Global Information Assurance Certification Paper

GIAC Security Leadership Certificate (GSLC)
Practical Assignment
Version 1.0 (April 8, 2002)

Establishing A Security Operations Group

Bob Isaak
December 28, 2003

Establishing a Security Operations Group 3
Summary 3
Introduction 4
Operating Charter 5
Membership & Linkages 5
The Security Steering Committee 5
The Security Council 5
Security Operations Group – Illustration 6
Security Operations Group 6
Roles and Responsibilities 7
Due Diligence & Gap Identification 7
Vulnerability Management 9
Policy Compliance 11
Intrusion Detection and Prevention 12
References 13
Appendix 1 Vulnerability Assessment Process 14

Establishing a Security Operations Group

Summary

Corporate IT environments are increasing dependant on their IT infrastructure and this infrastructure is under constant probing and attacks by serious hackers intent on corporate espionage or others with less malicious but equally disruptive motives.

Corporate security groups lack operational focus and awareness and are challenged in their existing roles to deal with the rapid identification and exploitation of hardware or software vulnerabilities.

Business pressures have stretched day-to-day operations resources that are often skilled but unaware of security issues.

A gap exists between corporate security and day-to-day operations teams. This gap is the implementation and maintenance of a corporation's desired security baseline. This gap can be addressed by a small group of highly skilled technicians with a passion for security. Depending on how the IT vendors respond to this problem this group may be a temporary organizational unit or it may end up being an added cost of doing business.

The following discussion looks at the formation of a small group of technicians focused on security operations and also some of the start up tasks that this group will undertake once they have been established.

Introduction

The process of putting security infrastructure and practices in place and ensuring they are adhered on a day to day basis is, rightly or wrongly, often beyond the capabilities and mandate of the security department in large corporations. Corporate security is often concerned with creation of policy, legal and privacy issues, fraud investigation, periodic audits, communication and compliance with external regulatory bodies and incident investigations. Typically they would not be involved in the day to day maintenance of corporate systems which can change from day to day and as a result the security profile may drift off what was established during the last periodic audit.

The implementation of corporate security policies and practices is often left to the day to day operational staff for execution. While this may seem like the appropriate place it may in fact not be the best fit. While the technical skills of the operational staff are adequate for the security tasks; the demands on their time or other priorities may detract them from ensuring that a security perspective is reflected in the configuration of the systems under their control.

The focus of the day to day operational effort is often directed at making something work, allowing access to systems or files, enabling a service, opening a connection between two points on a network or helping end users with their computing problems. These day-to-day tasks may often be executed in a number of ways but often the most expedient path is chosen at the expense of the security posture.

Taken in isolation a single change, which deviates from the secure alternative may not significantly alter the security posture. However taken in aggregate the changes that occur daily can significantly alter the security posture over a relatively short period of time. This deviation would not be picked up by corporate security until its next scheduled audit if at all, and this may only occur annually.

Another factor, which contributes to the notion that day to day operational staff may not be the most appropriate upholders of security, is the rate of change in security issues that is in effect today. If operational staff are not vigilant and conversant in the security issues of the day they will be unaware of gaps that may have appeared in their environment. The time required to maintain this up to the minute awareness may exceed what is available to the day-to-day operations staff.

The principle of segregation of duties is also a contributor to the difficulty that day to day operations staff may have in maintaining a secure environment.

In recognition of the focus of Corporate Security and the demands on the often-stretched resources of the day to day systems administrators the establishment of a team of skilled systems administrators who are focused on security issues seems justified. The following discussion presents how this organization might be positioned, the corporate linkages it will need, and an outline of two of its initial tasks, Due Diligence & Gap Identification and Vulnerability Management.

Operating Charter

In the publication, *Information Protection Center (IPC)* [1], the author offers the following mission statement, which provides some insight into the mandate of this security operations group:

- ***To protect The Company's Networks, Assets, Revenue and Corporate Image by continuing to find and address vulnerabilities in networked computers and systems and thereby improving The Company's overall security baseline;***
- ***To detect misuse of, or attacks against, The Company's networks and respond to minimize the impact of these security incidents;***
- ***To provide assistance to operational teams to correct deficiencies in system configurations;***
- ***To provide a single point of contact for operational security issues within The Company***

Membership & Linkages

The diagram and the group definitions below illustrate how the group would be positioned in a large organization.

The Security Steering Committee

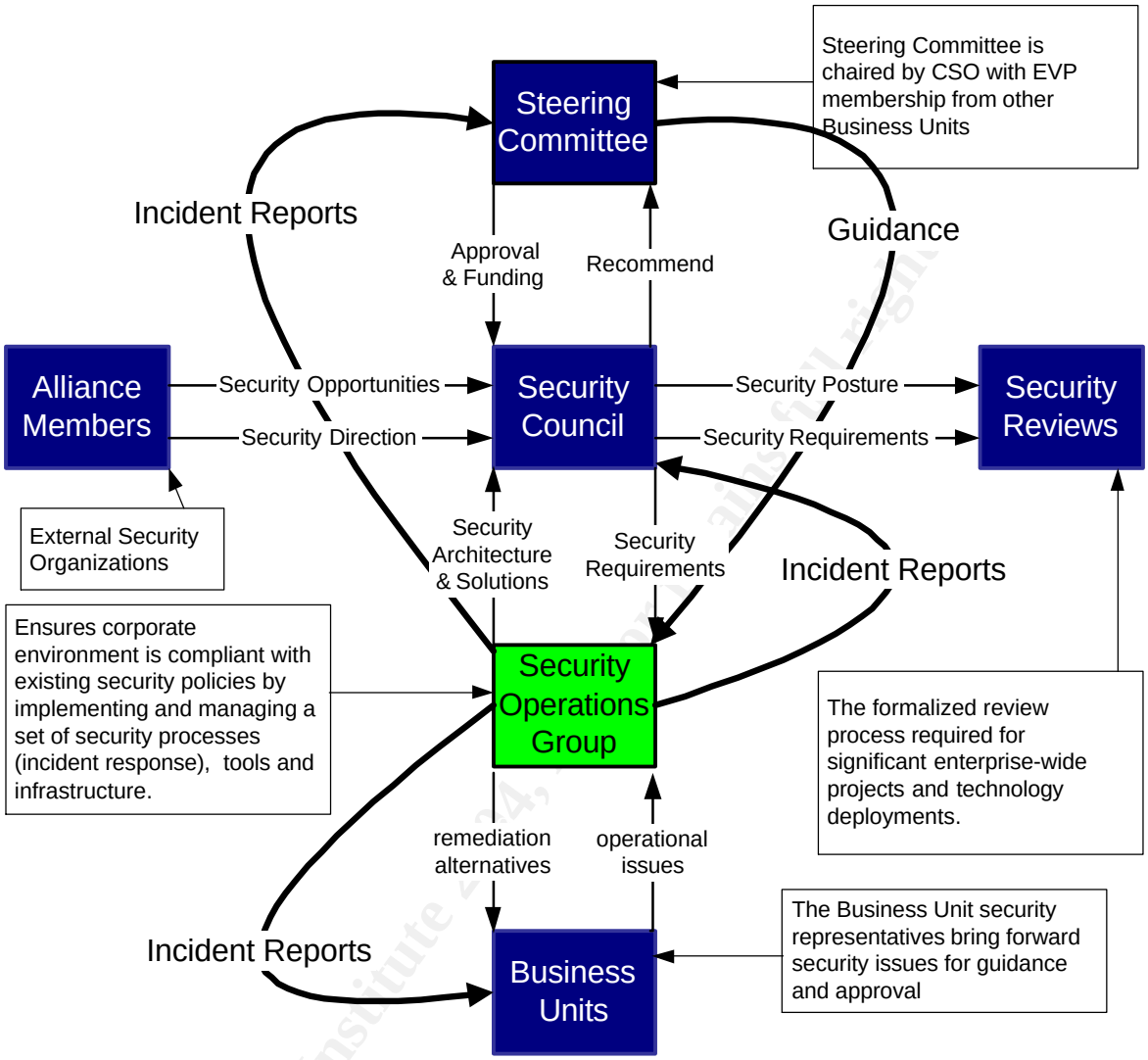
Membership from across the corporation who are at the Executive Vice President Level, which ensures that security concerns receive executive support, direction and funding. Awareness of the issues and alternatives would be one of the deliverables back to this group.

