both cost and containment effective.

# Infrastructure Monitoring

Jennifer L. Bayuk



# Monitoring,

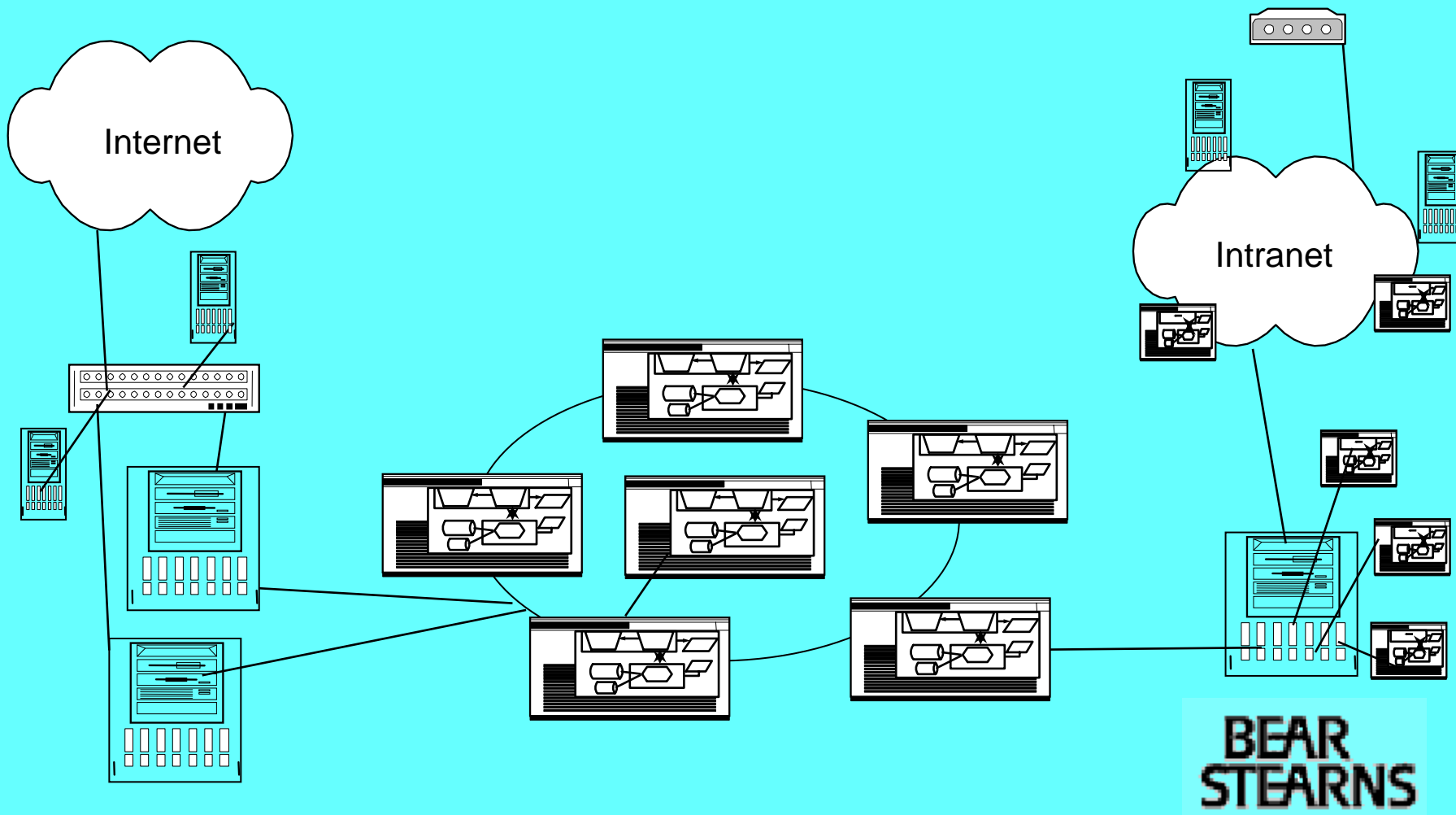
---

