Patch Management

Operating Procedure

Government of Ontario IT Standards (GO-ITS)

Document No. 42
Version 0.70a
Status: Approved

OCCIO/OCCTO
MANAGEMENT BOARD SECRETARIAT
CORPORATE ARCHITECTURE AND STANDARDS BRANCH
TECHNICAL STANDARDS SECTION

Last Review Date: December 14, 2004

Foreword

Government of Ontario Information & Technology Standards are the official publications on the standards, guidelines, technical reports and preferred practices adopted by the Information Technology Standards Council under delegated authority of the Management Board of Cabinet. These publications support the Management Board Secretariat's responsibilities for coordinating standardization of Information and Technology in the Government of Ontario. Publications that set new or revised standards provide policy guidance and administrative information for their implementation. In particular, they describe where the application of a standard is mandatory and specify any qualifications governing its implementation.

Table of Contents

INTRODUCTION **4**
1 INTRODUCTION TO THE PATCH MANAGEMENT OPERATING PROCEDURE **4**
1.1 Purpose of the Standard 4
1.1.1 Audience and Assumptions *4*
1.1.2 Applicability *4*
1.1.3 Goals and Strategies *4*
1.2 Scope 6
1.2.1 In Scope *6*
1.2.2 Out of Scope *7*
1.3 Recommended Versioning and/or Change Management 8
1.3.1 ITSM Process Governance and Ownership *8*
1.3.2 Version Control *8*
1.4 Contact Information 9
1.5 Type of Standard 9
1.6 Publication 9
1.7 Acknowledgements 10
1.7.1 Development Team *10*
1.7.2 Reviewers *10*
PATCH MANAGEMENT OPERATING PROCEDURE **12**
2 PRINCIPLES **12**
2.1 Alerts 12
2.2 Accountability 12
2.3 Patch Conflicts 12
2.4 Patch Testing 12
2.5 Patch Repository 13
2.6 Remote and Mobile Users 13
2.7 Threat/Risk Metrics for the OPS 13
2.8 Severity Levels 14
2.8.1 Definition of Severity *14*
2.8.2 OPS (Corporate) Severity *14*
2.8.3 Cluster Severity *15*
3 MANDATORY REQUIREMENTS **16**
3.1 Reporting Metrics 16
3.2 Tracking Metrics 16
3.3 Communication Strategy 16
3.4 Patch Lifecycle 18
3.4.1 Severity Zero *18*
3.4.2 Severity One *21*
3.4.3 Severity Two *24*
3.4.4 Severity Three *26*
3.4.5 Severity Four *28*
ROLES AND RESPONSIBILITIES **30**
4 DEFINITIONS **34**
5 ACRONYMS **36**
ERRATA **37**
DOCUMENT NUMBERING **38**
COPYRIGHT **38**
APPENDIX **39**
5.1 Appendix A: Severity Lifecycles 39
5.1.1 Summary Table *39*
5.1.2 Severity Lifecycles Detailed Diagrams *40*
5.2 Appendix B: Severity Case Examples 45
5.2.1 Alerts from 2003 ..... *45*
5.2.2 Alerts from 2004 ..... *46*

Introduction

1 Introduction to the Patch Management Operating Procedure

1.1 Purpose of the Standard

Patch Management is the process by which security fixes and application patches or updates are collected, analyzed, tested and implemented throughout the IT environment. In March 2004, ITELC approved an OPS "Patch Management Strategy" which included a standardization of OPS operating procedures. This document details the ITELC-approved systematic approach to Patch Management that is meant to establish consistency across the OPS enterprise and to reduce the level of risk. This Patch Management Operating Procedure represents a key aspect of a comprehensive Patch Management Strategy.

A synopsis of the key contents of the procedure may be found in the appendix under Appendix A: Severity Lifecycles: Section 5.1.1 Summary Table.

1.1.1 Audience and Assumptions

This document is written for system administrators, technical managers, functional managers, security specialists and other IT staff members who manage information systems. It provides a structured approach to identifying and implementing security patches or otherwise mitigating the risk of vulnerability.

This document assumes that readers will have some operating system and application expertise. Because of the volatile nature of vulnerabilities and patches, readers are expected to take advantage of other resources (including those listed in this document) for specific vulnerability and patch information.

1.1.2 Applicability

Government of Ontario IT Standards and Enterprise Product Standards apply (are mandatory) for use by all ministries/clusters and to all former Schedule I and IV provincial government agencies under their present classification (Advisory, Regulatory, Adjudicative, Operational Service, Operational Enterprise, Trust or Crown Foundation) according to the current agency classification system. Additionally, this applies to any other new or existing agencies designated by Management Board of Cabinet as being subject to such publications.

Kindly refer to http://intra.pmed.mbs.gov.on.ca/mbc/pdf/Agency_Establishment&Accountability-Dir.pdf for a list of provincial government agencies with their classification under the current classification system, as well as their previous Schedule under the former Schedule system.

1.1.3 Goals and Strategies

The goal of the patch management strategy is to enhance the reliability and availability of the OPS I&IT infrastructure. To this end, vendor security patches for vulnerabilities need to be

implemented on all (i.e. 100%) OPS computers in a robust and controlled manner as they are released. The following conditions and elements have been identified as requirements to achieve an efficient and effective patch management strategy:

Patching service levels based on the risk to the OPS environment;

Standard OPS operating procedures to include common definitions for patch Severity and common processes and lead times for deployment. ITSM and Change Management / OCCTO has ownership of the operating procedures;

Clusters/Infrastructure service providers (including business areas) to have developed processes to comply with the above;

A technology solution to automate the process (where feasible);

A communications and awareness strategy;

The method of patching to address LAN, WAN, and remote users of the OPS network.

Patch Management is just one element of an effective security policy (and an effective security policy is just one element of good infrastructure and asset management). Other activities related to the security of the infrastructure (such as Antivirus updates and scans) are also important elements of an effective security policy, but are not dealt with explicitly under Patch Management. It is expected that, although Patch Management will work to secure the infrastructure, these other elements or activities are in place to further support the security of the environment and its data.

This document has been designed mainly to address the first two items above and provide references to the remaining elements.

1.2 Scope

1.2.1 In Scope

1.2.1.1 All Patches to OPS infrastructure

The scope of the Patch Management process includes all Patches that address vendor product security vulnerabilities related to OPS desktops, laptops, servers and common infrastructure (including those managed by third-party service providers) regularly connected or connecting to the common infrastructure. This includes, but is not limited to, Microsoft and other third party software/application patches, hot fixes, updates, feature packs, and service packs, as well as equipment hardware or firmware updates, fixes, or adjustments (all of which hereafter referred to generically as Patches).

Service Packs that present no immediate security issues, nonetheless, also fall within the scope of proper security patch management. In order to pro-actively maintain a current level of patching, all Service Packs (unless they require more immediate application) fall within the target timelines of Severity Four.

1.2.1.2 Definition of Key Roles in Patch Management

The Roles (and their related responsibilities) as agreed upon and outlined in the ITELC approved OPS “Patch Management Strategy” are included in the scope of this operating procedure. Defining key roles in the Patch Management process is important to ensure clarity of responsibility and efficient communication when time plays a critical factor.

1.2.1.3 Definition of Severity, Timelines, Communication and Reporting Procedures

Common definitions for Severity levels, expected timelines, communication and reporting responsibilities are included in the scope of this operating procedure. This common understanding is important in realizing a well coordinated and concerted Patch Management effort.

1.2.1.4 Third-Party Service Providers/Partners/Contractors

Third-Party Service Providers/Partners/Contractors that have devices that regularly connect or are connected to the common infrastructure must be included within the scope of patching and this requirement must be written into their contracts.

1.2.2 Out of Scope

The following items are considered Out of Scope for this document, but not necessarily out of scope for a comprehensive Patch Management strategy.

1.2.2.1 Patch Management/Cluster Specific Tools

Operating procedures for an OPS tool (when determined) will form a separate document and are therefore out of scope for this document.

1.2.2.2 Performance Patches

Performance Patches that provide application enhancements, updates and bug fixes not related directly to security vulnerabilities do not necessarily fall within the Severity levels defined later in this document. Application owners are responsible for all patching efforts required for performance patches, including maintaining current versions, communicating to stakeholders, initiating the necessary Change and Configuration processes, testing and verifying implementations.

1.2.2.3 Local Implementation/Security Strategies, Common Infrastructure Best Practices

Local implementations and security strategies for patch management at the local cluster level have not been included in the scope of this document to allow clusters the freedom to implement the details of patch management in ways that best fit the needs of their environment.