The Security Council

Members are Director Level positions and are drawn from across the organization including sales and marketing. Corporate wide security issues are discussed and agreed upon at this level. Examples of this would be a corporate wide end user security awareness-training program or the adoption of a new technology such as SSL or IPSEC VPNs.

[1] Information Protection Center (IPC) Operations Blueprint, Andrew Mackie, November, 2001 http://members.rogers.com/amackie/ipc/OPS-man-admin.htm

Security Operations Group – Illustration



Security Operations Group

Membership is taken from senior technical resources that have an aptitude for security issues and technologies. The individual members would come from a cross section of the operating units and would be representative of the technologies in use by the corporation. Equal representation from the Intel, UNIX, Network, Application, Mainframe and Midrange areas would be required as a starting point. The eventual weighting of each area would be dependent on how reliant the corporation is on the specific platform.

The role of this group would evolve along with changes in the security environment. While the group would be free of day to day maintenance requests and trouble tickets it would need to be aware of day to day issues.

This awareness of day to day issues is a critical factor in this group's ability to achieve is goals. It must be aware of the demands the corporation is placing on its IT assets and staff and must be able to layer the security perspective on top of the corporate demands. Strong ongoing linkages with other business units would be an essential responsibility of the Security Operations Group.

Roles and Responsibilities

Once established and staffed this group would start by going through and exercise of due diligence and gap identification. In parallel the ongoing management of vulnerabilities would be a critical task on this groups list of activities.

Due Diligence & Gap Identification

Prior to implementing any new technologies the Security Operations team will need to gain a thorough understanding of its existing environment. As a starting point the following questions can be asked:

1. What policies exist today?
2. Are they being enforced?
3. What systems are in place?
4. How are the systems prioritized?
5. Have the base operating systems been hardened?
6. What is the patching policy or standard?
7. Has the network been segmented to protect core assets and,
8. What ports and protocols are allowed to traverse the network?

Systems should be examined with the objective of fully exploiting whatever security capabilities the systems have. An example of this would be identifying the required operating system services that are required for the role or intended application of a server and removing or disabling all others. This default deny stance should be exercised wherever possible.

In an article published by Peter Tippett entitled *Sweat the Small Stuff*[2] the author states: "Collectively, the five simple preventative measures below will reduce risk in an average organization by 10 fold or more."

> *FIVE EASY PIECES*
> *1. Turn off unneeded services in boxes attached to the Internet.*
> *2. Never use a Web server for anything else.*
> *3. Regularly apply security patches to critical machines.*
> *4. Block all executable attachments at the gateway.*
> *5. Use screen saver lockouts.*

Whether you believe the risk reduction claims or not there is little argument against the benefits that would accrue to the organization that ensured that

[2] Tippett, Peter, M.D., Ph.D., Sweat the Small Stuff: Making your Enterprise More Secure with Less Effort

the technologies in use today be configured in a secure way. Some examples of what can be done with little or no additional infrastructure are summarized below:

- **Establish or update your security policies.**
  - Establish or update security policies for all platforms and applications
  - Policies should be clear and concise
  - Policies should be enforceable
  - Policy audits should be done continuously if practical or at a minimum quarterly.
  - Based on Industry Best Practices

  "The majority of vulnerabilities are the result of misconfigured systems, networks and user constructs. There are hundreds of system settings that must be managed to achieve a secure environment."[3]

- **Prioritize the environment**
  - Conduct an inventory of infrastructure and applications
  - Determine infrastructure classifications
  - Group servers and desktops according to classification

  A Gartner research note published in September 2003 by Mark Nicolett and John Pescatore advocates that security professionals *"…need a way to prioritize the mitigation of vulnerabilities. Mitigation efforts should be prioritized based on potential business impact and the probability that a vulnerability will be exploited."*[4]

- **Harden operating systems**
  - Identify role of platform
  - Start with vendor recommendations for role of platform
  - Customize to ensure compatibility with applications.
  - Incorporate into base operating systems images for role

- **Segment the network**
  - Network infrastructure should be implemented so that critical assets can be logically or physically separated from non-critical assets. Establish trusted and non-trusted guidelines and move infrastructure into the appropriate zones. An example of this would be the DMZ where Internet facing infrastructure might be located. Another zone could be designated for wireless access points that are made available to contractors or visiting vendors.

[3] Nicolett, J. Pescatore, Gartner Group: **Specific Vulnerability Management Functional Requirements**, TG-20-7277M, September 11, 2003.

