Global Information Assurance Certification Paper

NIDS ISMS

An ISMS conception and design
for a corporate environment.

Author: Tim Strong
Assignment: G7799 Version 1.1 – Sans Parliament Hill 2004
Date: January 11, 2005.

Table of Contents

Abstract

The topic of the ISO-17799 practical assignment shall be focused in the ISMS of an network based intrusion detection system. While ISMS does not necessarily focus on a security technology, product or process, I have elected to do so in this paper. This can bring about somewhat of a doubled edged sword since I am writing an Information Security Management System for an actual information security system. Information security systems, such as IDS, do not operate themselves any more or any less from other information or infrastructure components such as desktops, networks, data centers or applications.

The paper will cover all aspects of ISMS using the 7799 guidelines and the PDCA process. This includes definition of requirements, project plans, risk & asset identification, policy development, enforcement & compliance. The paper will also cover the basics of the situation today and how the ISM improved the situation if the IDS system.

The ISMS for the IDS will be in an organization with 40 000 employees, but focusing on three divisions that contain a total of 9000 employees. The organization already has 7799 based policies that may or may not be applicable to the 3 divisions in question. Where applicable these policies will be used, where not applicable new ones will be created. The same will hold true for standards & guidelines. That is, divisional guidelines and standards will most likely by created to supplement and complement the organizational guidelines and standards.

Part One - Definition

The main objective of this paper is to develop an ISMS (Information Security Management System) for the newly retrofitted network IDS (intrusion detection system) in our company. Our company (referred to as OC hereon after) has a multitude of IDS systems, standards & information security practices. This is primarily due to the size of OC.

OC has over 40 000 employees, over 60 000 network addressable devices, about 20 large offices and hundreds of smaller offices and sites. The primary business of OC is telecommunications. There are numerous smaller divisions but the most notable are wireless, video and retail outlets for OC products. The focus of the ISMS will be on the IDS in those three divisions. Wireless, video and retail will be referred to as the WVR division hereon after.

WVR is a significantly more manageable environment than OC as a whole. While WVR does comprise of 3 separate legal entities, the organizational structure for IT, IS and information security is handled by a single department within OC. This has resulted in closely aligned strategies and systems across WVR. WVR has a total of about 9000 employees, approximately 10 000 network addressable devices, 9 main sites and very few branch offices with the exception of about 300 retail outlets.

The corporate security department at OC dictates all policy for OC including the WVR division. The policy is 7799 based and covers all aspects of OC operations. However, solid policy is just a single aspect of an ISMS and even though the policy exists in OC, the ISMS that helps support it is still under construction or lacking in certain areas. IDS is an area which has a strong divisional aspect for implementation and management. As such, even if the ISMS was complete, it would not satisfy the requirements at a divisional level.

The IDS system in OC and the WVR division has seen many incarnations depending on who was deploying it, where it was being deployed, who was paying for it and who would be managing it. Traditionally the focus has been on host IDS. Both the OC Corporate Security department and the WVR division have hundreds of host based ISS sensors deployed on servers throughout the organization. While the ISMS for HIDS also needs work, it will not be the main focus of this paper. HIDS in WVR is much more closely aligned to OC than NIDS. This will lead to much of the OC HIDS ISMS being applicable to the WVR division.

NIDS is a relative the newcomer to the block in terms of IDS at OC. While OC still has some decisions to make for a product standard and a long term roadmap, the WVR division has been able to forge ahead with an implementation of McAfee Intrushield sensors. The main purpose of the Intrushield implementation is to limit damage caused by malware and aid in

tracking down infected systems.

The NIDS devices are placed at the interconnect points between the WVR division and the OC backbone. The Intrushield devices are true appliances that contain no user updateable operating system or moving parts (except a fan). The hardware is 100% ASIC (Application Specific Integrated Circuit) based and therefore does not contain a popular architecture such as Intel or PowerPC. There are a total of 6 devices reporting alerts back to a central database. The database has a web/java based console for viewing and acknowledging the alerts generated by the devices. The web based console is accessible by the WVR security expert as well the network operations teams (view only) and the OC Corporate Security operations team (view & acknowledge). Only the WVR security expert has permission to maintain the signature sets and perform routine maintenance on the IDS system.

The security culture in OC is sporadic. There are certain departments and divisions that utterly embrace security, while others see security at a hindrance to business operations. Drilling down below the departmental & divisional level, the user communities are much the same. Some users are information security savvy while others don't even know that OC has a Corporate Security Department. This erratic culture is being worked on by Corporate Security. The most noticeable facet is the launch of a new mandatory online security awareness training program. The program is about one hour long, is interactive and has been custom designed for OC. The custom design feature is an important one since the training can be tied directly back to the policies and other links on the Corporate Security intranet homepage.

Another large area that contributes to the sporadic security culture is consistency. While 2002-2003 saw a complete rewrite of all information security policies to the ISO-17799 standard, these policies have never been formally launched or socialized. To make matters worse, the old policies written in 1992-1994 are still posted on the intranet site. The awareness training will help direct people to the new 7799 policies, but anyone doing research on the Corporate Security intranet site has pretty good chance of ending up in the old policy section.