Strategies such as maintaining Desktop Images or Automation of the patching process are therefore out of the scope of this document. Wake-On-LAN strategies at this time remain under investigation and expect to be available once a tool is also made available. For now, Wake-On-LAN remains out of scope. Details of cluster patching cycles, organizational information beyond a primary contact list, and specific cluster implementations of patch management are also considered out of scope.

Remote, Mobile and offsite users are out of scope of the target timelines and as long as they remain unconnected to the common infrastructure. This is addressed further in the Principles section.

1.3 Recommended Versioning and/or Change Management

1.3.1 ITSM Process Governance and Ownership

On-going ownership and responsibility for maintenance and evolution of the Operating Procedure for Patch Management resides with the Office of the Corporate Chief Technology Officer "OCCTO", ITSM Strategies and Change Management Branch.

The documents are available at:

http://www.gov.on.ca/MBS/techstan/

For further information, please contact:

Head of ITSM Strategies and Change Management Branch
Office of the Chief Technology Officer
77 Wellesley Street West, 8th floor
(416) 325-4240
Corporate.Cab@mbs.gov.on.ca

1.3.2 Version Control

Version	Date	Revised By	Description	Filename
0.01	June 28, 2004	B. Lu	Initial draft	Operating Procedure for Patch Management 2004-06-24.doc
0.02	Aug. 23, 2004	B. Lu	Second draft	Operating Procedure for Patch Management 2004-08-25.doc
0.03	Aug. 30, 2004	B. Lu	Modified Threat/Risk Matrix, Severity One and Zero procedure.	Operating Procedure for Patch Management 2004-08-30.doc
0.04	Sept. 29, 2004	B. Lu	Cluster feedback and flowchart diagrams added.	Operating Procedure for Patch Management 2004-09-21.doc
0.05	Oct. 4, 2004	B. Lu	Severity two to four flowchart diagrams	
0.06	Oct. 18, 2004	B. Lu	Simplified flowcharts, fixed punctuation in lists. Feedback from conference call.	Operating Procedure for Patch Management 2004-10-18.doc
0.70	Nov. 02, 2004	B. Lu	Final Draft for review. Used GO-ITS template. Updated diagrams and responsibilities around 3rd Party SP, business units, ABCs	Operating Procedure for Patch Management 2004-11-02.doc

1.4 Contact Information

	Contact 1	Contact 2
Name	Head	Manager, ITSM
Organization/ Ministry	MBS	MBS
Division	OCCTO	OCCTO
Branch	ITSM Strategies and Change Management	ITSM Strategies and Change Management
Section/ Unit		ITSM
Office Phone	(416) 325-4240	(416) 212-0856
E-mail	go-its@gov.on.ca	go-its@gov.on.ca

1.5 Type of Standard

Check One	Type of Standard
☑	Implementation or Process Standards – requirements or specifications, which may include best practices and guidance, for the implementation of a technology or the performance of an activity related to the use of technology, applicable throughout the provincial government. (e.g. mandatory O/S configuration requirements, security procedures, change management procedures, web page design requirements etc.).
☐	Information Standard – specifications for a data format (e.g. XML schema, metadata, and/or related data models)
☐	Technical Standard - networking and communications specifications, protocols, interfaces (API's) (e.g. standards adopted from recognized standards development organizations such as W3C, OASIS or IETF such as TCP/IP, XML, SOAP, etc.)
☐	Architecture Standard – application patterns, architecture and standards principles governing the design and technology decisions for the development of major enterprise applications
☐	Product Standard – an enterprise-wide product which is mandatory for use such as a single corporate-wide application, which all ministries and agencies use to record and access their HR information.

1.6 Publication

Please indicate if this standard should be restricted to publishing on the Internal (Intranet) IT Standards web site or whether it is intended for publishing on the public (Internet) Government of Ontario IT Standards web site.

Check One	Publish as Internal or External
☐	Internal Standard
☑	External Standard

1.7 Acknowledgements

1.7.1 Development Team

Name	Cluster/Ministry	Branch
Lorrie MacKinnon	MBS	ITSM Strategies & Change Management Branch
Binh Lu	MBS	ITSM Strategies & Change Management Branch
Dale Tasker	MBS	Corporate Security Branch
David Chan	MBS	Corporate Security Branch
Latifa Ho	LRC	LRC Security Services (LSS)
John Lorenc	EBC	EBC I&IT Services Management
Ken Proch	JUS	Technology Management Branch
Sheri Burgos	iSERV	iSERV
Ciaran Hickson	CAC	Enterprise Technology Solutions Branch
Monique Sabourin	CAC	Enterprise Technology Solutions Branch

1.7.2 Reviewers

Check	Area	Date: (month/year)
☐	Technical Standards Unit, Corporate Architecture Branch, OCCTO	
☐	Corporate Architecture and Standards Branch (CASB Architects), OCCTO	
☐	Infrastructure Development Branch & iSERV, OCCSD	
☑	Corporate Security, OCCIO	11/2004
☐	Strategy, Policy, Planning and Management Branch (SPPM, OCCS)	
☐	Corporate ACT and Domain Working Groups	
☐	– Information Architecture Domain (IADWG)	
☐	– Technology Architecture Domain (TADWG)	
☐	– Application Architecture Domain (AADWG)	
☐	– Security Architecture Working Group (SAWG)	
☐	Cluster ACT/ARB (for cluster standards promoted to corporate standards)	
☐	ITSC members (*provide name*)	
☑	Others (*named below*)	

Name	Cluster/Ministry	Branch
Roy Finlayson	CSC	Technology and Services Management
Anthony Khoo	iSERV	iSERV
Margaret Lapierre	HSC	Technology Management
John Violette	MTO	ITSM Branch

Patch Management Operating Procedure

2 Principles

2.1 Alerts

The Corporate Security Branch (CSB) issues alerts in response to vulnerabilities in the security of the IT environment or infrastructure. Every alert will include the following information on each vulnerability listed in the alert:

Identification/description of the vulnerability (publisher or CSB assigned identification);

CSB assigned Severity level;

Risk Assessment;

Affected software or hardware;

Link to related patch, recommended mitigation procedure and/or further information.

Every vulnerability has a required timeline for patching of the environment or mitigation of the Threat/Risk as determined by its Severity level. This timeline begins once the alert for the vulnerability is issued. It is the responsibility of the Cluster Security Officer or Cluster Approver to inform their Cluster of Patch Alerts.

2.2 Accountability

Once an alert is issued by CSB, all ministries and agencies are accountable for carrying out the required patching in a timely manner, as well as ensuring that any appropriate patch testing and necessary reporting is completed.

CIOs are accountable for ensuring that the IT environments within their ministries are patched according to identified timelines. A Cluster CIO holds responsibility and decision-making authority for any escalation of patching required and is ultimately accountable if their cluster chooses not to apply a patch.

2.3 Patch Conflicts

Lower Severity patches should never undo higher Severity patches. If a known conflict exists, lower Severity patching is to be delayed until the patch vendor can determine an appropriate resolution. As lower Severity patches can often predate higher Severity patches, patch implementers and release management should be aware that patch conflicts can occur and should not assume that the vendor has accounted for all possible patching combinations.

2.4 Patch Testing

Basic patch testing is meant to verify that the patch has not broken the existing system or anything running on or related to the system. Testing to verify that the patch has fixed what it was intended to fix is a responsibility left to the patch vendor.

All patches should be tested whenever possible. It is important that patches are tested on a system configured almost exactly like the target system because system configuration issues often cause patches to fail. Under circumstances where patch testing cannot be thoroughly conducted in time to meet the timelines for the Severity level of the alert, then patch testing should be risk managed, either by isolating or removing the untested system from the network or applying the patch and testing after the fact.

2.5 Patch Repository

A recommended best practice for Clusters to adopt is to manage their own Patch Repository so as to familiarize themselves with the features of each patch and for easier distribution of patches and patch deployment packages across their own LAN and to their remote users.

2.6 Remote and Mobile Users

Although Remote and Mobile Users are not within the scope of the defined Severity timelines, they should still be included in all patching efforts where possible and in any reporting metrics as an information item. In terms of patching, Remote and Mobile Users should be treated as new equipment when connecting to the network. They do not have to be counted in the full patching of infrastructure when unconnected, but must be patched before or as they connect to the network or common infrastructure. There is no implied target timeline commitment for Remote and Mobile Users in this operating procedure, but a "best effort" approach applies, especially to Users who regularly connect to the infrastructure.