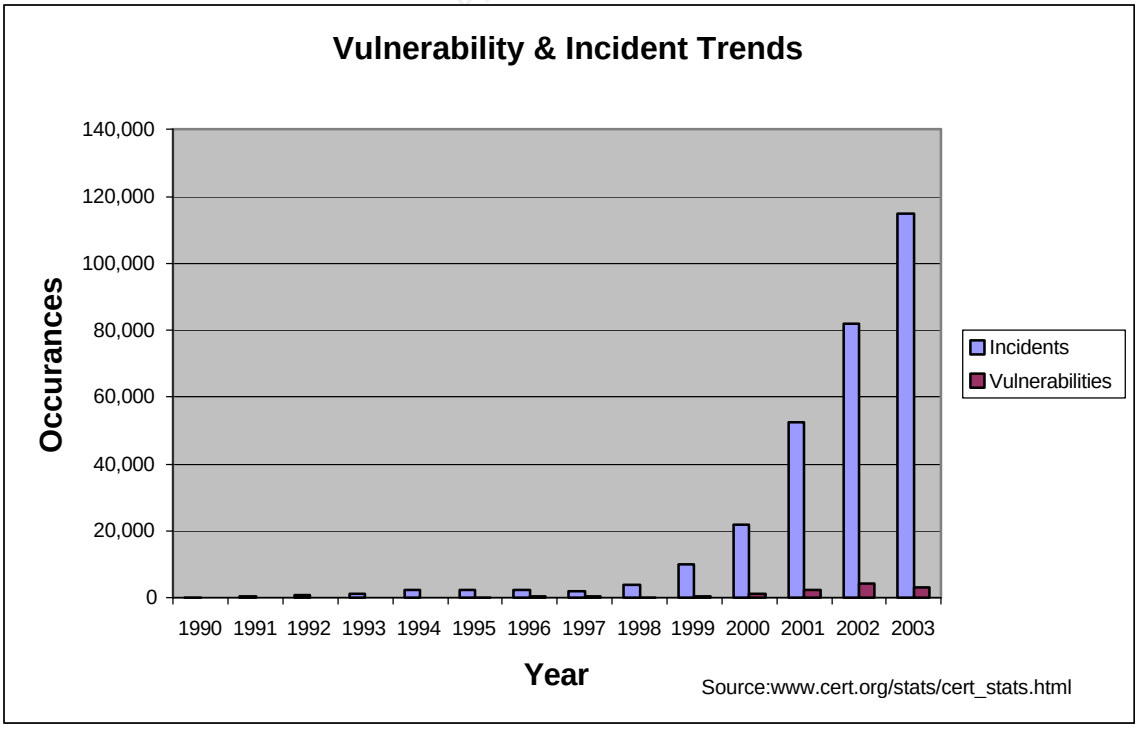
[4] Nicolett, J. Pescatore, Gartner Group: **Specific Vulnerability Management Functional Requirements**, TG-20-7277M, September 11, 2003.

By undertaking an examination of this kind, a thorough knowledge of the systems and configuration of those systems will be gained. In addition awareness and an understanding of any security gaps will allow for more targeted solutions to be sought. At the conclusion of this self-examination exercise and fully utilizing the security measures that are available in existing systems and infrastructure, new technologies can be examined to address any remaining gaps.

One of the areas that will emerge as a priority is how to keep track of all the vulnerabilities that are not only published but that exist in your corporate environment. In addition it is necessary to track the remediation effort that is planned for all vulnerabilities. The next section will look into the second start-up task of the newly formed Security Operations Group and that is the area of Vulnerability Management. The tools and processes that are available to assist in keeping this under control will also be presented.

Vulnerability Management

The following graphic[5] shows that while the number of vulnerabilities has shown a modest decrease in the last 2 years the number of incidents has risen dramatically. This trend supports the view that in spite of a decrease in published vulnerabilities the associated incidents arising from them is a growing problem.



[5] www.cert.org/stats/cert_html

Users of technology today are constantly being made aware of flaws in the technology that they have chosen to use in their respective environments. The flaws are not confined to any particular application, operating system or piece of hardware rather they exists across all vendors and all platforms.

Recent business & political events have heightened the efforts to find and publish vulnerabilities that exist within computer systems in use by businesses today. Technology vendors have been forced to release an increasing number of fixes or patches to remedy published vulnerabilities in their respective systems. Corporations are on the receiving end of these efforts and end up chasing the seemingly endless patch releases.

Administrators of computer systems these days are under pressure to implement the latest fixes if they wish to limit their exposure to known vulnerabilities. This pressure to patch leads to the fact that systems administrators are spending more and more time patching or replacing their systems to maintain a desired security posture. The rapidly escalating number of vulnerabilities and the cost of remediation efforts require companies to have in place a solid set of processes and tools to control the spiralling costs of this risk mitigation effort.

Vulnerability management is not limited to being aware of vulnerabilities, determining your exposure to them, and downloading the appropriate patches.[6] The process of managing vulnerabilities is a process where all vulnerabilities are recorded, quantified, prioritized and for which the remediation plans must be assigned and tracked. If a patch is currently deemed to be unnecessary, will it stay that way, or will a subsequent exploit take advantage of an old vulnerability. The vulnerabilities need to be documented and affected systems need to be identified and tracked should the priority of the vulnerability change.

In a similar fashion, vulnerabilities that affect hundreds or even thousands of systems need to be managed to the point where all vulnerable systems have either been remedied or in some way have the vulnerability mitigated. This requires a process and or an automation tool to record how many instances of a vulnerability exist within the organization, who has been assigned to apply the fix or patch, what progress is being made and how do you ensure that the patch has been correctly applied.

Once a patch has been applied to production systems, is there a process to update server and desktop base images so that newly deployed machines do not reintroduce the vulnerability into the environment. How are laptops that are returning from vacation or other absences dealt with. A Vulnerability Management Process as illustrated in Appendix 1 and a set of tools for

[6] Berinato, Scott, **Patch and Pray**, CSO Magazine, August 2003, http://www.csoonline.com/read/080103/patch.html

assessing and managing vulnerabilities will be needed if this component is to be dealt with satisfactorily.

Vulnerability Assessment and Management tools (VAM) are being developed by a number of software vendors a few of which are listed below.

Company	**Product Name**	
TruSecure	Alert Manager	www.trusecure.com/products/index/shtml
Foundstone	Remediation	www.foundstone.com
Tenable	Lightning Console	www.tenablesecurity.com/products.html

There are a considerable number of vendors who offer vulnerability assessment services but few at this point offer services that not only detect vulnerabilities but also manage the remediation or mitigation of that vulnerability and ensure that remediation efforts have in fact been implemented.

Maintaining an awareness of the number and severity of vulnerabilities is another component of Vulnerability Management and a key responsibility of the Security Operations Group. The following is a list of some of the vulnerability alerting services available today.

CERT	http://www.cert.org/nav/index_red.html
Symantec	http://www.securityresponse.symantec.com/
TruSecure	https://www.trusecure.com
SANS	http://www.sans.org
CVE	http://www.cve.mitre.org/
CIS	http://www.cisecurity.org/

Upon completion of the two areas discussed (Due Diligence & Gap Identification and Vulnerability Management) the Security Operations Group will have made significant strides in improving their organization's security baseline. The groups focus can now shift to researching the available technologies that will address the Gaps identified in the initial phases of this group's activity. Among the technologies that might be investigated the following two, Policy Compliance and Intrusion Prevention would both merit investigation for implementation in the near term.

Policy Compliance

This tool would be operational in nature and would conduct continuous scans of the environment to identify, track and report on exceptions to published Corporate Security Policies. Of significant interest here is the possibility that users with local admin accounts on their desktops have disabled, changed or removed the Domain Admin account on their desktops. The removal of the Domain Admin account will significantly alter the vulnerability scanning efforts not to mention the patch deployment activities, which are required to address vulnerability management efforts.

The fact that a user has local admin privileges is also worth questioning. As long as there is a single user in the environment who can convince management that they require local admin rights there will be potential problems with systems configured in this way and mitigation steps should be taken to protect against problems from these sources.