*or **knowing** your controls are working,*

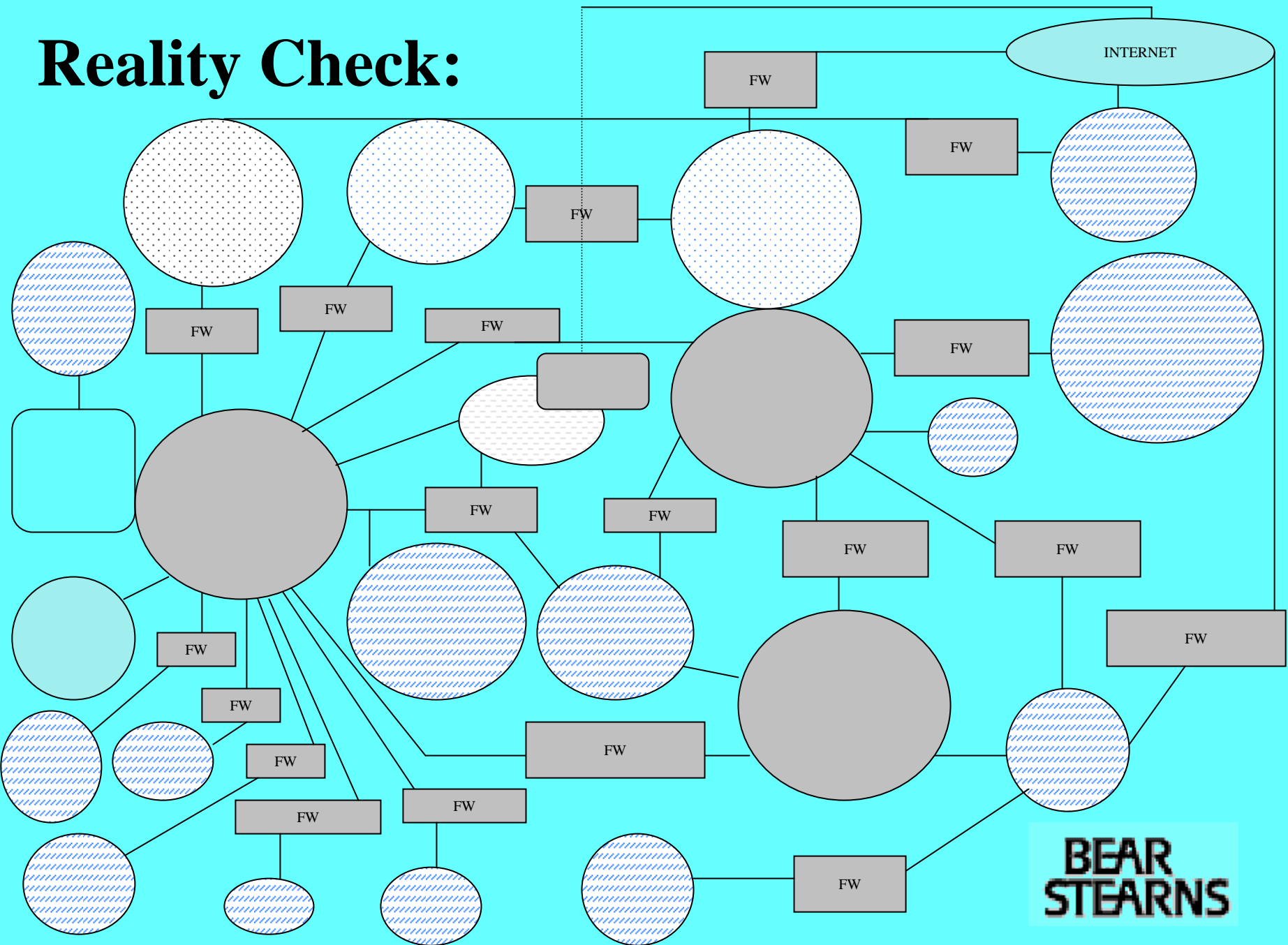
*or at least **establishing activity** to ensure control objectives are met*