2.7 Threat/Risk Metrics for the OPS

A Threat/Risk matrix is used to classify Severity levels of vulnerabilities based on a High/Medium/Low evaluation of:

Exposure Level: Number and Type of Systems potentially affected by a malicious program with consideration for factors such as:

- Number of sites impacted;
- Number of mission critical systems potentially impacted;
- Number of systems impacted;
- Geographic distribution of systems.

Impact Level: Impact and Damage to Systems that a malicious program could have if encountered. Included in this metric are factors such as:

- Ability of existing installed technology to mitigate the Threat/Risk;
- Risk of high server and/or network traffic performance degradation;
- Potential for data destruction/modification or release of confidential information;
- Loss of productivity;

- Compromise of security settings;
- High cost or effort to recover or repair damage.

The Rate of Distribution at which a malicious program spreads may be used by CSB/Clusters to elevate Severity levels.

The following table summaries the classification of Severity levels:

Table 1 - Severity Threat/Risk Matrix

Number and Type of Systems	High	2	2	2	1	0
	Medium	3	3	2	2	
	Low	4	3	2	2	
		Low	Medium	High	High w/Exploit	Environment Under Attack
		Impact and Damage to Systems				

Please refer to appendix for case studies as examples of how Severity Levels have been assigned to past alerts.

2.8 Severity Levels

2.8.1 Definition of Severity

Severity Zero:	Defined as the environment under attack;
Severity One:	Both Threat/Risk metrics are high and an exploit has been published;
Severity Two:	One metric is high with or without a published exploit OR both metrics are high and no published exploit;
Severity Three:	Both Threat/Risk metrics are medium or a mix of medium and low;
Severity Four:	Both Threat/Risk metrics are low.

2.8.2 OPS (Corporate) Severity

OPS Severity level is initially assigned to a vulnerability by CSB based on the Threat/Risk metrics noted above. For vulnerabilities that are suspected to be Severity One, a conference call of the Incident Response Team (which includes all Cluster Security Officers and CSB) is held so that the Severity level can be agreed upon. For any other Severity level, including Zero, Two, Three or Four, no agreement through conference call is required (though one may still be held at the discretion of CSB).

It is assumed that the conditions for Severity Zero are clear enough if the environment is under attack, and the threat/risk is urgent enough not to require a conference call consensus on the Severity. For Severity Two, Three, or Four, it is expected that there would be sufficient time for clusters to evaluate and reassign Severity as required.

2.8.3 Cluster Severity

Cluster Severity is the Severity that can be (re)-assigned to a patch by the cluster CSO or informed ITX2 based on the Threat/Risk metrics noted above. Cluster Severity can originate from a threat or vulnerability discovered within the cluster or after a cluster receives an OPS alert and evaluates the potential impact of the vulnerability in the context of the cluster environment. If the vulnerability is assigned a Cluster Severity that differs from the original OPS Severity, this change must be communicated to CSB as soon as possible along with the rationale for the change.

Every Cluster and iSERV may perform an additional Threat/Risk analysis of the vulnerability on their particular environment. If a Threat/Risk analysis shows justification for a Cluster to change its Cluster Severity, then that Cluster is not required to institute a Change Freeze but should still participate in all Corporate Severity activities. In other words, Clusters that already have their environment completely patched, or that otherwise do not have any vulnerable exposures should nonetheless follow identified communication protocols, take part in CSB initiated conference calls and submit Threat/Risk analysis reports to CSB for tracking purposes.

3 Mandatory Requirements

3.1 Reporting Metrics

Once CSB issues an alert, immediate acknowledgement of the alert from CSO/iSERV should be sent to CSB. CSOs (who are responsible for IT security in the cluster) will collect the information described below from their clusters and provide this to CSB. Collected information, status updates and reports should be sent via email at intervals required by the OPS Severity level. Reports should include:

Date and Time of report;

Cluster (re)assigned Severity (if appropriate);

Percentage of Desktops Patched (at time of reporting) not including mobile/remote users;

Percentage of Desktops Patched in complete environment (if different from above);

Percentage of Servers Patched (at time of reporting);

Percentage of Other Devices Patched (at time of reporting);

Also should be included are times related to percentage complete, and what processes are in place to patch mobile units.

This information is used to track progress, identify potential issues, and to close the Corporate Request for Change (CRFC) once patching is completed.

3.2 Tracking Metrics

Corporate Security Branch (CSB) will be responsible for tracking of the reporting metrics and communicating to the Corporate Change Management Advisory Board (CCAB) in order to open or close a CRFC.

3.3 Communication Strategy

Standard templates have been developed for use by CSB to communicate defined Severity levels. Standard communication protocols have also been developed. The following are basic principles of the patch management communication strategy (details to follow in the Patch Lifecycle section):

For all Severity levels, cluster security officers (CSOs) are informed and keep their respective change managers and service desks informed;

For Severity Zero, CCIO, CIOs and the Corporate Chief are notified by the Head of CSB;

For Severity One, CSB will hold a conference call of the incident response team to confirm the Severity level. CSB then notifies identified ITX2s in each cluster and iSERV;

The Cluster is responsible for all communication required to its ministries/business areas/business units that have a connection to OPS infrastructure. The Cluster (and ultimately the Cluster CIO) is responsible for informing any ABCs (Agencies, Boards or Commissions) that operate on OPS provisioned infrastructure during all Severity situations.

Third-party/Vendor Alerts sent directly to Clusters/iSERV that have not come from CSB should be forwarded to Corporate Security for their assessment.

3.3.1.1 Communication Protocols

Severity	ZERO	One	Two	Three	Four
Communication Method	Multiple electronic channels†	Multiple electronic channels†	Multiple electronic channels†	E-mail	E-mail
Frequency of Status Reporting to CCAB	As possible and upon completion	Daily	Weekly	Bi-Weekly	Monthly
Timeline for Completion of Patching	Immediate	2 days	7 days	30 days	90 days

†Including Phone, BlackBerry, Web postings and E-mail.

3.3.1.2 Table of Contacts

A Table of Contacts identifying who are the primary and secondary contacts for alerts and notifications is maintained by CSB. This table should be periodically verified and updated as required. Although clusters should make an effort to keep CSB informed of all contact changes, it is the responsibility of CSB to keep this table current and ensure that all critical communication points are managed.

Clusters/iSERV must also maintain their own table of contacts for putting into action any alerts that are issued by CSB. For the clusters/iSERV, CSB represents the single point of contact for communications, alerts and reports outside of their cluster.

3.4 Patch Lifecycle

3.4.1 Severity Zero

Definition[°]: Environment Under Attack
Target Timeline: Immediate
Deployment Approval: CSB in immediate consultation with clusters, iSERV and CCAB
Decision-making Authority: CCIO (with Head of CSB as backup)
Procedures:

Cluster/iSERV Initiated Severity Zero:

Cluster/iSERV confirms environment under attack and increasing numbers of exploits/compromises are being experienced/reported;

ITX2 ensures appropriate action is taken to safeguard the integrity of the environment;

Cluster CAB/iSERV implements Change Freeze;

CSO/iSERV notifies CSB of cluster Severity Zero by phone (416-327-2100) and followed-up by email;

CSB evaluates the potential risk of an OPS wide attack and initiates the Patch Management process as appropriate (as follows for a corporate Severity Zero):

Corporate Initiated Severity Zero:

1 – Communication

I&IT Corporate Security Branch (CSB) is informed or determines that environment is under attack as demonstrated by exploits/compromises being experienced/reported;

Head of CSB notifies CCIO, CIOs, and Corporate Chiefs;

CSB notifies CSOs/iSERV and CCAB (by BlackBerry);

CSB notifies the Network Integrator (EDS via TAC by Phone);

CSO/iSERV is responsible for informing their Cluster of Patch Alerts;

- CSO informs the local Service Desk, Change Managers;
- CSO/iSERV reports to CSB regularly or as time permits until situation has normalized;

Clusters are responsible for communicating to their Third-party Service Providers (with the exception of the Network Integrator), Business units within the cluster ministries, and ABCs;

CSB updates CCIO, CIOs, and Corporate Chiefs as appropriate.

[°] NOTE: The Rate of Distribution at which a malicious program spreads may still be used by CSB/Clusters to elevate severity levels.

2 – Change Freeze

CCAB notifies cluster CABs and all institute Change Freeze.

- Applying a Change Freeze to changes in progress is left to the discretion of the cluster/iSERV to be decided on a case-by-case basis;
- Pre-approved/Standard[**] changes are allowed to proceed through a Change Freeze unless CCAB/Cluster CABs deem them inappropriate.

3 – Mitigation

CSO/iSERV ensures identified ITX2s (or designated cluster patch security authorities) are informed and action is taken; actions may include:

- Isolation of network devices or segments;
- Blocking of ports or changes to firewall rules;
- Deployment of required patches or anti-virus measures;
- Any means necessary to safeguard the integrity of the environment, including emergency shutdown of servers or services.