Intrusion Detection and Prevention

The number and distribution of an enterprises IT assets make it a considerable task to successfully deploy a single patch to 100% of the affected systems within the Corporate Network. This fact plus the volume of patches that are being issued by vendors make it very difficult to remain current on all patches in all systems on all platforms. All of this points to a Gap that can be addressed by Intrusion Detection and Prevention technologies. Significant strides are being made in this area and in particular the Intrusion Prevention vendors are developing high quality products that will be available in the very near future.[7]

There are a number of other technologies and activities that can add value and which one is selected will depend on what is already a part of a Corporations security infrastructure.

The important point to conclude with is that to establish and maintain a respectable security posture today will require a dedicated team of senior system specialists with widespread links into all areas of the corporate environment. This team will establish, maintain and update the tools and processes that will be required to manage the IT environment from a security perspective. The length of time that it will be necessary for this operating unit to be in place will depend on a number of factors. The most significant one is the changes that software and hardware vendors will be called on to make to their products to address security vulnerabilities. These changes will be and should be demanded by all businesses who rely on their IT infrastructure for, or in support of, their revenue generating activities.

Equally important is how effective this team will be in increasing the security awareness not only to the end users but also to other systems administrators who are not as focused on security issues. If all systems administrators were aware of the issues and were allowed the time to make their configuration set-ups and changes in a secure way, the need for this group would be reduced if not removed entirely.

[7] Nicolett, Mark, Pescatore, John, Stiennon, Richard D., Hallawell, Arabella : **Management Update: Security Infrastructure will focus on Intrusion Prevention**. November 26, 2003

References

Berinato, Scott, **FrankenPatch**, CIO Vol 17 -No.3- November 1,2003, http://www.cio.com/archive/110103/security.html

Berinato, Scott, **Patch and Pray**, CSO Magazine, August 2003, http://www.csoonline.com/read/080103/patch.html

Mackie, Andrew: Information Protection Center (IPC) Operations Blueprint, November, 2001 http://members.rogers.com/amackie/ipc/OPS-man-admin.htm

Nicolett, Mark, Pescatore, John, Gartner Group: **Specific Vulnerability Management Functional Requirements**, TG-20-7277M, September 11, 2003.

Nicolett, Mark, Gartner Group: **Predictions for IT Security Directors in 2004, December 8, 2003**

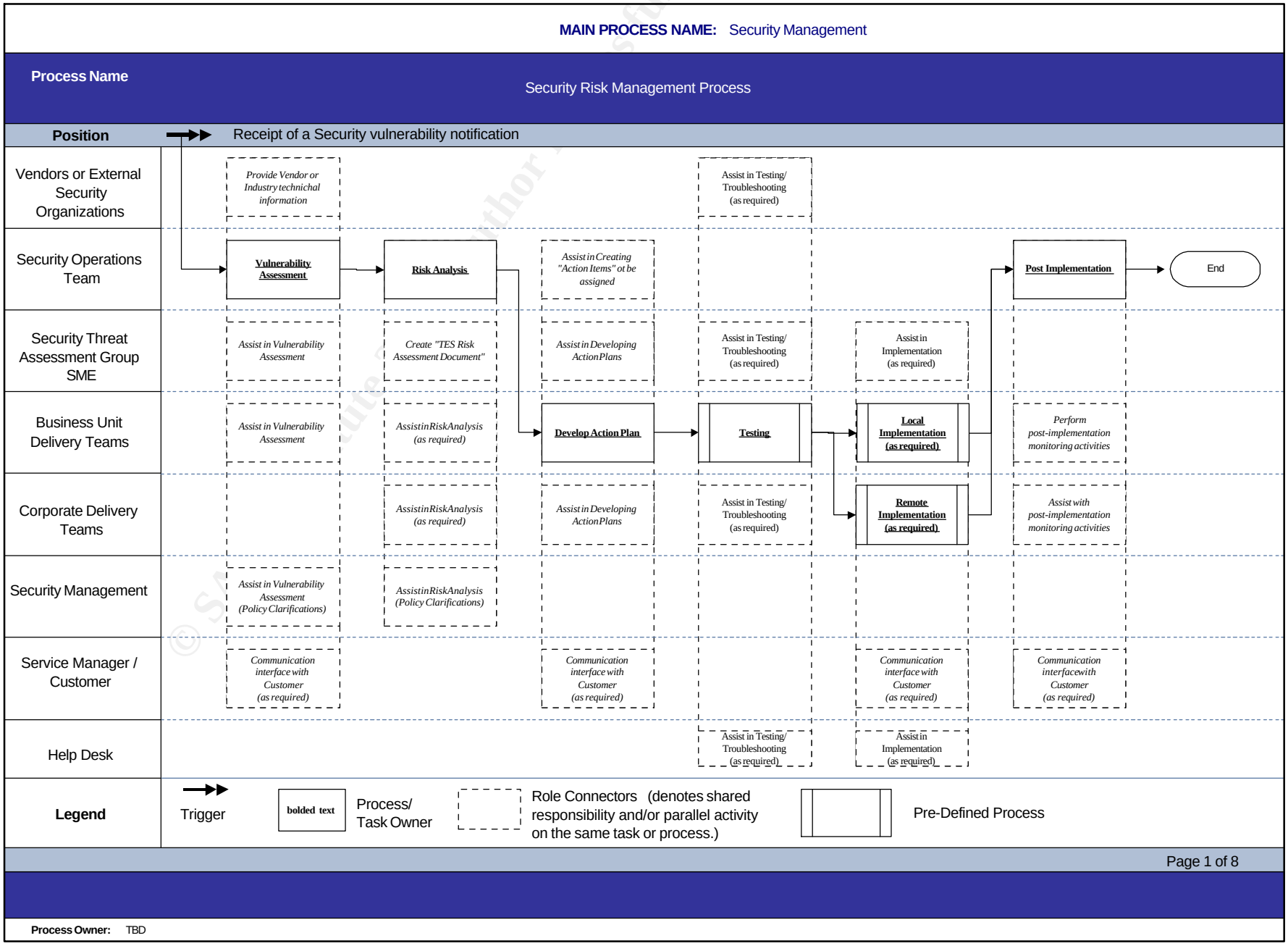
Nicolett, Mark, Pescatore, John, Stiennon, Richard D., Hallawell, Arabella Gartner Group: **Management Update: Security Infrastructure will focus on Intrusion Prevention**. November 26, 2003

Spafford, George, **Don't Patch and Pray**, CIN CIO Information Network http://www.cioupdate.com/trends/article.php/3065821

Tippett, Peter, M.D., Ph.D., **Business-Driven Security: A Risk Mitigation Approach**, September 2002