On the good side of things though, the IS/IT PMO (Project Management Office) now has security on their standard project template for all IT/IS projects. This template was developed in conjunction with Corporate Security, business analysts and project managers. It should be pointed out though, that this will only address new projects. It will not help develop a new ISMS or process for existing systems or infrastructure components. It will neither help if a project is initiated and/or managed outside of the PMO.

The current processes for managing the NIDS system are, for the most part, adhoc. But, as with so many other systems, significant effort is being made to

formalize and document the processes being used. The formalization includes a workflow analysis which may result in the process changing if there is a better way to do things.

Since the NIDS are essentially on the perimeter of the WVR division, they detect alerts inbound and outbound from the WVR division. In addition to this, due to the network design, the NIDS can also detect events moving around within the WVR division between the departments. For example, it can detect an event going from the wireless department to the retail department; Or from the video department to the wireless department. Since the NIDS is primarily used for source mitigation and source identification, the WVR division only cares whether or not the propagator is inside or outside of the WVR network. The adhoc process differs slightly for these two situations.

If the propagator is within the WVR network, the incident is referred to both the WVR IM (Incident Management) team and Corporate Security operations group. Corporate Security operations has a dedicated team call RAR which stands for Rapid Action Response. The RAR team usually does the initial triage and kill on the propagator. After the initial kill, the WVR IM team goes in for the final cleanup and checkup. This wrap up includes ensuring the AV is up to date, all patches installed and any other information security critical task.

In the 2nd situation, the propagator is in the OC backbone propagating into the WVR network. In this case, the incident is referred to the RAR team exclusively. If during the incident analysis it appears that the WVR victim was successfully compromised, then the incident is also referred to the WVR IM team for a checkup on the victim.

While these two processes deal with how WVRs IDS is used in an endpoint protection ISMS, it will not be the main focus of this paper. The ISMS described in this paper is going to have the NIDS as the system we are trying to protect, not the endpoint systems. Since IDS can be considered as a protection mechanism for an ISMS that serves the network and endpoints, it is very easy to overlook the assets, risks & threats associated against the actual IDS system itself. Throughout the paper, this idea will be reinforced several times… This is an ISMS for an IDS, not IDS as part of an ISMS for some other asset.

PDCA Process

Many companies such as Induction develop there ISMS using the PDCA methodology.[1] That is, Plan, Do, Check, Act… PDCA. During the planning phase, we will be dealing with how to take the IDS ISMS from conception to production. This will include all dealings between OC and the WVR division with regards to corporate standards and management practices. The planning stage will also serve as an identification stage for policies, processes, controls, assets, risks and risk management. This is by far the most critical step in the

PDCA process. If the planning is not correct, then the subsequent steps will be of little use.

The second step is “Do”. In this stage we will identify the steps taken to execute the plan for the new ISMS. It will be broken down into three very discreet categories: problem, action and steps taken. The problem and action categories will provide an overview, while the steps taken category will be the execution of the action. The steps are based on the information developed during the planning stage.

The third step is “Check”. The controls developed during the planning stage and executed during the “Do” stage need to be checked. Since OC is a 7799 based organization, the controls will checked against an audit checklist derived from OC 7799 policies. Should these policies not be sufficient to develop a robust audit checklist, once again divisional 7799 policies may be used to generate an audit checklist that will provide value.

The final step is “Act”. This is the stage where we make sure the ISMS does not get put on the shelf and forgotten. This section will contain the logistics of maintaining the IDS ISMS as well as an analysis of improvements that could be made to the WVR NIDS system. This section will also contain details about the operation of the NIDS and how it ties into ISMSes for other systems.

Putting all of this together, the root of this paper comes down to a very basic level. Using the PDCA methodology, this paper will develop an ISO 17799 based ISMS for a NIDS system within the WVR division of OC.

Part Two – Plan

Problem Identification

Now that we have a baseline of the current situation of NIDS in WVR, we can start to plan for our ISMS and document all the significant portions of the system. In the PDCA model, the planning stage actually consists of two steps: Identify the problem and analyze the problem.

We touched upon identifying the problem in the introduction, but let's expand on the issue and clearly mark the situation we are identifying. In this case we will start with the root problem and clearly explain why it is the root problem. Next we will move onto analyzing the problem. Most of the planning of the first PDCA phase will be done during this analysis. In other words, we will design and specify the ISMS.

The root problem is the WVR divisional IDS has no solidly defined ISMS. The IDS system despite being implemented with everyone's blessing, is poorly documented, maintained by a single person, accessed by numerous departments and has never been checked against OC 7799 policies or controls. While much of the situation is attributable to resource constraints, a well designed ISMS should be able to alleviate much of the deficiencies caused by resource constraints.

Since OC has no clearly defined standards for NIDS, the WVR division implemented a NIDS system within their own perimeter on OC network. WVR is a smaller division and all of the planning, deployment and tuning was done by a single person. While there where some discussions with other teams such as OC Corporate Security and OC network operations, these were merely discussions seeking approval to implement. These discussions yielded nothing in terms of documentation of the NIDS system being installed. Since the WVR rollout was a one person show, the main thrust was to get the system up and running, not documenting the details.