CCAB is notified of any emergency blocking and emergency firewall rule changes;

ABCs and Ministry Business units with IT Centres take appropriate mitigation action;

Third-party service providers take action as appropriate and applicable to contractual agreements, including reporting progress back to clusters;

Clusters take action as appropriate for iSERV Facility Managed or Co-located Servers for which they have administrative responsibility.

4 – Lifting Severity Zero and Change Freeze

CSB in consultation with CSOs/iSERV and CCAB lifts Severity Zero;

CCAB approves the removal of emergency blocks and removal of Change Freeze at the corporate level once the situation has normalized;

CCAB informs Cluster CABs of the ending of the Corporate Change Freeze;

- Local Change Freeze is generally lifted when Corporate Change Freeze is lifted or earlier in consultation with CSB and CCAB.

For iSERV: Customer Approval is required for all Patches for Managed Dedicated Server Hosting Services. Customer is informed after the environment is protected for non-patch mitigation (such as Network blocks, Emergency Server/System shutdown or changes not required on Customer Servers);

For iSERV Shared Web Hosting and Infrastructure Servers: Customers are only informed of all changes through the CCAB process. Customer approval is not required.

[**] Definition of Pre-approved/Standard changes will differ from organization to organization.

The following diagram illustrates the lifecycle of a Corporate Initiated Severity Zero:

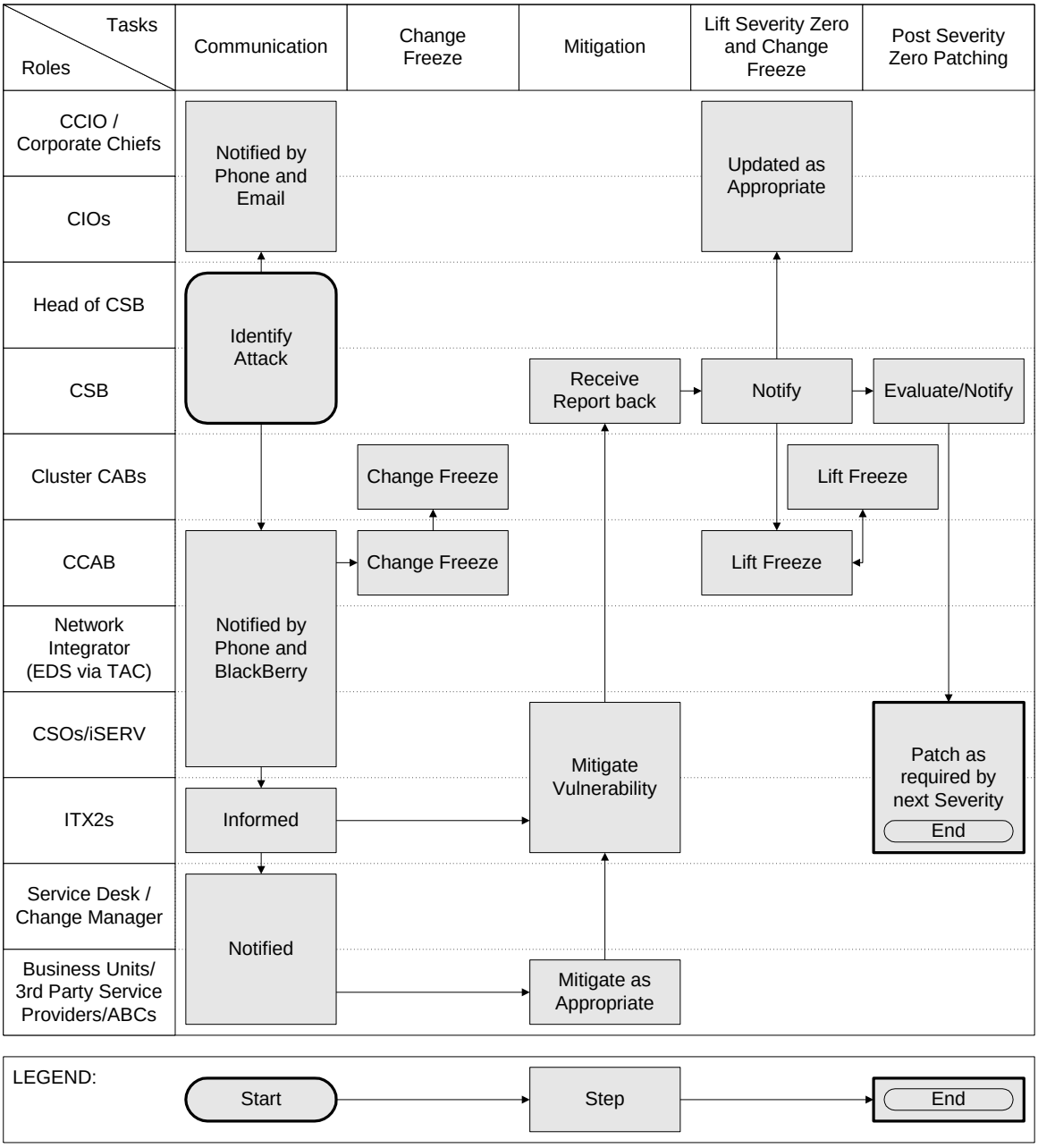

Figure 1 - Severity Zero lifecycle

3.4.2 Severity One

Definition°: Both Threat/Risk metrics are high and exploit published
Target Timeline: 100% within 2 Calendar Days of Notification
Deployment Approval: Infrastructure Heads (ITX2s)
Decision-making Authority: Cluster CIOs
Procedures:

1 – Communication

I&IT Corporate Security Branch (CSB) identifies or is informed of vulnerability;

CSB initiates conference call of Incident Response Team to confirm the Severity level.

2 – Issuing Alert

CSB issues a Severity One Alert to all clusters, iSERV and the Network Integrator and notifies identified ITX2s;

CSB posts alert on the OPS I&IT Security Intranet site (http://intra.security.gov.on.ca);

CSO/iSERV is responsible for informing their Cluster of Patch Alerts;

Clusters are responsible for communicating to their third party Service Providers (with the exception of the Network Integrator), Business units within the cluster ministries, and ABCs;

Every Cluster and iSERV may perform an additional Threat/Risk analysis of the vulnerability on their particular environment. ITX2, with advice of cluster CSO, may adjust the Severity level if appropriate.

- If any Cluster or iSERV determines that vulnerability is not a Severity One, the cluster CIO is notified and the CSO must report back to CSB on adjustment of Severity, risk analysis findings, and any issues with timelines (e.g. extension due to need for additional testing);
- For iSERV: if clients are affected by change of Severity, then they must be informed at the same time as CSB on findings, noting which servers/applications are affected.

3 – Submitting CRFC

CSB submits a “Request for Change” (informational CRFC) with CCAB.

4 – Mitigation

CSOs/iSERV and identified ITX2s ensure the deployment of the necessary resources to complete patching in a timely manner, and that action is initiated to:

- Acquire and test patches (or work-around) or make decision to risk manage;
- Develop deployment strategy;
- Deploy patches or measures for remediation;

° NOTE: The Rate of Distribution at which a malicious program spreads may still be used by CSB/Clusters to elevate severity levels.

- Inform Service Desk and Change Managers.

ABCs and Ministry Business units with IT Centres take appropriate mitigation action;

Third party service providers take action as appropriate and applicable to contractual agreements, including reporting progress back to clusters;

Clusters take action as appropriate for iSERV Facility Managed or Co-located Servers for which they have administrative responsibility;

CSO/iSERV reports to CSB regularly (daily until patching is complete) on:

- Severity level assigned by cluster;
- Progress in patching (percent complete) of all infrastructure in cluster ministries;
- Any issues in meeting patching timelines (e.g. need for additional testing).

CSB takes action as necessary on reports;

For iSERV: Customer Approval is required for all Patches for Managed Dedicated Server Hosting Services. Customers are consulted and provided with a short window of opportunity (24 hours) for review and approval prior to patch deployment. Customers must within this time provide approval; otherwise iSERV may take alternative actions until such approval is received. Such actions may include:

- Network blocks or other such changes not performed on Customer Servers;
- Isolating sections of the network that are unpatched until resources are available to patch them or their threat/risk level can be fully evaluated;
- Prioritizing patching efforts according to systems that can afford the least amount of downtime.

- For iSERV Shared Web Hosting and Infrastructure Servers: Customers are only informed of all changes through the CCAB process. Customer approval is not required.