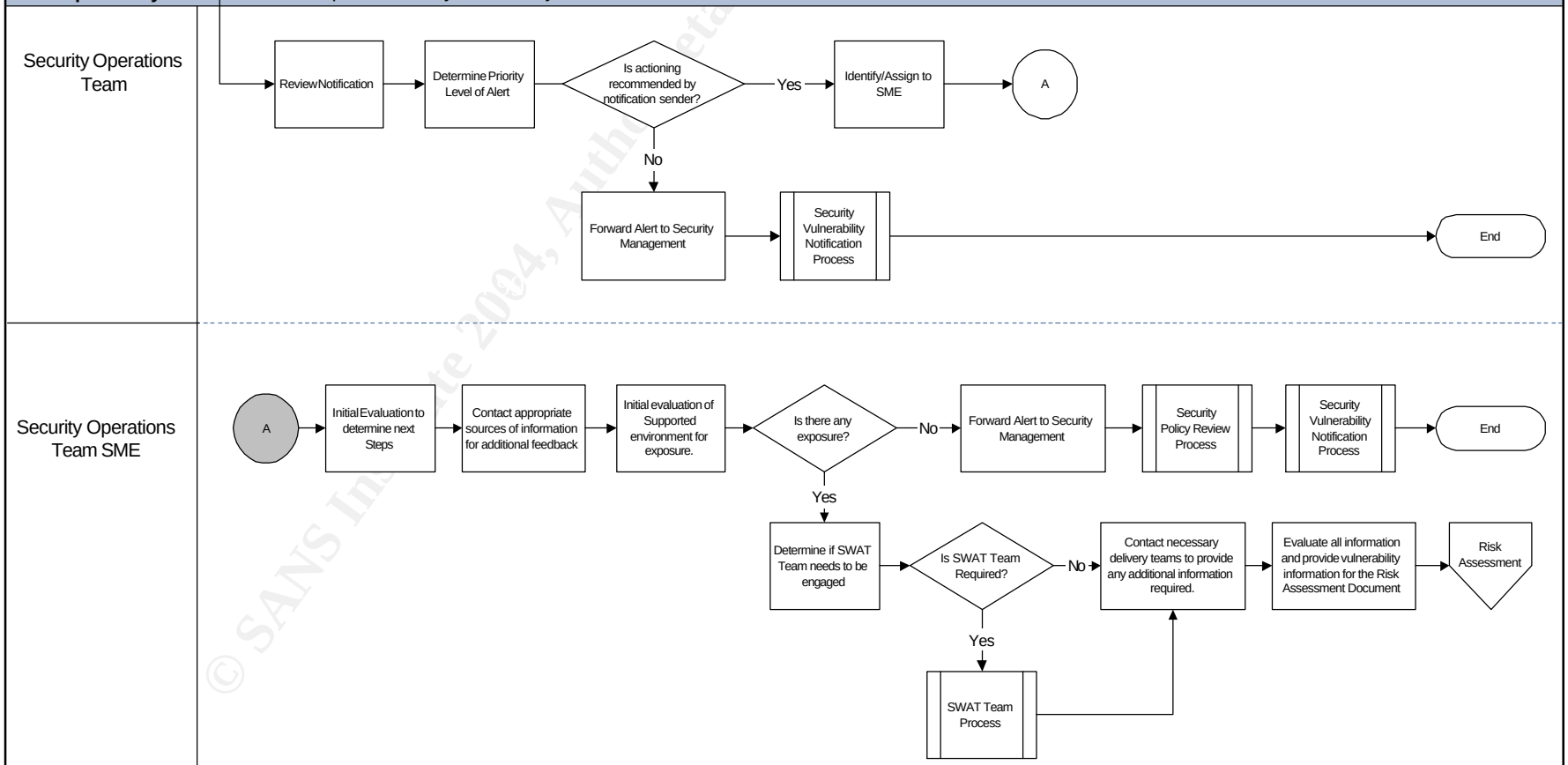
Tippett, Peter, M.D., Ph.D., **Sweat the Small Stuff: Making your Enterprise More Secure with Less Effort**

Appendix 1 Vulnerability Assessment Process



Sub-Process Name: Vulnerability Assessment Process

Responsiblity → Receipt of a Security vulnerability notification



Legend

Trigger

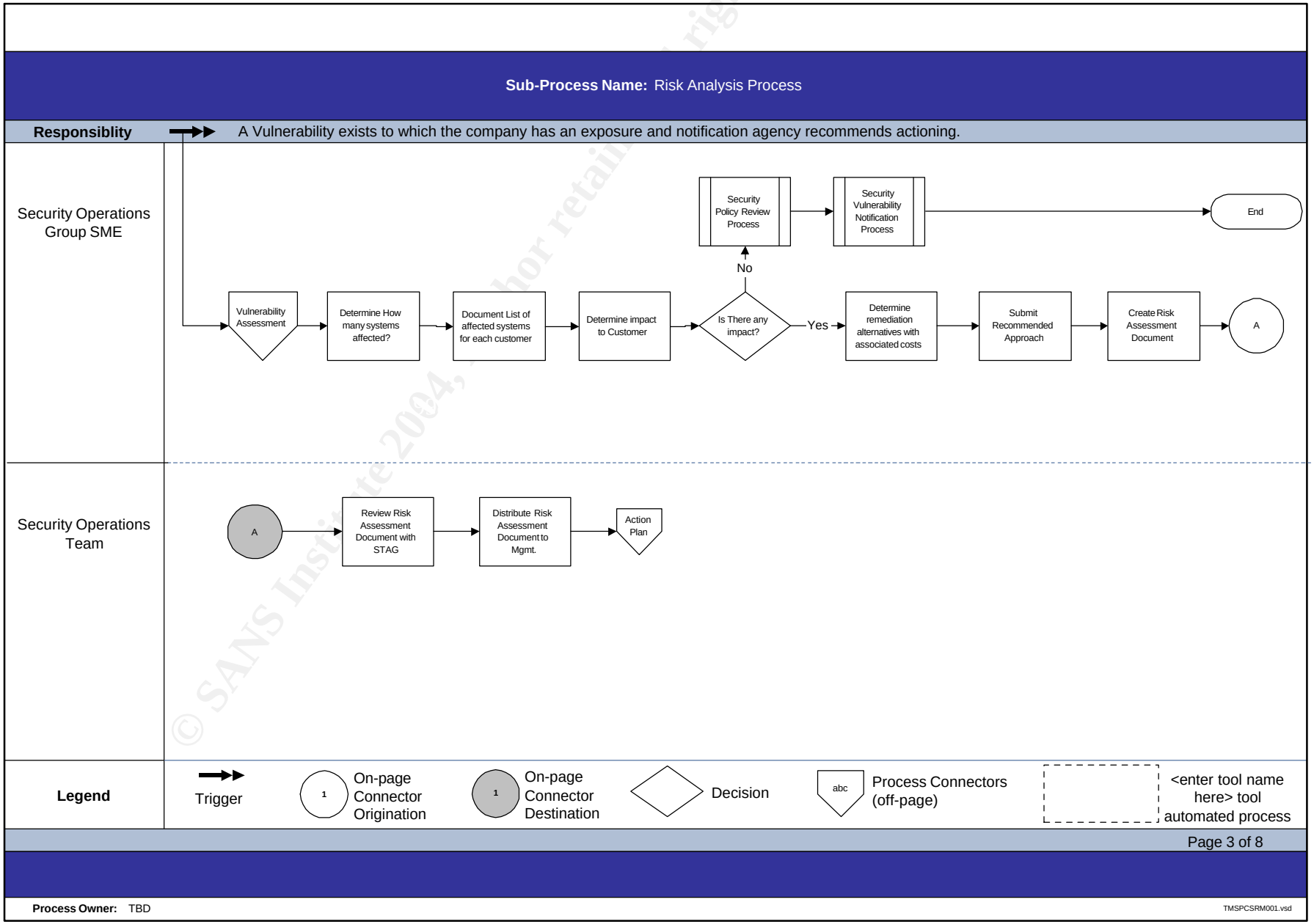
1 On-page Connector Origination

1 On-page Connector Destination

Decision

abc Process Connectors (off-page)