# Wouldn't it be nice?

---



# Reality Check:



# What is out there?

---

*Inventory the tools available to operations....*

```
root      630      1  0   Oct 17  24:51 /usr/sbin/syslogd
netscape 1488    1487  0   Oct 17  0:27 /opt/bin/ns-httpd -d /opt/ns-home/hs/config
root      1501      1  0   Oct 17  0:16 /opt/bin/ns-admin -d /opt/ns-home/adm/config
root      1556      1  0   Oct 17  0:00 /esm/bin/solaris-sparc/esmd -fv
root      1567    1508  0   Oct 17  0:03 /usr/bin/sshd
root      1569    1528  0   Oct 17  0:53 /opt/OV/bin/ovlmd
root      1577      1  0   Oct 17  0:23 /usr/sbin/inetd -s
root      1578      1  0   Oct 17  5:59 /usr/seos/bin/selogrd
entrust   1621      1  0   Oct 17  14:59 /opt/entrust4/bin/entadmsrv
root      1690      1  0   Oct 17  0:09 /usr/trip/bin/twadmin
ovmgr     28604  28579  0  14:46:52  0:00 /usr/lnms/bin/ev
```

*These things have logs, configs and well-defined services.*

The logo for Bear Stearns, featuring the words "BEAR" and "STEARNS" stacked vertically in a bold, black, sans-serif font. The text is centered within a white rectangular box.

# Monitoring Categories

---

- **Logs**
- **Configurations**
- **Services**

# Logs

---

- **Access control**
- **Activity**
- **Exception-based**

# Configurations

---

- **Parameter options**
- **Initialization routines**
- **Access control lists**

# Services

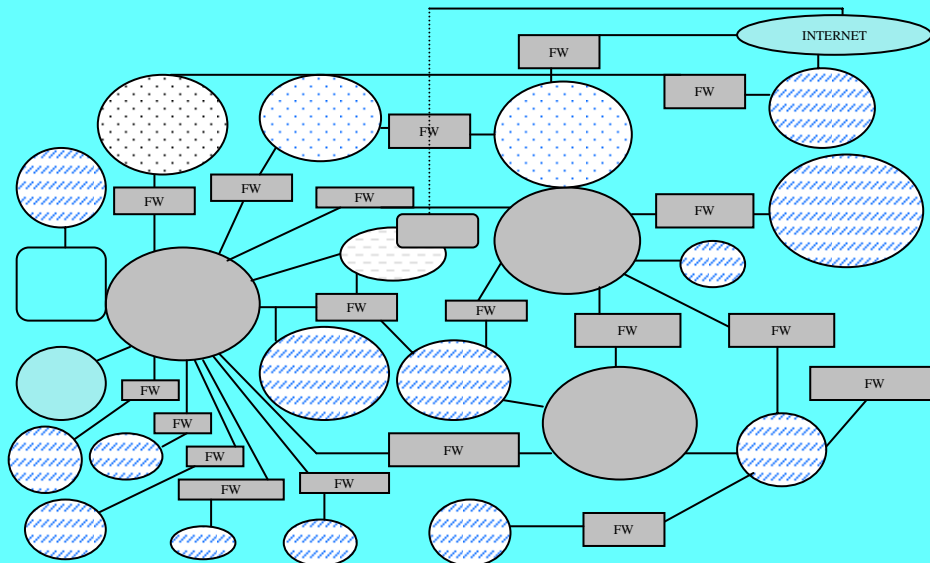
---

- **Architecture provisions**
- **Tweak detection**
- **Vulnerability inventory**