5 – Closing CRFC

CSB notifies CCAB to close CRFC once patching is complete.

6 – Monthly Reporting

CSB will roll up information OPS-wide and present it as a standing information item in monthly security reports to CCIO, CIOs, and Corporate Chiefs.

The following diagram illustrates the lifecycle of a Corporate Initiated Severity One:

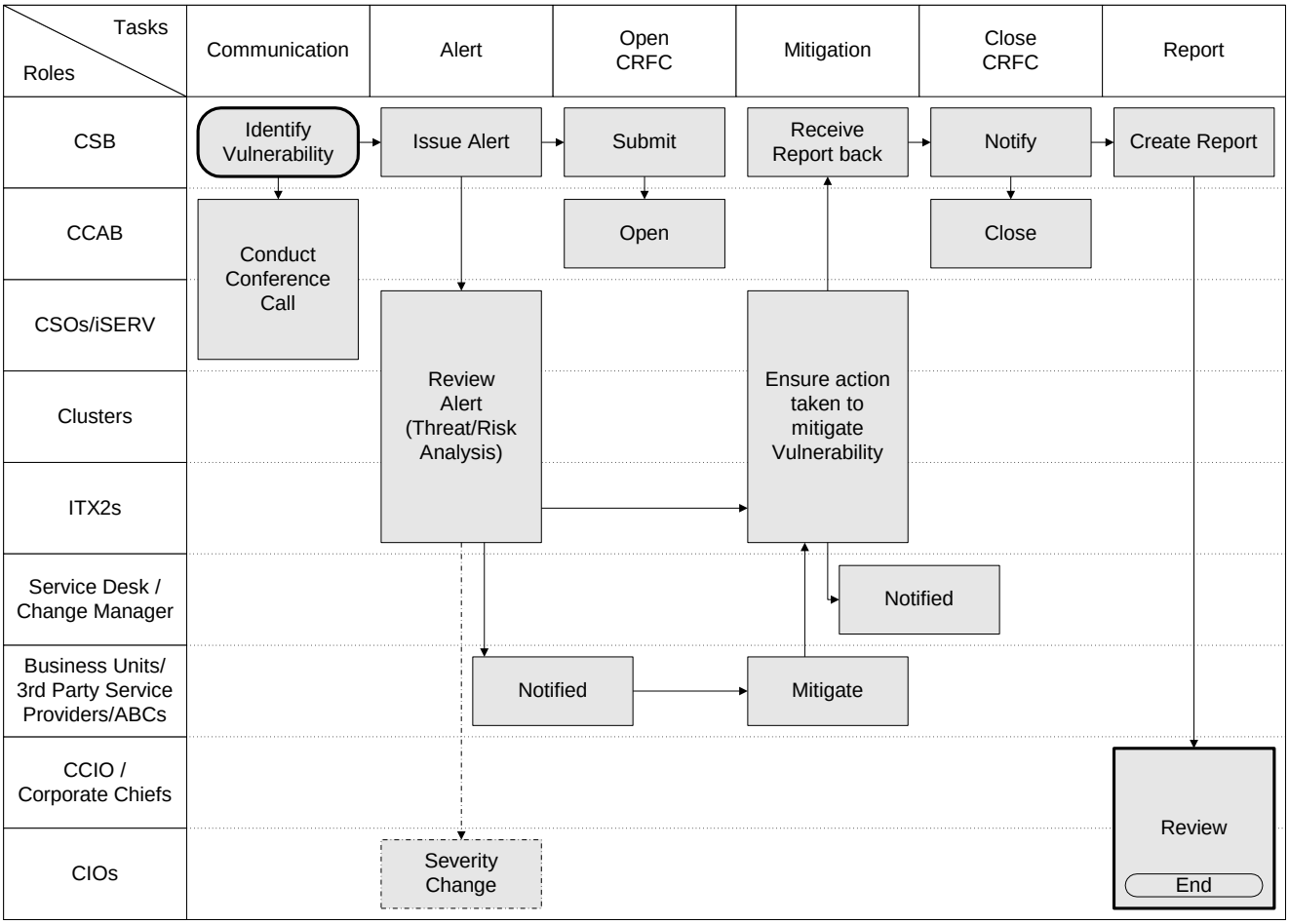

Figure 2 - Severity One lifecycle

3.4.3 Severity Two

Definition°: One metric is high with or without a published exploit OR both metrics are high and no published exploit
Target Timeline: 100% within 7 Calendar Days (1 Week) of Notification
Deployment Approval: Infrastructure Managers
Decision-making Authority: Cluster CIOs
Procedures:

1 – Communication

I&IT Corporate Security Branch (CSB) identifies or is informed of vulnerability;

If CSB suspects that the vulnerability may be Severity One or higher, then CSB may initiate conference call of the incident response team to confirm Severity level.

2 – Issuing Alert

CSB issues a Severity Two Alert to all clusters, iSERV and the Network Integrator;

CSB posts alert on the OPS I&IT Security Intranet site (http://intra.security.gov.on.ca);

CSO/iSERV is responsible for informing their Cluster of Patch Alerts;

Clusters are responsible for communicating to their third party Service Providers (with the exception of the Network Integrator), Business units within the cluster ministries, and ABCs;

Cluster may adjust Severity level with cause.

3 – Submitting CRFC

CSB submits “Request for Change” (informational CRFC) with CCAB.

4 – Mitigation

Upon receiving alert, CSOs/iSERV ensure appropriate infrastructure managers are informed and that action is initiated to:

- Assess alert to determine if patches are applicable;
- Acquire and test patches (or work-around) or decision made to risk manage;
- Develop deployment strategy;
- Deploy patches or measures for remediation;
- Inform Service Desk and Change Managers.

ABCs and Ministry Business units with IT Centres take appropriate mitigation action;

Third party service providers take action as appropriate and applicable to contractual agreements, including reporting progress back to clusters;

Clusters take action as appropriate for iSERV Facility Managed or Co-located Servers for which they have administrative responsibility;

° NOTE: The Rate of Distribution at which a malicious program spreads may still be used by CSB/Clusters to elevate severity levels.

CSO/iSERV reports to CSB regularly (at least weekly until patching complete) on:

- Severity level assigned by cluster;
- Progress in patching (percent complete) of all infrastructure in cluster ministries;
- Any issues in meeting patching timelines (e.g. need for additional testing).

CSB will take action as necessary on reports;

For iSERV patching: Customer Approval is required for all Patches for Managed Dedicated Server Hosting Services. Customer is consulted and provided with a short window of opportunity (minimum of 72 hours) for review and approval prior to patch deployment;

For iSERV Shared Web Hosting and Infrastructure Servers: Customers are only informed of all changes through the CCAB process. Customer approval is not required.

5 – Closing CRFC

CSB notifies CCAB to close CRFC once patching is complete.

6 – Monthly Reporting

CSB will roll up information OPS-wide and present it as a standing information item in monthly security reports to CCIO, CIOs, and Corporate Chiefs.

The following diagram illustrates the lifecycle of a Corporate Initiated Severity Two:

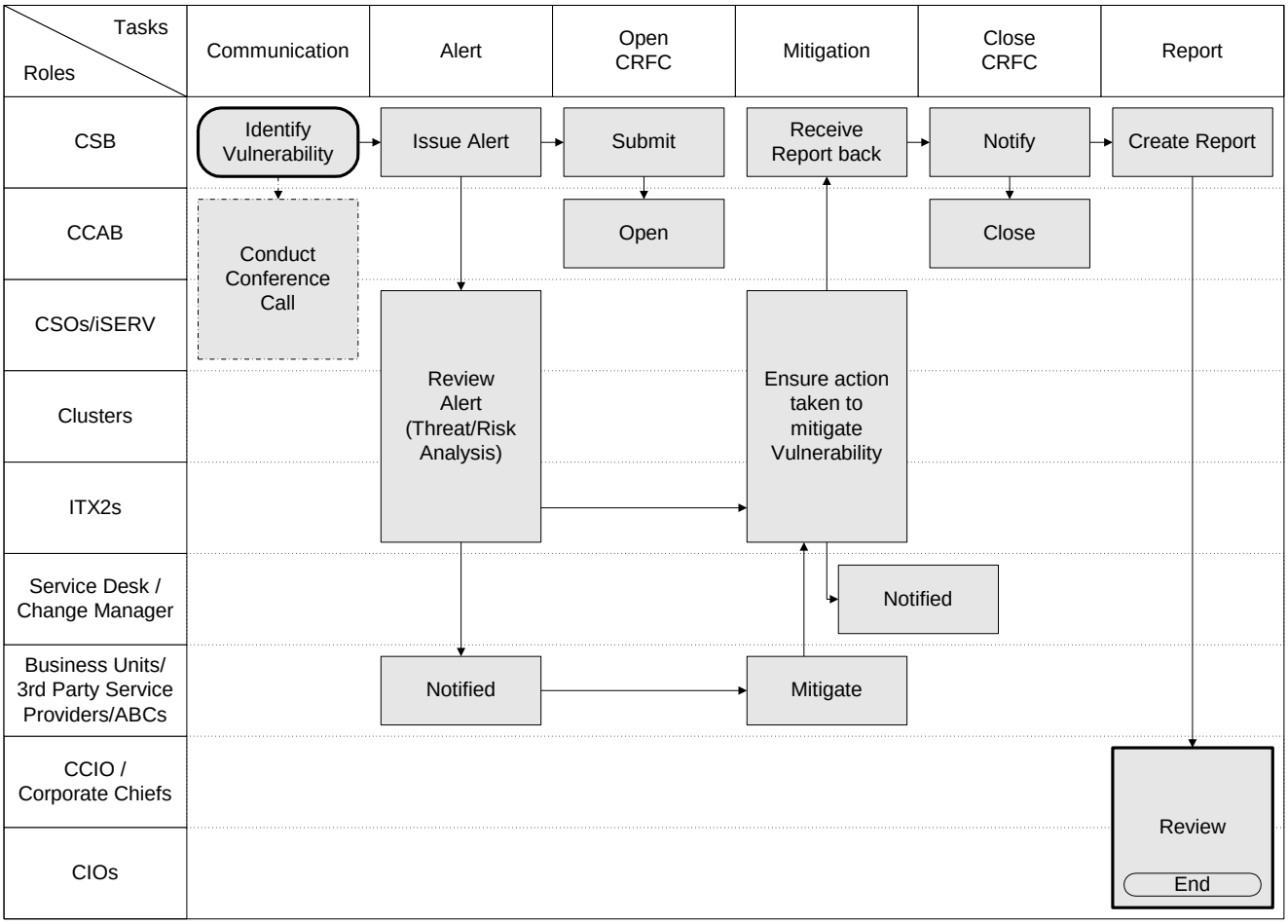

Figure 3 - Severity Two lifecycle

3.4.4 Severity Three

Definition°: Two Threat/Risk metrics are medium or a mix of medium/low
Target Timeline: 100% within 30 Calendar Days (1 Month) of Notification
Deployment Approval: Infrastructure Managers
Decision-making Authority: Cluster CIOs
Procedures:

1 – Communication

I&IT Corporate Security Branch (CSB) identifies or is informed of vulnerability.

2 – Issuing Alert

CSB issues Severity Three Alert to clusters, iSERV and the Network Integrator;

CSB posts alert on the OPS I&IT Security Intranet site (http://intra.security.gov.on.ca);

CSO/iSERV is responsible for informing their Cluster of Patch Alerts;

Clusters are responsible for communicating to their third party Service Providers (with the exception of the Network Integrator), Business units within the cluster ministries, and ABCs;

Cluster may adjust Severity level with cause.

3 – Submitting CRFC

CSB submits a "Request for Change" (information CRFC) with CCAB.

4 – Mitigation

Upon receiving alert, CSOs/iSERV ensure appropriate infrastructure managers are informed and that action is initiated to:

- Assess alert to determine if patches are applicable;
- Acquire and test patches (or work-around) or decision made to risk manage;
- Develop deployment strategy;
- Deploy patches or measures for remediation;
- Inform Service Desk and Change Managers.

ABCs and Ministry Business units with IT Centres take appropriate mitigation action;

Third party service providers take action as appropriate and applicable to contractual agreements, including reporting progress back to clusters;

Clusters take action as appropriate for iSERV Facility Managed or Co-located Servers for which they have administrative responsibility;

CSOs/iSERV reports to CSB regularly (at least bi-weekly until patching complete) on:

- Severity level assigned by cluster;
- Progress in patching (percent complete) of all infrastructure in cluster ministries;

° NOTE: The Rate of Distribution at which a malicious program spreads may still be used by CSB/Clusters to elevate severity levels.

- Any issues in meeting patching timelines (e.g. need for additional testing).

CSB will take action as necessary on reports;

For iSERV patching: Customer Approval is required for all Patches for Managed Dedicated Server Hosting Services. Customer is consulted and provided with a reasonable window of opportunity (minimum 2 weeks) for review and approval prior to patch deployment;

For iSERV Shared Web Hosting and Infrastructure Servers: Customers are only informed of all changes through the CCAB process. Customer approval is not required.

5 – Closing CRFC

CSB notifies CCAB to close CRFC once patching is complete.

6 – Monthly Reporting

CSB will roll up information OPS-wide and present it as a standing information item in monthly security reports to CCIO, CIOs, and Corporate Chiefs.

The following diagram illustrates the lifecycle of a Corporate Initiated Severity Three:

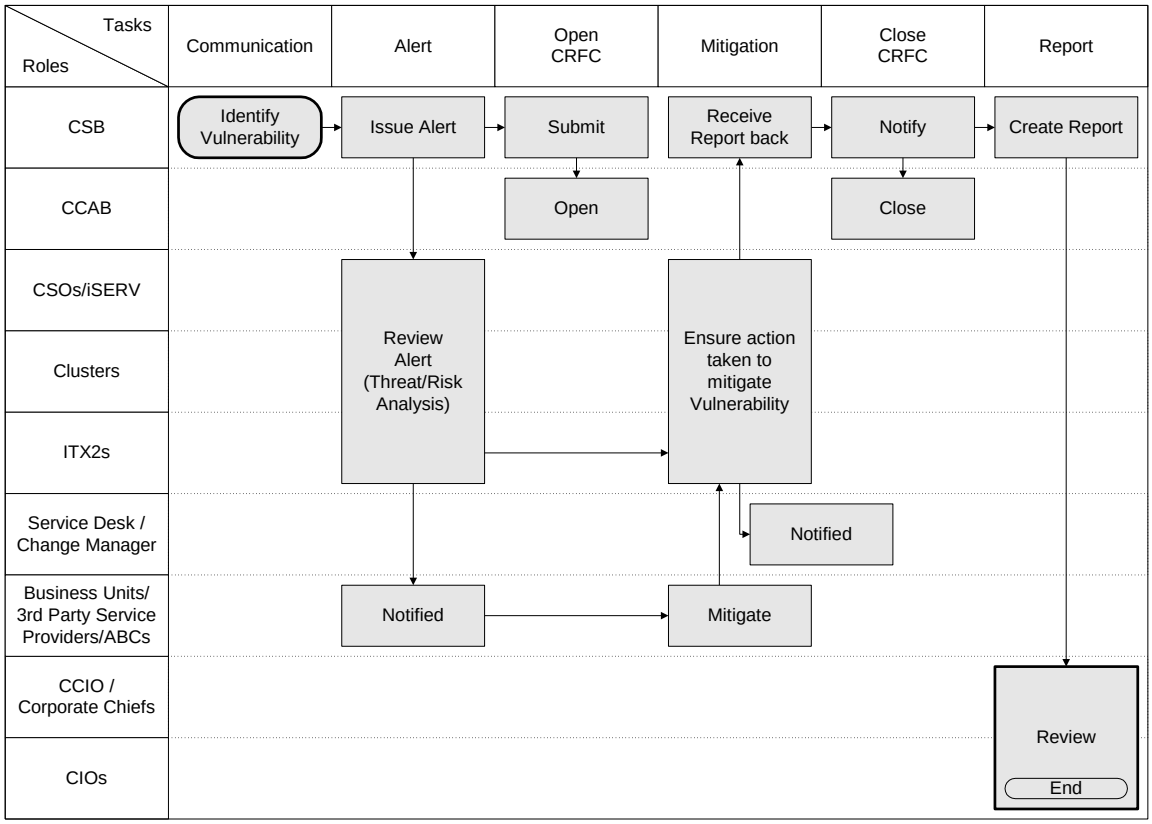

Figure 4 - Severity Three lifecycle

3.4.5 Severity Four

Definition°: Both Threat/Risk metrics are low
Target Timeline: 100% within 90 Calendar Days (3 Months) of Notification
Deployment Approval: Infrastructure Managers
Decision-making Authority: Cluster CIOs
Procedures:

1 – Communication

I&IT Corporate Security Branch (CSB) identifies or is informed of vulnerability.