The fact that the system is a one man show is also a problem that has been identified. Single point of contact (SPOC) systems are extremely dangerous on many levels. The most obvious is if the SPOC person is terminated or unavailable. If WVR has come to rely on the IDS system, there will be a significant learning curve and cost for figuring out how the system works. This is not only true for the operation of the system, but also for the processes associated with the system. A second danger of SPOC is abuse. SPOC opens up all sorts of loopholes for intentional system damage and corporate espionage.

A third identified problem is the fact that the WVR IDS system is accessed by a

myriad of people & teams. This list comprises of the WVR security expert, WVRs network operations teams and OCs RAR team. While it is a good thing to have an IDS system monitored by several teams, this benefit is not present at OC. The teams monitoring the WVR IDS do so on an adhoc basis with no clearly defined procedure or policy as to which team or person is doing what and when.

The final problem identified with the WVR IDS system is that it has never been checked or audited. If systems are never checked, how does OC know that it is functioning properly? When the system is checked, controls need to be in place to ensure consistency of the checks. There is no point of WVR checking the system if the controls are different than the ones that OC uses. The result would be comparing apples and oranges.

Now that the major problems of the IDS system have been clearly identified, we can move onto analysis. As mentioned previously, this analysis will essentially define the core of the ISMS for the IDS system. As part of the analysis, we will define aspects that pertain to our major problems.

These aspects will include:

- Identifying existing policies from OC Corporate Security
- Defining the asset identification process
- Defining the risk identification process
- Outlining the WVR/OC management structure of the WVR IDS system

Once a high level overview of the policies and process is in place we will proceed to provide an outline of applicable policies as well as identifying the main risks.

OC Corporate Security has 7799 policies already defined for OC. These policies cover all aspects of IT within OC. The policies are well written and explained. The typical policy will contain 4 sections: Policy Statement, Explanatory Notes, Related Security Risks and Related Documents.

There are 4 existing OC policies that pertain to our problems.

- Run Books
- Segregation of Duties for Security Functions
- Event Investigation
- Review of Compliance

We will examine these policies in more detail later in the ISMS.

In order for an ISMS to be successful, it must be known what is defined as an asset and which assets the ISMS is supposed to manage. In the case of WVRs NIDS system, the assets in question are all part of the IDS system itself. This is one of the tricky areas for creating an ISMS for a system that protects other

systems. It is easy to think that the systems that the IDS is protecting are the assets. In our case, the highest value lays in the data the IDS collects, thus making it our main asset. The steps to identify the IDS assets in this case should be relatively straightforward. Using the database as a core asset, step out component by component in both a logical and physical map.

Problem Analysis

Now that we have a process for determining WVR IDS assets, let's develop a process to identify risk to those assets. A threat on its own is not a risk. An asset on its own is not at risk. But assets have vulnerabilities and once we combine threats and vulnerabilities, we have risk. It is absolutely imperative that we identify the risks to our IDS system with respect to our four major issues. This is another area that can easily get out of hand so we need a process to keep the risks in check with regards to WVRs IDS system. This is done by identifying vulnerabilities. In a paper entitled "Using Vulnerability Tree for Decision Making in Threat Assessment ", Vidalis and Jones say there are several ways to identify vulnerabilities.[2] Since we have already identified four major problem areas, we will apply those issues to our assets to develop a vulnerability list. For example, lack of documentation is not a vulnerability. But when we apply the lack of documentation issue to the IDS software asset, the lack of documentation becomes a vulnerability. The risk level in this situation would be the exposure to the threat by not having documentation of the asset, or on the flipside, the result of mitigating a threat by having good documentation of the asset.

Management Structure

The management structure for the IDS system is essentially non-existent, so one will need to be created. In the WVR division, there are no security committees or groups that can take this on. However, the security expert from the WVR participates in two committees managed by OC. We will evaluate if the ISMS management structure can be added to the responsibilities of these two committees or if a new committee will need to be created. We'll start by describing in more detail some of the roles that various people and groups have.

A keystone person is the WVR security expert. This person holds the security & technical expertise to operate the NIDS system. In addition to the expertise this person has, they also responsible for implementing the IDS as well as manage the budget for the IDS for expansion & maintenance. There are no other security experts within the WVR division, however substantial support comes from the WVR incident management (IM) and OC Corporate Security Operations teams.

The WVR IM team creates, tracks and closes all IT/IS related incidents within the division. They have no access to the IDS console and no solid security expertise for working with an IDS in terms of configuration, maintenance or

alerts. The IM team's strength lies in its ability to manage incidents. Once again, this is a powerful characteristic to have for an ISMS that is designed for accept input from the IDS, not the IDS ISMS itself.