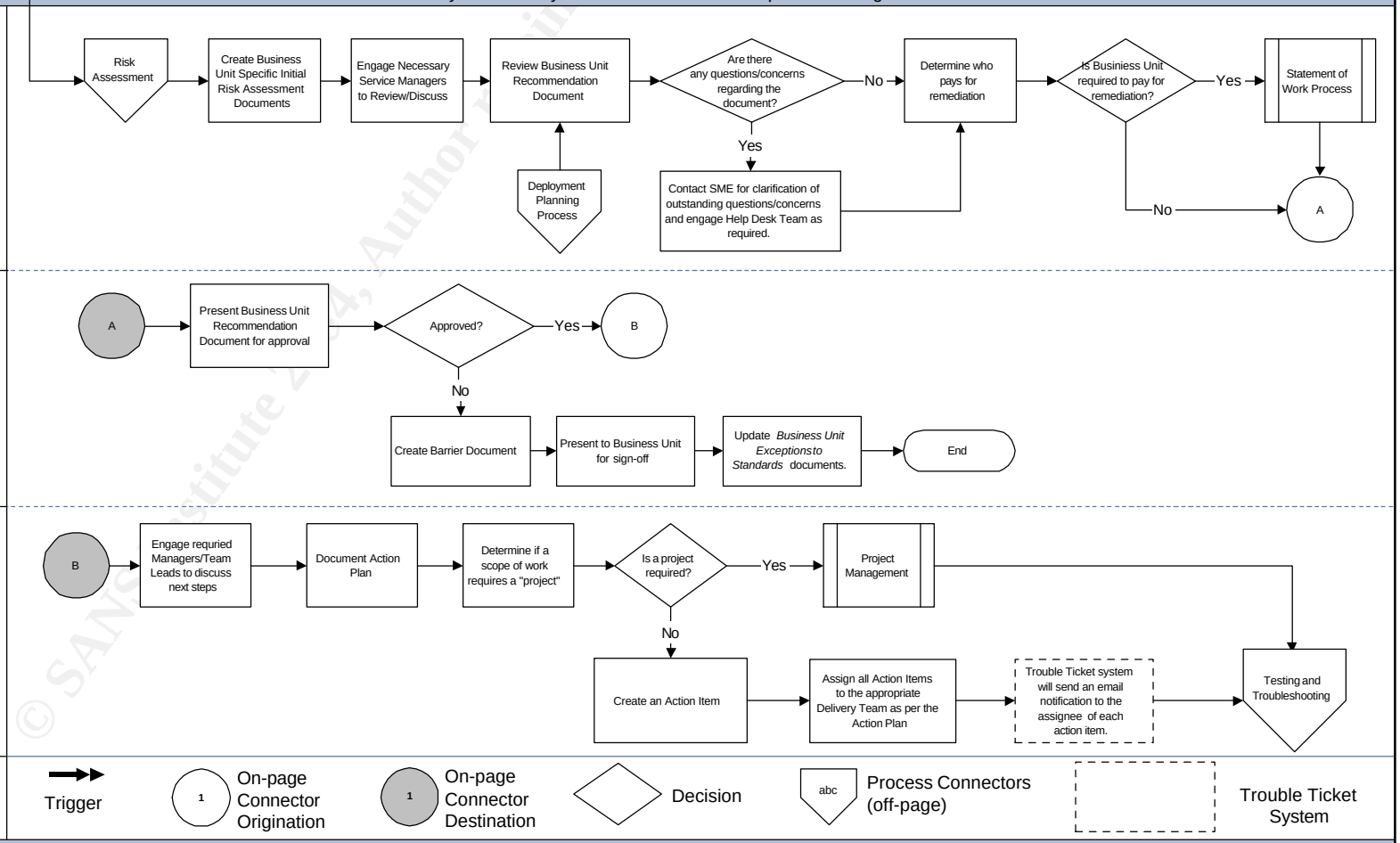
Process Owner: TBD



Sub-Process Name: Action Plan Process

TMSPCSRM001-003

Responsiblity Risk Assessment Document been issued by the Security Threat Assessment Group for actioning.