2 – Issuing Alert

CSB issues Severity Four Alert to all clusters, iSERV and the Network Integrator;

CSB posts alert on the OPS I&IT Security Intranet site (http://intra.security.gov.on.ca);

CSO/iSERV is responsible for informing their Cluster of Patch Alerts;

Clusters are responsible for communicating to their third party Service Providers (with the exception of the Network Integrator), Business units within the cluster ministries, and ABCs;

Cluster may adjust Severity level with cause.

3 – Submitting CRFC

CSB submits a "Request for Change" (information CRFC) with CCAB.

4 – Mitigation

Upon receiving alert, CSOs/iSERV ensure appropriate infrastructure managers are informed and that action is initiated to:

- Assess alert to determine if patches are applicable;
- Acquire and test patches (or work-around) or decision made to risk manage;
- Develop deployment strategy;
- Deploy patches or measures for remediation;
- Inform Service Desk and Change Managers.

ABCs and Ministry Business units with IT Centres take appropriate mitigation action;

Third party service providers take action as appropriate and applicable contractual agreements, including reporting progress back to clusters;

Clusters take action as appropriate for iSERV Facility Managed or Co-located Servers for which they have administrative responsibility;

CSOs/iSERV reports to CSB regularly (at least monthly until patching complete) on:

- Severity level assigned by cluster;
- Progress in patching (percent complete) of all infrastructure in cluster ministries;

° NOTE: The Rate of Distribution at which a malicious program spreads may still be used by CSB/Clusters to elevate severity levels.

- Any issues in meeting patching timelines (e.g. need for additional testing).

CSB will take action as necessary on reports;

For iSERV patching: Customer Approval is required for all Patches for Managed Dedicated Server Hosting Services. Customer is consulted and provided with a reasonable window of opportunity (minimum 2 weeks) for review and approval prior to patch deployment;

For iSERV Shared Web Hosting and Infrastructure Servers: Customers are only informed of all changes through the CCAB process. Customer approval is not required.

5 – Closing CRFC

CSB notifies CCAB to close CRFC once patching is complete.

6 – Monthly Reporting

CSB will roll up information OPS-wide and present it as a standing information item in monthly security reports to CCIO, CIOs, and Corporate Chiefs.

The following diagram illustrates the lifecycle of a Corporate Initiated Severity Four:

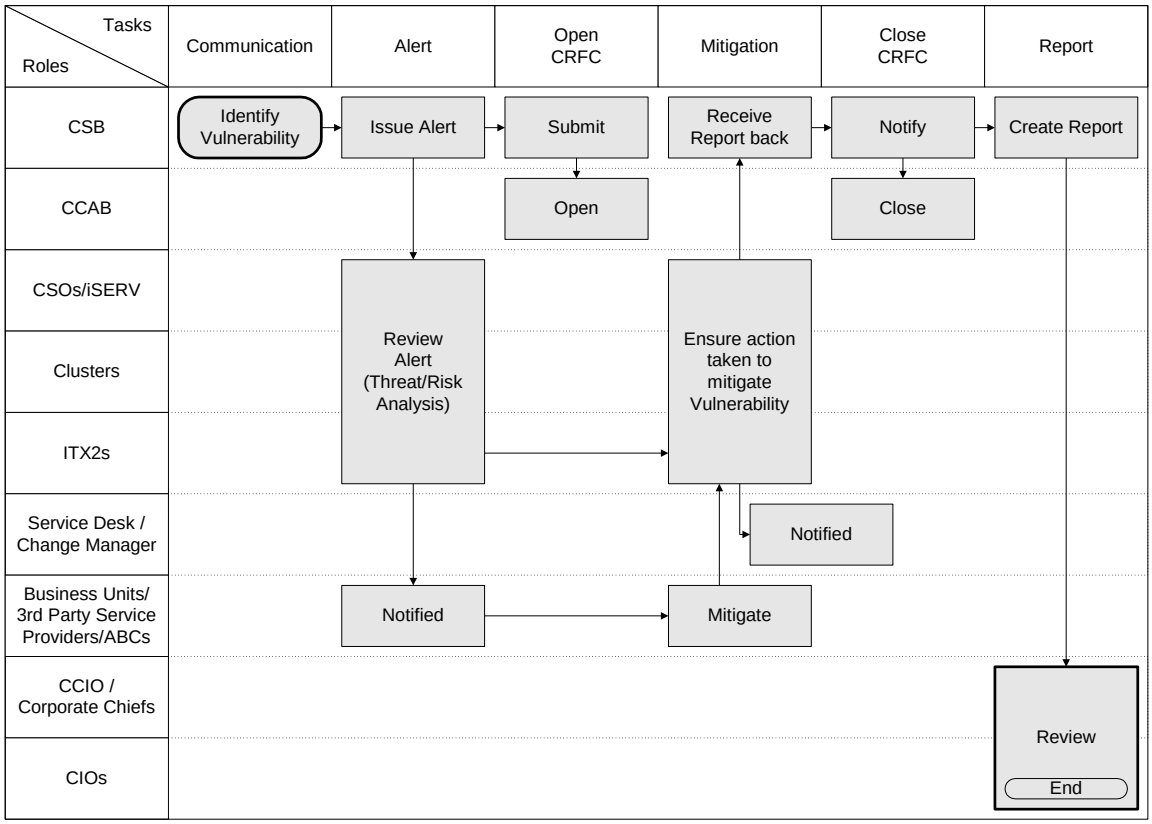

Figure 5 - Severity Four lifecycle

Roles and Responsibilities

3.4.5.1 CCIO

The CCIO is responsible for decision-making in the event of a Severity Zero (i.e. under attack). If the CCIO is unavailable, the Head of CSB acts as the backup decision-making authority.

3.4.5.2 OCCTO – ITSM

Office of the Corporate Chief Technology Officer:

- Enterprise Security Architecture standards;
- Enterprise ITSM best practices and management of CCAB;
- ITSM is responsible for the strategies and procedures underpinning the OPS Patch Management Strategy and is the owner of this document.

3.4.5.3 OCCTO – Corporate CAB

CCAB is notified of any emergency blocking of ports, or firewall rule changes.

Responsibilities include:

- Issuing corporate Change Freeze during Severity Zero;
- Informing Cluster CABs when a Change Freeze should be implemented;
- Approving removal of blocks that may have been put in place for a Severity Zero;
- Informing Cluster CABs when a Change Freeze can be lifted.

3.4.5.4 OCCSD – iSERV

Office of the Corporate Chief Service Delivery:

Responsibilities include:

Integrity and availability of the Integrated Network;

Integrity and availability of services managed by iSERV.

Facility Managed or Co-located Servers remain the responsibility of the Clusters to track, report and ensure patch currency. On such servers, iSERV provides the data centre facility with network connectivity and the client has full administrative responsibility for their system.

3.4.5.5 Corporate Security Branch (CSB)

Monitors corporate environment for potential security vulnerabilities. CSB acts as a single point of communication between clusters/agencies and Corporate CAB for patch management. Responsibilities include:

Determining Severity;

Evaluating the potential risk of OPS wide attacks;

Initiating OPS wide Patch Management process as appropriate;

Elevating Severity levels if Rate of Distribution of malicious programs changes;

Preparing alerts/communications and posting information to the OPS I&IT Security Intranet site (http://intra.security.gov.on.ca);

Opening CRFC;

Monitoring and tracking progress of patching efforts, and taking action as necessary;

Lifting Severity Zero alert in consultation with CSOs/iSERV and CCAB;

Closing CRFC when installation is complete;

Rolling up and presenting of patch statistics as standing information items in monthly security reports to CCIO, CIO, and Corporate Chiefs.

3.4.5.6 Head of CSB

Corporate Security Branch Head is responsible for activities of Branch in respect of Patch Management, for notifying CCIO, CIOs and Corporate Chiefs in the event of a Severity Zero, and for acting as a backup decision-making authority during a Severity Zero.

3.4.5.7 Cluster Security Officers (CSOs)

In the context of Patch Management, CSOs act as the single point of contact for communication and reporting between the clusters and the Corporate Security Branch. CSOs are also responsible for ensuring that patching action is initiated. CSOs serve a dual reporting relationship between the clusters and CSB. Responsibilities include:

- Participating in Incident Response Team calls;
- Notifying CSB of Severity Zero initiated at the cluster;
- Informing their Cluster of Patch Alerts;
- Ensuring that patching is initiated at the cluster;
- Reporting to CSB regularly or as time permits on cluster patch progress;
- Reporting to CSB on adjustments of Severity, risk analysis findings and issues with timelines as appropriate;
- Communicating to Service Desk and Change Manager;
- Consulting with CSB and CCAB to lift Severity Zero;
- Updating CCIO, CIO and Corporate Chiefs as appropriate.