Corporate Security Operations actually contains several groups that manage several aspects of information security in OC. These aspects range from remote access to personal firewalls to HIDS. The two groups that could potentially be the most useful would be the ISS HIDS group and the Rapid Action Response (RAR) group. The HIDS group has good familiarity with maintaining an IDS system. The group currently manages hundreds of sensors throughout the OC environment, as well as the backend database and console access to the IDS data. The RAR team is the primary group in OC that monitors the consoles. Even though they have limited expertise in maintaining an IDS system, they do have outstanding knowledge in the forensic area and "knowing what to look for".

Now that we have described the key players in more detail, let's examine the two potential committees that could be responsible for the IDS ISMS: The Threat Management Assessment Committee (TMA) and the OC Incident Response Review Committee (OCIRR).

The TMA's primary objective is to analyze vulnerabilities released by hardware and software vendors and determine a risk level to OC. This committee also develops recommendations for implementing patches and/or mitigating measures. This committee is owned by OC Emergency Measures (EM) and is made up of members from RAR, WVR, OC, OC and WVR IM.

The OCIRR committee is essentially a status committee. The primary objective of OCIRR is to share information within OC and its partners regarding information security incidents that have recently taken place. This committee is also owned by OC EM and contains the same members of the TMA plus OC network operations and several business partners who use the OC network.

The most apparent drawback to setting up the IDS ISMS management structure under either TMA or OCIRR is the lack of IDS expertise on those committees. These committees are strongly geared towards other systems OC is managing utilizing an ISMS. In light of this, a new committee specific to OC NIDS should be created. The committee will operate at the OC level for a few main reasons.

- Limited information security resources within WVR.
- OC Corporate Security dictates all policy and high level practices for OC.
- When OC implements NIDS, the committee will already be there.

The committee will be owned by the OC Corporate Security Operations IDS team. Members of this committee will include:

- The WVR security expert (for "hands on" NIDS expertise).
- The ISS IDS team (for IDS management expertise).

- The RAR team (for security expertise).

It should be noted that since IDS is powerful tool for use on other systems, close links should be maintained between the NIDS committee and any other committee that might require data (raw or refined) from the IDS system.

Policies

Next up in our planning process is to expand on the policies previously identified. While the specified policies already exist from OC Corporate Security, there is no guarantee at this stage that the policies will be appropriate for the WVR NIDS system. In order to obtain a firmer grasp on what the polices entail, we will provide an outline of each policy with its purpose, intended audience and the area of the 7799 standard that the policy addresses.

Policy name: Run Books
Purpose: The purpose of the run book policy is to ensure that operational procedures will be carried out correctly. This policy will address the issue of having a single point of contact for the IDS system. It is required to keep the IDS system operational should there be an issue with the SPOC.
Audience: The audience of this policy will be the operator of the system. While the ISMS will improve on the entire management of the IDS, the operation still lies with one person.
Areas of standard that will be addressed: This policy will address section 8.1.1 of the ISO 17799 standard. This section deals with accurately documenting operating procedures for a system.

Policy name: Segregation of Duties
Purpose: The purpose of this policy to ensure that operational functions of the IDS are separated from the security functions. This will address the issue of the WVR security expert having unchecked control over all aspects of the IDS. This policy is required since the IDS could be altered to conceal illicit activities.
Audience: The audience of this policy will be the WVR security expert and the RAR team. In other words, it will be the administrator and security experts.
Areas of standard that will be addressed: This policy deals with section 8.1.4 of the ISO 17799 standard. This section deals with segregation of duties for systems and services.

Policy name: Event Investigation
Purpose: The purpose of this policy is to ensure that all security tools are monitored and unexpected events are investigated. This will address the issue of who does what and when with the data the IDS produces. It is required to ensure that unexpected events are dealt with and no unexpected events are missed.
Audience: The audience of this policy will be the RAR team.

Areas of standard that will be addressed: This policy deals with section 9.7 of the ISO 17799 standard. The section deals with system monitoring.

Policy name: Review of Compliance
Purpose: The purpose of this policy is to ensure that the WVR IDS system is compliant with the controls set forth in the ISMS. This will address the issue of no one ever checking the WVR IDS system. This policy is required to ensure that the IDS system is functioning and being managed in a proper fashion.
Audience: The audience of this policy will be everyone involved in the management, administration, operation and use of the WVR NIDS system.
Areas of standard that will be addressed: This policy will address section 12.2.1 of the ISO 17799 standard. This section deals with compliance to security policies.

Threat Risk Assessment

The next step in our planning phase is to identify the actual risks associated with our problem areas. Since we are essentially treating our problem areas as vulnerabilities, we simply need to input an applicable threat list against those vulnerabilities to determine risk. This process was described earlier on in the planning stage.

However, we can not determine risk until we have identified the assets. Since we have only outlined the procedure to identify the assets, we still need to enact upon that procedure to generate an asset list. Since we define the IDS data as our main asset, let's work back from that point as per the procedure to find the other assets.

IDS Data	Database	Server	NIDS devices
	IDS Software	OS	
		Network Connections	

Table 1

Here we have effectively documented our key assets for the IDS. We have started with the core asset of IDS data and moved out to edge listing every asset that supports the IDS as we go.