Revision: March 12, 2003

ITIL Service Management: Security Management

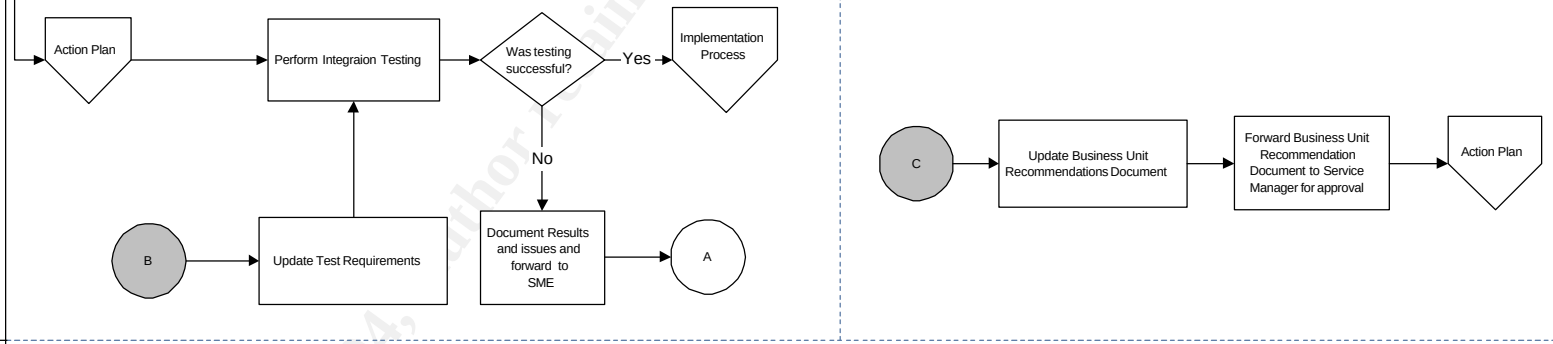
Process Owner: TBD

TMSPCSRM001.vsd

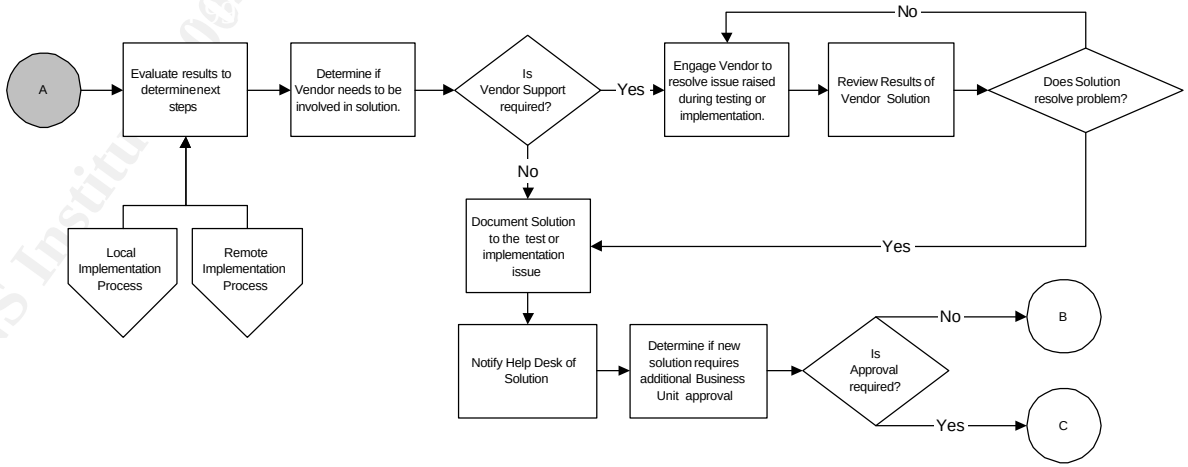
Sub-Process Name: Testing Process

Responsiblity Action Planning completed and Business Unit recommendation accepted.