# Remember the point

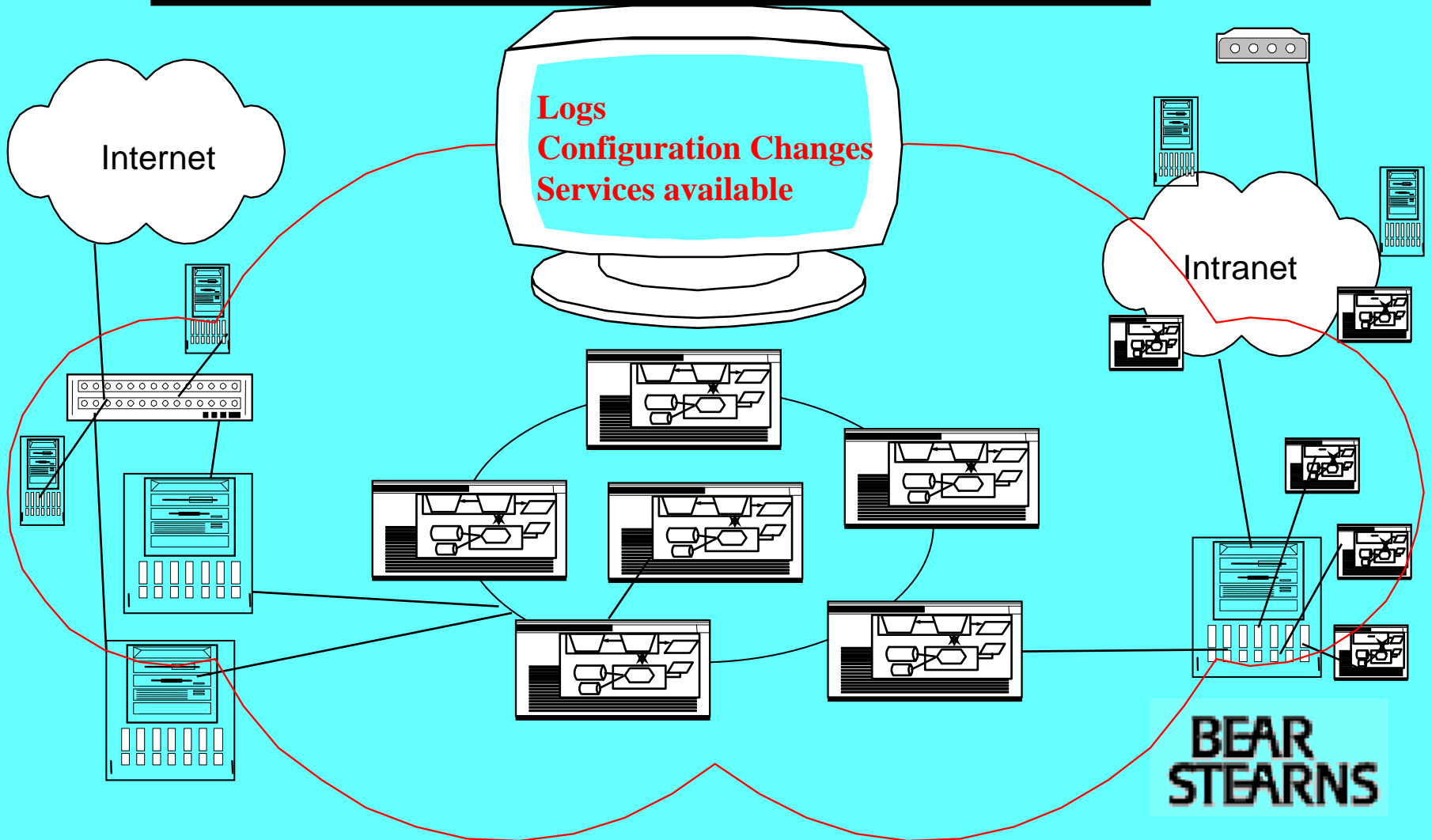
---

*Now, where did we put those engineering specs for the preventive controls?*



**BEAR  
STEARNS**

# Wouldn't it be nice?



# Reality Check:

## Monitoring Trade-offs

- Due Diligence
- Resources
- Detection Methods
- Storage/Retrieval

**BEAR  
STEARNS**

# Monitoring Organizations

---

- **System**
- **Network**
- **Application**
- *Security*

**What are the rest of them doing,**

---

**or, how small can I keep my  
staff?**

# Monitoring Requirements

---

- **Obligatory**
- **Nominal**
- **Standard**
- **Critical**

# Example Monitoring Requirements

---

Monitoring Category:	Monitoring Requirements:			
	Critical	Standard	Nominal	Obligatory
Configuration	System, Network, Security, & Application Administrators	System & Security Administrators	System Administrators	System Administrators
Log	System, Network, Security, & Application Administrators	System, Network, & Security Administrators	System & Network Administrators	Network Administrators
Service	Network & Security Administrators	Network Administrators	None	None

# Summary

---

- **Classification**
- **Approach**
- **Consistent Application**

*jbayuk@bear.com*

\*\*\*\*\*

Bear Stearns is not responsible for any recommendation, solicitation,  
offer or agreement or any information about any transaction, customer  
account or account activity contained in this communication.

\*\*\*\*\*

*www.bayuk.com*