Before we determine our vulnerabilities, we need to rank our assets. Ranking assets is an important step in evaluating risk and there are many methods available to evaluate assets. However, since the purpose of this paper is to describe an ISMS, the specific TRA (Threat Risk Assessment) process will not be explained in detail. The process used is the SoS (Statement of Sensitivity) method as outlined in "Threat and Risk Assessment Working Guide" issued by the Canadian Security Establishment (CSE).[3] Using this system, we assign a rating from 1-5, with 5 being the most important asset.

We will now determine our vulnerabilities for each asset by cross referencing our problem areas against each asset. This methodology was also described earlier in the planning stage.

	Asset Rating	No Documentation	SPOC	Adhoc Monitoring	No Compliance checking
IDS Data	4		Vulnerable	Vulnerable	
IDS Database	3		Vulnerable		
IDS Software	3	Vulnerable	Vulnerable		Vulnerable
Server	2	Vulnerable			
OS	2	Vulnerable			
Network	2	Vulnerable			
NIDS Devices	3	Vulnerable	Vulnerable		Vulnerable

Table 2

From this table, we can see that our 4 problem areas produce a total of 12 vulnerabilities across all of WVRs IDS assets!

The final step in determining the risks for WVRs IDS is to input threat. Once again since not all threats are applicable to all vulnerabilities, we will start by generating a matrix of threats and vulnerabilities. The threat list used is based on the "Threat and Risk Assessment Working Guide" issued by the Canadian Security Establishment (CSE).[4] Since we are only identifying the top risks, only three vulnerabilities will be used against the threat list. In addition to this, only plausible threats from the CSE guide will be listed.

	SPOC into the IDS Data	Adhoc Monitoring of the IDS Data	No Compliance checking IDS software
Sabotage - Staff Termination	Medium		
Subversion - Criminal Activity	Low		
Subversion - Misuse/Abuse of Equipment	Low		Low
Subversion - Tampering	Low		Low
Criminal Acts - Criminal Activity	Low		
Criminal Acts - Tampering	Low		Low
Criminal Acts - Staff Termination	Medium		
Accidents - Loss or shortage of Personnel	High		
Accidents - IT Malfunctions		High	Medium
Accidents - Emergency Evacuation	Medium		
Fraud - Theft of Data	Medium		Low
Fraud - Manipulation of Data	Medium		Low

Table 3

This abbreviated risk matrix shows the risk level of some threats and vulnerabilities for WVRs IDS system.

From this matrix we will pick the three risks for further analysis. We will further analyze:

- Loss or shortage of personnel with regards to single point of contact.
- IT malfunction with regards to monitoring.
- IT malfunction with regards to compliance.

Controls

The driving force for managing these risks will be policy controls. While policy is not always an effective method for dealing with risk, it should work extremely well in this situation. Everyone involved in the WVR IDS system is part of some security group and/or has a security background. No other employees adhere better to policy than those that create it. If the risks lie in another area of OC or the WVR division, then controls other than policy would probably need to be implemented. In this respect, the NIDS committee is fortunate that everyone in question understands the need for policy.

The threat of loss or shortage of personnel could have disastrous effects on WVRs IDS system when it comes to a SPOC. The nature of the threat can come in several forms… sickness, vacation, death, termination. The vulnerability in this case is really the fact you have one person operating and maintaining the IDS system. There are a number of threats that could affect this vulnerability, but by far loss of personnel produces the highest risk to the IDS system. The likelihood that this will occur is very high. One of the forms of this threat is vacation, and everyone takes vacation at OC! Since this has such a high likelihood combined with the fact that the vulnerability affects WVRs highest ranked asset, the risk level is extremely high. The control selected for this risk will be a policy. The policy will state that no single person will be responsible for all aspects of WVRs IDS. The reason for this is to ensure that even is WVR suffers a loss of personnel, there will be someone around with enough knowledge to maintain the IDS system. A second reason for this control is not only knowledge, but also security. The control will be aligned to the segregation of duties standard in 7799. As such, it will split the operational and security duties of the IDS. The OC policy statement for this control is

> "Segregation of duties is mandatory for security functions: security functions must be segregated from normal administrative functions and performed only by Security personnel."[1]

The risk level after implementing this control will be low. This control has the added benefit of an immediate result and will buy WVR some time to work on

[1] Reference details removed to due to restricted information.

the control for developing the run books.

The second risk the NIDS committee will be dealing with is an IT malfunction with regards to monitoring. The nature of the threat in this situation comes from the fact that a malfunction of the NIDS system might go unnoticed. This risk comes about from the vulnerability of no person or team consistently monitoring the IDS system. The likelihood that this will occur is high. In the difficult world of intrusion detection it is all too common to have a misconfiguration that generates false positives and/or false negatives (missed events). This misconfiguration can easily be classified as an accidental IT malfunction. The risk level is also high due to the fact that this threat can allow the IDS data to be inaccurate. In other words, fail. This control will include the applicable OC Corporate Security 7799 policy as well as the creation of an information sharing database between the RAR team and the IM teams. The OC policy statement for this control is:

> "The system manager is accountable for ensuring that results from the security monitoring tools on OC systems are monitored, and all unexpected events detected by this monitoring are recorded and investigated promptly."[2]

The control has been selected to ensure all unexpected events are investigated and properly tracked. Since alerts will be more closely monitored by both security experts and incident handlers, there will be a greater chance of noticing something that is either present or missing due to an IDS malfunction. Since false negatives are extremely hard to track down, this risk can only be reduced to a medium.