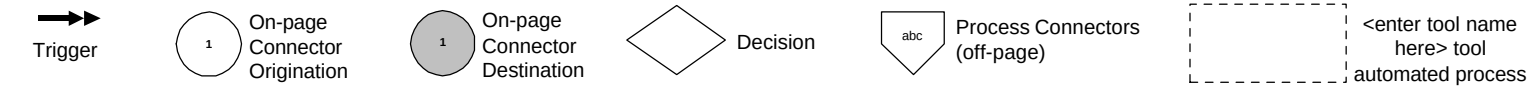
Business Unit Delivery Teams



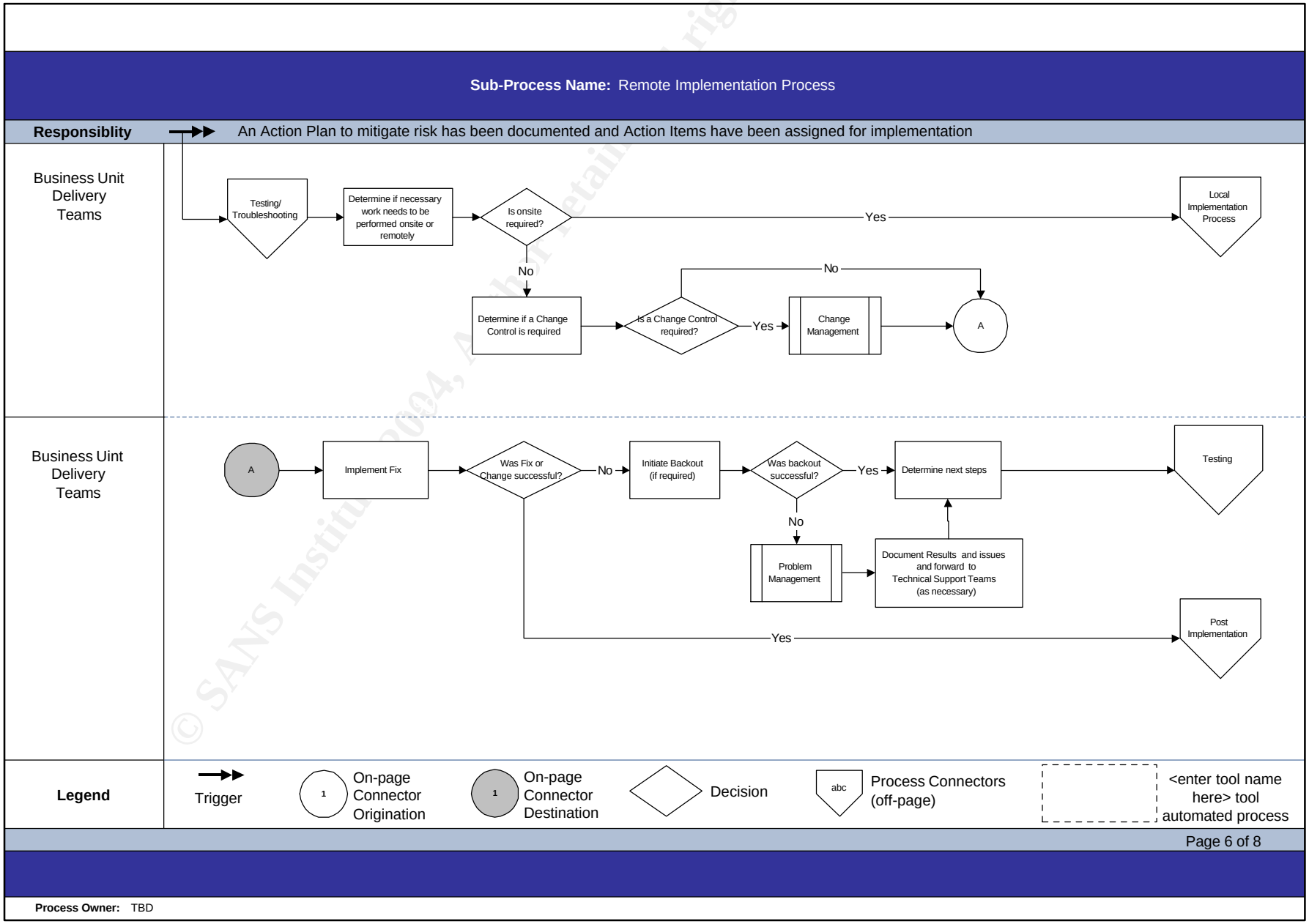
Security Operations Group SME



Legend



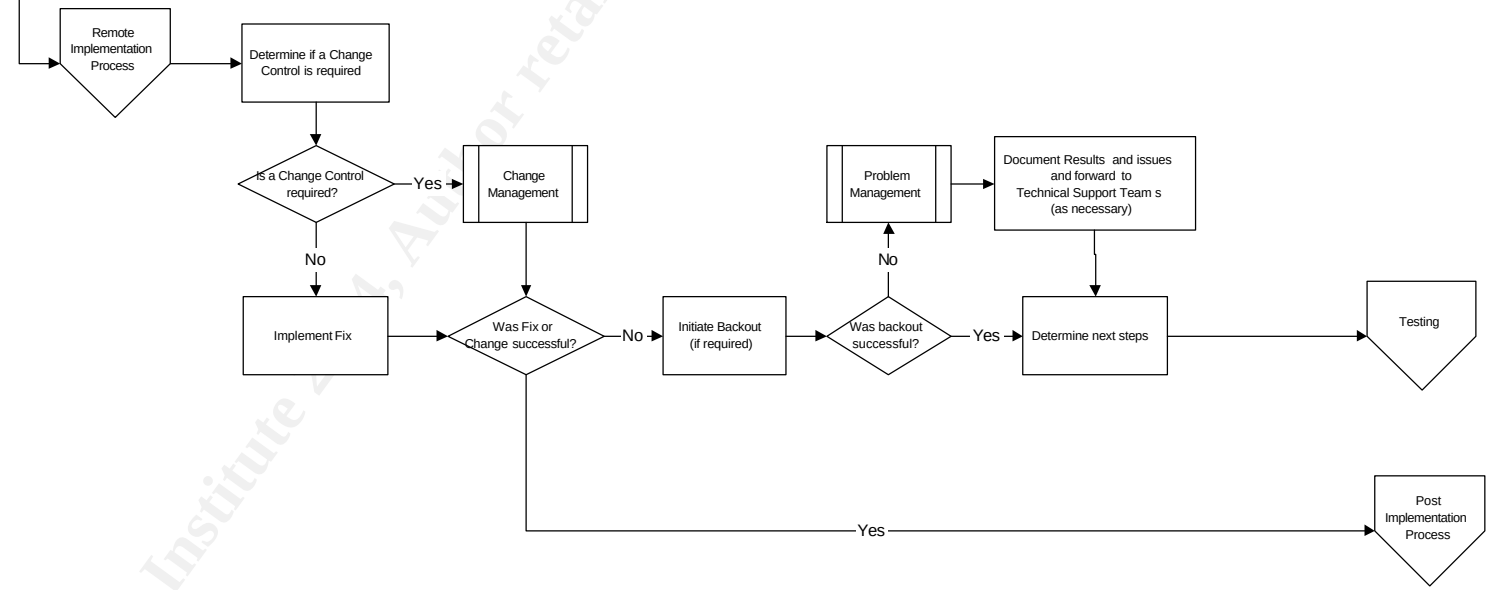
Process Owner: TBD



Sub-Process Name: Local Implementation Process

Responsiblity → Action Items assigned require on-site implementation

Business Unit Delivery Teams



Legend

Trigger

1 On-page Connector Origination

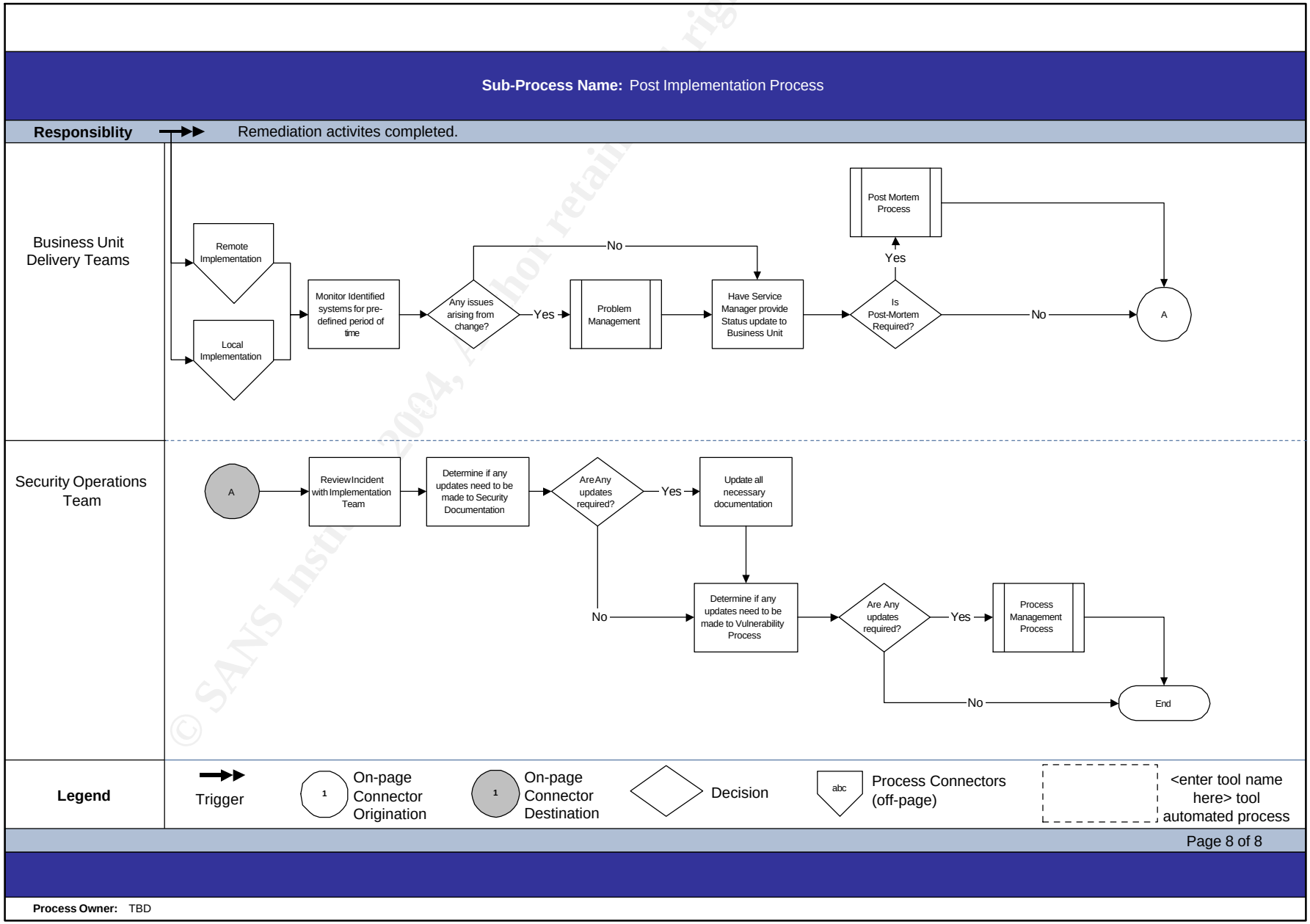
1 On-page Connector Destination

Decision

abc Process Connectors (off-page)

Process Owner: TBD

TMSPCSRM001.vsd



Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS New Orleans MGT512	New Orleans, LA	Aug 21, 2017 - Aug 25, 2017	Community SANS
Community SANS New York MGT512	New York, NY	Aug 28, 2017 - Sep 01, 2017	Community SANS
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Toronto MGT512	Toronto, ON	Sep 18, 2017 - Sep 22, 2017	Community SANS
Community SANS Columbus MGT512	Columbus, OH	Sep 25, 2017 - Sep 29, 2017	Community SANS
SANS Oslo Autumn 2017	Oslo, Norway	Oct 02, 2017 - Oct 07, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
Community SANS Banff MGT512	Banff, AB	Oct 23, 2017 - Oct 27, 2017	Community SANS
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
Community SANS Memphis MGT512	Memphis, TN	Nov 06, 2017 - Nov 10, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Northern Virginia Winter 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Miami 2018	Miami, FL	Jan 29, 2018 - Feb 03, 2018	Live Event
SANS Southern California- Anaheim 2018	Anaheim, CA	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced