

OPERATIONS MANUAL Stage Two - Integrative

Hal Flynn 2000-05-11

OPERATIONS MANUAL Information Protection Center

Stage 2 - Integrative

Scope of Improvement: At the Integrative stage the IPC either has direct or collaborative effect on passive security (policies and awareness), active security (IRT) as well as architectural decisions. The IPC has become a center of security excellence which has a say in all aspects of security. More importantly, it is in close working relations with the business managers, helping them with security solutions which enable their operations. It is only at this stage that the IPC can be truly proactive.

Architecture: The architecture begins with a vision which identifies the organisation's defining goals. A set of principles are established to achieve those goals. Policies further refine or constrain the organisational environment.

Strategic plans and a business model are the planning vehicles for achieving the organisations goals. The information or technical architecture is the implementation in technology of processes and tools to support the organisation in meeting its goals. Limitations in technology or resources force the organisation to accept intermediate compromises as they evolve toward the target architecture.

During this planned evolution there will be changes in what technology can deliver and possibly changes in the organisation's goals. An Advanced Architectural Working Group is required to track technology forecasts, evaluate new capabilities and propose changes to business strategies and/or the architecture to improve the organisation's capabilities in meeting its goals.

- There are four components which make up a comprehensive structure for architectural decisions. These are Principles, Standards, Models, and Inventory. These components were defined as:
 - Principles are the most important components. They are based on the values of the organisation. (i.e., the degree of risk acceptance, trust placed in employees, etc.) They drive all other aspects. They must be distinctive and few in number (i.

- e., specific enough to drive the behaviour)
- Standards are specific rules or guidelines for implementing the models.
- Models are pictures of the desired structure, with emphasis on what goes where and how it is all connected.
- Inventories are the least important. They must include only key components that are currently used within the environment.
- The design approaches of architectures are specifically aimed at enabling information systems to respond rapidly to the changing information needs for the Organisation's business functions.
- All architectures consider technological trends and their relative availability as well as their implicit complications to arrive at the following objectives:
 - Applications will be designed to operate effectively in a three tier Client/Server structure within distributed LAN/WAN environments.
 - Designs of applications that makes maximum use of sharable utilities like objects.
 - The resulting facilities will maintain an environment of common reference data and directories.
 - Security will be provided at multiple levels, based on the critical nature of the process or data being accessed.

Architectural Configuration: The IPC's activities in environmental scanning and VA give it a unique and integrated view of the organisation's security posture. The IPC will recommend new security technologies to the Architecture Configuration Control Board (ACCB). This board is ultimately responsible for the change management process that enables the overall organisational architecture to evolve and still maintain a secure baseline posture. The ACCB needs to document the network topology and IP addressing. This is an absolute necessity since the ACCB can only manage what it knows. The ACCB must manage the IP Registry and control the network topology as part of the security baseline. This management extends over those support organisations that implement IP allocation and network topology.

The ACCB requires approval of its Terms of Reference by the Organisation's Senior Management Board. The ACCB Terms of reference include the following:

- establish operational policy that requires that remote exploits that degrade the integrity of the perimeter be addressed ASAP while those that could be exploited within the perimeter be addressed within 30 days
- establish and manage versions of software as standards

- oversight of design and implementation of extranets
 - provide verification of policy conformance
 - review and approve preliminary and final network plans as well as security controls
 - discuss any special security considerations (e.g., privacy, confidentiality)
 - periodically review 3rd party connections
- assist with product selection evaluations
 - what is business need
 - what supporting technology is required
 - what special requirements (e.g., exceptions at perimeter, remote management capability)
 - require access to sensitive information
 - what security measures or controls are included
 - who has tested or evaluated it
- use the outcome of Threat and Risk Assessments (TRAs) to establish priorities for addressing risks and propose solutions such as:
 - further network intrusion detection systems
 - host-based intrusion detection (e.g., tripwire, swatch, TCPwrappers, etc.)
 - special file auditing (e.g., /etc/passwd, /etc/group, /.rhosts or /etc/hosts.equiv)
 - requirement that network logs record:
 - service initiation requests
 - user/host requesting service
 - network traffic
 - new connections
 - connect durations
 - use of ntp to synchronise time across environment
 - facilitates tracking of events across logs of different hosts
 - stronger case where prosecution warranted

Risk and Priority List: The VA results and an understanding of the architecture's technical implementation allow the establishment of the organisations risks. An analysis of these risks and the measures that can be used to mitigate them is called a Threat and Risk Assessment (TRA). The TRA is used by the ACCB to set the priorities for addressing these.

- the policy requires each Departmental Manager to have an up-to-date statement of sensitivity (know what they have and the value of what they have) and to carry out a TRA on each system under their control

- the risk and priority of addressing that risk comes from a trade-off analysis that balances the cost of protection Vs. cost of incident

[Admin](#) [Passive](#) [Protective](#) [Detective](#) [Assessive](#) [Responsive](#)

Original development of these pages was supported by
the Province of Manitoba

The content is maintained by [Andrew Mackie](#)

Last modified: April 29, 2000

[Privacy Statement](#)

Copyright 2006, SecurityFocus