The final risk that the ISMS will tackle is also an IT malfunction threat but in the vulnerability context of not having any compliance checking of the IDS system. The nature of the threat comes from mis-operational aspects of the malfunction. This could be a malfunction caused by placing sensors in the wrong location within the network, unplugged sensors, badly performing databases or network connections. This is a very different malfunction than a misconfiguration of the security settings within the IDS. The likelihood of this threat occurring is only medium. There are many parties involved that could accidentally do something to alter the IDS. This risk affects an asset with a sensitivity rating of 3. These two ratings give this risk a medium risk level. The controls in this situation will involve driving the OC 7799 policy down into the WVR division as well as socializing the policy to groups involved with the IDS system. The OC policy statement for this control is:

> "OC systems must be reviewed by mandated parties for compliance with security policy."[3]

The reason for selecting this control is ensure that a regular review of all aspects of the IDS system is completed. The risk level after this control is in place should drop to low. It will be low risk due to the heightened awareness of the

[2] Reference details removed to due to restricted information.
[3] Reference details removed to due to restricted information.

IDS system.

Part Three – Do

In the "Do" phase of developing an ISMS using the PDCA method, we will define the actual steps for implementing the controls to remedy the problems. In order to remain focused, we will continue to use the top risks identified in our planning phase. Initially we had areas of concern we wanted to tackle: Documentation, SPOC, monitoring and compliancy. After we completed our risk analysis, it was determined that documentation was not one of the highest ranked risks. The NIDS ISMS committee will focus on "Doing" the steps to mitigate the remaining three risks (problem areas).

Problem: The WVR NIDS system was implemented and is currently maintained by a single person in the WVR division. The most significant consequence of this is the threat of loss of personnel. The problem in this risk scenario would be no one knows how to operate the NIDS system. While other groups might know how to monitor the system, the operational aspect would be lost. A secondary problem with SPOC is the potential for all sorts of other threats to manifest themselves as risk levels as defined in table 3 (risk table).
Action: This issue addresses the problem by respecting and enforcing the OC Corporate Security policy on segregation of duties. While this policy is specifically geared towards segregation of duties in a security model, the NIDS ISMS will use it to ensure information sharing on all aspects of the NIDS system
Step 1: Obtain policy from OC Corporate security.
Step 2: Review policy with NIDS committee to determine if it will serve as an adequate control without modification. If, necessary, modify the policy to create a divisional policy.
Step 3: Determine if the control can be implemented with existing personnel resources or if additional resources are required.
Step 4: Divide duties and responsibilities among the resources.
Step 5: Setup recurring information sharing sessions between the resources facilitated by the NIDS ISMS committee.

Problem: The IDS system & alerts are not consistently monitored. At the onset of the ISMS design, this problem was mentioned as no clearly defined process for monitoring alerts. After the risk analysis, it became apparent that the largest risk in the area is the fact an IDS misconfiguration could go unnoticed. Once again, the issue is very specific to differentiating between an ISMS for the IDS and an ISMS for another system that relies on monitoring the IDS.
Action: The action for remedying this problem will come in the form of two controls. The first one is the typical policy pull from OC, while the second control is a technical control of creating an information sharing system between the RAR team and the IM teams.
Step 1: Obtain policy from OC Corporate security.
Step 2: Review policy with NIDS committee to determine if it will serve as an adequate control without modification. If, necessary, modify the policy to create

a divisional policy.
Step 3: Train RAR team for monitoring the WVR NIDS.
Step 4: Ensure consoles are available for RAR and correct access levels are granted.
Step 5: Obtain requirements then research and select an incident management (IM) tracking system.
Step 6: Implement IM tracking system and train appropriate groups on use.
Step 7: Setup recurring sessions with all WVR NIDS teams and IM teams based on the use of the IM tracking system.

Problem: The WVR NIDS system has never been checked or audited. Without an independent review, there could be serious problems with the IDS system as a whole. The initial speculation was that this would present itself in the form of a system wide configuration misconfiguration. After the risk analysis, it was determined that the most likely form of this risk would present itself as an accidental IT malfunction.
Action: As with the other two problems, a solid control policy is the best bet for checking our IDS system for compliancy. Once again, there is no point in reinventing the wheel and we will simply pull the appropriate policy from OC. The control will dictate the need for independent review.
Step 1: Obtain policy from OC Corporate security.
Step 2: Review policy with NIDS committee to determine if it will serve as an adequate control without modification. If, necessary, modify the policy to create a divisional policy.
Step 3: Develop a compliancy checklist for the IDS policies in question.
Step 4: Decide on the timing of the compliancy checks (Monthly, bi-annual, annual).
Step 5: Engage independent third party to perform compliancy checks.
Step 6: Review and correct any deficiencies found by the compliancy check.

The final stage in the "Do" phase is to apply the controls. In order not to get out of hand with which the controls do and don't apply to the WVR NIDS system, a statement of applicability needs to be determined. Rather than trying to list all aspects the controls cover, a different approach is listing the aspects that the controls don't cover.

The policy control for segregation of duties covers all management and security operational aspects of the IDS system. The exclusions from this are security monitoring personnel. This identified gap is due to the fact that the monitoring personnel are already a team (RAR) and have an existing load balanced workforce. The control that deals with compliance checking covers all aspects of the WVR IDS system. The main purpose of this control is to ensure that WVR does not end up in the same situation in the future. This OC policy control closely ties in and complements the "Check" cycle of the ISMS PDCA process. The only exclusion to this control is what happens to the alerts after they are

passed to the incident management teams. The technical control for implementing an IM tracking system will not be implemented despite the fact it plays an important role in incident management. The control will not be implemented because it has no direct impact on the IDS system itself. The impact of this control is on how the data is handled once it leaves the IDS system, as such, its focus is outside the IDS system, hence the control not being implemented.

Part Four – Check

The next step in the PDCA process is “check”. The WVR division has decided to fortify this phase of the process with an actual control. While this might appear as redundant, in fact it is not. PDCA is merely a process, not a standard. The standard is ISO 17799. In order to be inline with 7799, the compliancy control will be implemented as mentioned in the “planning” & “doing” phase. The beauty of this control is that it can be enforced by the NIDS ISMS committee regardless of the process used to develop the ISMS.

In this section, we will develop audit checklists for the three controls implemented and describe how the checklists will improve the overall system.

Control: Segregation of duties.
Objective: To ensure that a single person does not have exclusive knowledge and control of the WVR IDS system. This is an important objective for preventing abuse/misuse and ensuring continuous system operation.
Audit questions need to be asked during separate interview processes with all parties involved to the WVR IDS system.
Audit question #1: Are the administrative, management and security functions of the system performed by different people and/or teams?
Audit question #2: Is there a single person who could alter the system in such a way that no one else could gain access?
Audit question #3: Is there a single person who is depended upon for operation of the IDS system?
Audit information #1: From the system under review, obtain a user list showing the roles (privileges) that each user has in the system. Is there a user that has excessive privileges?
Audit information #2: From the system under review, obtain audit trail information that contains system modification information (who, what, when). Are there any entries that where a user has exceeded his/her authority for making changes to the system?

Control: System Monitoring
Objective: To ensure IDS alerts are monitored on a consistent regular basis. The importance of this objective comes from the ability to spot system malfunctions during routine monitoring of system alerts.
Audit questions need to be asked exclusively to RAR team members during separate interview processes.
Audit question #1: Are alerts from the system monitored on a regular basis? If so, how often?
Audit question #2: Are alerts ever flagged & investigated as abnormal outside of the need for security monitoring? In other words, are unexpected results documented & reported to the system operators and/or system managers and/or system administrators?

Audit question #3: Are members of the team routinely trained in use of the system and what constitutes unexpected behavior.
Audit question #4: Do members of the team receive feedback from the system operators and/or system managers and/or system administrators on the unexpected behavior previously reported to them?
Audit information #1: Perform monitoring of the system for a period of 24 hours. Are there any unexpected alerts which could indicate a malfunction of the system?
Audit information #2: Deliberately inject a malfunction to the system. The malfunction should significantly alter the information presented to the team. Does the team react as expected? In other words, do they correctly differentiate the malfunction from an incident and/or security alert?

Control: Compliance with security policy.
Objective: The objective of this control is to ensure that the system is consistently operated in a manner that is inline with the policies set out within the ISMS. The importance of this objective comes from ensuring the system is properly maintained and provides accurate data.
Audit questions need to be asked during separate interview processes to all members of NIDS ISMS committee.
Audit question #1: Does the system have regularly scheduled reviews for compliancy to the policies and controls set forth in the ISMS? If so, how often are the reviews.
Audit question #2: Does the system committee review the findings from the compliancy reviews and take corrective action if necessary?
Audit question #3: Does the committee maintain past copies of the audits for historical review?
Audit question #4: Is the system operated and maintained in a manner that meets the requirements of the security and incident handling teams?
Audit information #1: Obtain historical copies of the audits. Have issues previously identified been resolved?
Audit information #2: Obtain general architectural information of the system. Have any changes been made since the last review that could significantly alter the data the system presents to the various teams?
Audit information #3: Obtain specific architectural information of the system such as database characteristics, sensor placement, server & console performance. Are all the components of the system functioning in a normal and expected manner?

The checklist provides a total of eighteen items to be checked out of three control areas. The checklist is combination of both interview type information gathering and qualitative analysis of the system. The checklist will be used to improve the system by identifying areas of the ISMS that do not meet the OC 7799 based policies. Since all of the controls for WVRs IDS system are policy based, checks need to be there to ensure that the policies are being followed.

In all instances of the checklist, the NIDS committee will be informed of the findings and have the power to correct any deficiencies. The final power of the checklist comes from its self assessment capability. Even though the checklist is designed for use with an independent reviewer, it can be enacted by the WVR NIDS committee for adhoc reviews of some or all of the controls in place.

Part Five – Act

In the final round of the PDCA process for building an ISMS we put on a continuous act. In this phase, we will describe how the committee will maintain and/or improve the ISMS. We will also cover any changes that could be made to the WVR NIDS information system to facilitate compliancy and/or ensure that problem areas don't develop again.

Since the WVR division and OC will be investing significant resources on this ISMS, a priority will be to make sure the ISMS does not fade away or become outdated. This responsibility will lie with the NIDS committee. This committee itself has the chance to fall apart if not properly maintained. There is no silver bullet for keeping interest and focus on an ISMS once it has been developed. However the ISMS for IDS has a distinct advantage. The people involved are all security professionals and therefore have a vested interest.

One of the ways to leverage this interest is to identify areas of concern that have a lower risk level than the top three. An example of this would be working on the lack of documentation vulnerability. Even though it was initially identified as a problem, the risk analysis during the planning stage indicated we should focus on other areas of the system. Now that the committee has those areas under control, it is time to go back and tackle some of the lower vulnerabilities. A substantial area of input into this process will come from the compliancy reviews. The expectation is that the reviews will provide a continuous list of areas where controls need to be implemented. Secondary information streams will come from the users of the IDS. While certain members of the user team will be on the ISMS committee, a significant number will not be on the committee. Far from brushing these people aside, they will be encouraged to submit ideas to the ISMS NIDS committee for improving the policies and controls which govern the NIDS system. The key element for maintaining and improving this specific ISMS is to leverage the security professional aspect and foster an environment of continuous improvement.

During the "act" we also want to seek out and recommend improvements to the system itself. While the main focus of the ISMS and the committee is information security, the committee should always be on the lookout for changes that can be made to the information system to facilitate security. In the case of the WVR NIDS, a major change could be made to allow for better and easier information security.

The most significant change would be to give complete NIDS control to the OC Corporate Security group. The WVR division leapfrogged OC as a whole when putting NIDS in place. As such, it has created a virtual IDS island within the sea of OC. The complication here has been evident several times through the ISMS design. By giving total control of the NIDS system to OC, it will be in a department that has significantly more resources and expertise than WVR could

ever provide. This is a change to the management of the IDS information system itself, not the ISMS.

Another change that could be made is to the information processes that use data from NIDS. This change would need to be evaluated in more detail to see if it would yield actual improvements. In essence the data generated by the IDS would be available to other teams for there own purposes. Currently, all IDS information destined for OC flows out from the RAR team. Altering this process might provide more power to the incident management teams and/or other teams that would use the IDS data. The idea that this process might yield a positive improvement comes from the fact that an even bigger community now provides feedback onto how the IDS information system is run. A larger community providing feedback should yield a larger pool of ideas to implement for the better.

Ensuring good solid open communications within the ISMS committee and between all parties involved with the WVR NIDS system will provide excellent opportunities for the ISMS to flourish. It is also very important in the final "Act" not to lose focus on the scope of the ISMS. That is, it is an ISMS for an IDS system, not an ISMS for some other system that makes use of data from the IDS system. An ISMS that makes use of IDS data would have been significantly different from this one. It would have contained many sections on detecting and responding to incidents for the specific system it was created for.

Endnotes

[1] "Introduction to BS7799 and ISO 17799 - Plan Do Check Act".
URL:http://www.induction.to/bs7799/pdca.htm (6 January 2005).

[2] Vidalis, S & Jones, A. "Using Vulnerability Tree for Decision Making in Threat Assessment". June 2003.
URL:http://www.glam.ac.uk/soc/research/publications/technical/CS-03-2.pdf (8 January 2005). p.4.

[3] "Threat and Risk Assessment Working Guide" – Annex A. October 1999.
URL:http://www.iwar.org.uk/comsec/resources/risks/itsg-04e.pdf (7 January 2005). p.73-75.

[4] "Threat and Risk Assessment Working Guide" – Annex H. October 1999.
URL:http://www.iwar.org.uk/comsec/resources/risks/itsg-04e.pdf (7 January 2005). p.39.

References

Arveson, P. "The Deming Cycle". 1998. URL:http://www.balancedscorecard.org/bkgd/pdca.html (4 January 2005).

Hoelzer, David. "Introduction to BS ISO/IEC 17799: Policy, ISMS and Awareness". 2004.

"Track 11 – SANS 17799 Security & Audit Framework" SANS. 2004.

Ringel, M & Limoncelli, T. "I Adverse Termination Procedures -or- "How To Fire A System Administrator"". URL:http://research.lumeta.com/tal/papers/LISA1999/adverse.html(4 January 2005).

"Information technology – Code of practice for information security management" ISO/IEC. 1 December 2000.

"Vulnerability and Threat Identification" Information Resources & Communications. 18 August 2004.
URL:http://www.ucop.edu/irc/itsec/vulnerability.html (8 January 2005).