3.4.5.8 Cluster CIO/CCSD

CIO responsibilities include:

Ensuring the integrity and availability of all IT (as well as iSERV Facility Managed) infrastructure (ministry and cluster) including maintenance of systems to current patch and anti-virus levels;

Controlling of remote access including the Cluster ministry(ies) as well as network users not covered by key OPS I&IT directives;

Ensure that third party service providers and ABCs comply with standards.

Additionally, a Cluster CIO/CCSD has the ultimate responsibility for cluster/iSERV decision-making in respect of patching for severities One through Four. As such, a CIO/CCSD holds responsibility and decision-making authority for any escalation of patching required and is ultimately accountable if their cluster/iSERV chooses not to apply a patch.

3.4.5.9 Heads of Infrastructure

Cluster Infrastructure Heads (ITX2s) are notified by CSB of Corporate Severity One.

Responsibilities include:

Adjusting Severity level in consultation with cluster CSO when appropriate;

Approving of Severity One deployment;

Ensuring that patching is completed in a timely fashion;

Ensuring that appropriate resources are assigned to patching effort, based on Severity.

3.4.5.10 Managers of Infrastructure

Infrastructure Managers are responsible for approving Severity Two, Three and Four deployment.

3.4.5.11 Application Solution Offices (ASO)

Responsible for testing and verifying the integrity of their applications against proposed patches

3.4.5.12 Cluster/Local CAB

Cluster CAB is responsible for implementing cluster/local Change Freeze during a Severity Zero;

CCAB informs Cluster CAB of setting and lifting of Change Freezes;

Cluster CAB is (as a minimum) informed of patching activity. Some clusters may choose to have their local CAB involved in the approval process for patching activities.

3.4.5.13 Service Desk

Service desk must be kept informed of all alerts and patching efforts, and is responsible for

using this information to assist in Incident Resolution.

Responsibilities include:

Informing users of potential service outages resulting from patching activity;

Communicating any issues arising from patching activity to local/cluster CAB.

3.4.5.14 Third Party Service Providers

Clusters and iSERV must ensure that third parties comply with OPS procedures.

Third-Party Service Providers/Partners/Contractors that have devices that regularly connect or are connected to the common infrastructure must be included within the scope of patching and this requirement must be written into their contracts. Clusters must ensure that: (1) this Operating Procedure is included in current contracts where possible, and (2) future contracts reflect this Operating Procedure.

4 Definitions

4.1.1.1 Change Freeze

A Corporate Change Freeze includes any additions, modifications, deletion to any corporate infrastructure or corporate asset, either directly or indirectly. This includes, but is not limited to: all firewalls, circuits, routers, meet me points, RAS/VPN, DMZ, multi cluster transitions, Messaging - Email, LAN/WAN configurations to core switches and any associated software changes or denial of access to data on any shared services. Note: Any Emergency Corporate Changes will be addressed under the Emergency Corporate CAB policy.

4.1.1.2 Exploit

Exploits are documented procedures, programs, and/or scripts that take advantage of vulnerabilities. Many vulnerability databases provide exploit instructions or code for most identified vulnerabilities. Exploit programs or scripts are actually just specialized software tools for exploiting a specific vulnerability. Such programs or scripts can propagate through email attachments, web pages, network worms, viruses or directed attacks.

4.1.1.3 Patch

A patch (sometimes called a "fix") is an application or software update that provides a quick repair job for a specific vulnerability in an application or operating system. It is often released by the software maker in response to a discovered vulnerability or similar problem in the software. A patch is the immediate solution that is provided to users; it can often be downloaded from the software maker's website. The patch is not necessarily the best solution for the problem, and the product developers often find a better solution to provide when they package the product for its next release.

4.1.1.4 Service Pack

Service packs are collections of patches and product updates, released as a single bundled package. Although service packs can be classified as non-critical updates, they do contain previously released critical updates. All Hot-fixes and critical updates that are released before a service pack (including all patches and updates from previous service packs) are usually bundled into the next service pack when it is released. A Service Pack can often serve as a benchmark or point of reference to determine the minimum level of patching required for a particular purpose or application.

4.1.1.5 Standard Change

Certain repeatable changes with a minimum risk and impact are deemed “Standard”. Standard changes are documented in a list approved by each organization’s Change Manager and reviewed by its CAB. The scope and type of changes that are deemed standard will differ across organizations. An example of a local standard change could be the relocation of a Printer; where as an example of a corporate standard change could be the testing of a UPS.

4.1.1.6 Vulnerability

Patch Management Vulnerability is considered an exposure or mis-configuration in an operating system or other system software or application software component that allows the security policies of the IT environment to be violated.

5 Acronyms

Acronyms	Explanation
ABC	Agencies, Boards, and Commissions
CIO	Chief Information Officer
CCAB	Corporate Change Management Advisory Board
CCIO	Corporate Chief Information Officer
CCSD	Corporate Chief of Service Delivery (iSERV)
CSB	Corporate Security Branch
CRFC	Corporate Request for Change
CSO	Cluster Security Officers
ITELC	Information and Technology Executive Leadership Council
ITSM	IT Service Management
ITX2	Infrastructure Head or Director level management position
LAN	Local Area Network
OCCIO	Office of the Corporate Chief Information Officer
OCCTO	Office of the Corporate Chief Technology Officer
OPS	Ontario Public Service
SMS	Systems Management Server
SUS	Software Update Services
WAN	Wide Area Network

Errata

Created: June 28, 2004

Draft approved by ITSC on November 17, 2004 and clarifications added to the document:

- Lifecycle diagrams enhanced to indicate where process flow starts and ends;
- Synopsis added to the appendix showing the key contents of the procedure (in table format);
- Table of contents updated to reflect new page numbering.

December 14, 2004: Approved by the Architecture Review Board

Document Numbering

Document No:	GO-ITS 42
Title:	Patch Management Operating Procedure
Doc. Type:	Microsoft Document
File Name:	GO-ITS 42 Operating Procedure for Patch Management.doc

Copyright

Appendix

5.1 Appendix A: Severity Lifecycles

5.1.1 Summary Table

Severity	Description	Timelines	Communications		CCAB	Local CAB	Approval of Deployment
			Who is notified	By Whom			
Severity Zero	- *Exploit has occurred;* - Environment under attack.	- Immediate action to protect the Environment.	- CCIO, CIOs and Corporate Chiefs	Head of CSB and CSB (for updates)	- Notified of any emergency blocking of ports, firewall rule changes; - Change freeze instituted after CIO/ADM vetting; - Approves removal of blocks.	- Notified Local change freezes instituted.	CSB: - Blocking of port, firewall / changes - Email blocking - Blocking by domain
			- CSOs/iSERV, CCAB - Network Integrator (EDS via TAC by Phone)	CSB			
			- Local Service Desk - Change Managers - Other Cluster resources	CSO			
			- CSB (reports/updates)	CSOs/iSERV			
			- 3rd Party Service Providers, Ministry Business Units, ABCs	Clusters			
Severity One	- Both threat metrics are high AND - Exploit has been published	- 100% within 2 Calendar Days of CSB Notification	- Incident Response group (including CSOs/iSERV) through Conference call	CSB	- CRFC opened by CSB	- Notify of scheduling impacts	- Infrastructure Heads
			- Clusters, iSERV, Network Integrator, identified ITX2s - I&IT Security intranet	CSB			
			- Local Service Desk - Change Managers - Other Cluster resources	CSO			
			- CSB (reports/updates)	CSOs/iSERV			
			- 3rd Party Service Providers, Ministry Business Units, ABCs	Clusters			
Severity Two	- One or both metrics are high and no published exploit	- 100% within 7 Calendar Days of CSB Notification	- Clusters, iSERV, Network Integrator - I&IT Security intranet	CSB	- CRFC opened by CSB	- Notify of scheduling impacts - CCAB member prepares CCAB information	- Infrastructure Managers
			- Local Service Desk - Change Managers - Other Cluster resources	CSO			
			- CSB (reports/updates)	CSOs/iSERV			
			- 3rd Party Service Providers, Ministry Business Units, ABCs	Clusters			
Severity Three	- Two metrics are medium or a mix of medium/low	- 100% within 30 Calendar Days of CSB Notification	- As per Severity 2	- As per Severity 2	- As per Severity 2	- As per Severity 2	- Infrastructure Managers
Severity Four	- Both Threat/Risk metrics are low	- 100% within 90 Calendar Days of CSB Notification	- As per Severity 2	- As per Severity 2	- As per Severity 2	- As per Severity 2	- Infrastructure Managers

5.1.2 Severity Lifecycles Detailed Diagrams

The following are detailed diagrams of the Severity Lifecycles for additional reference.

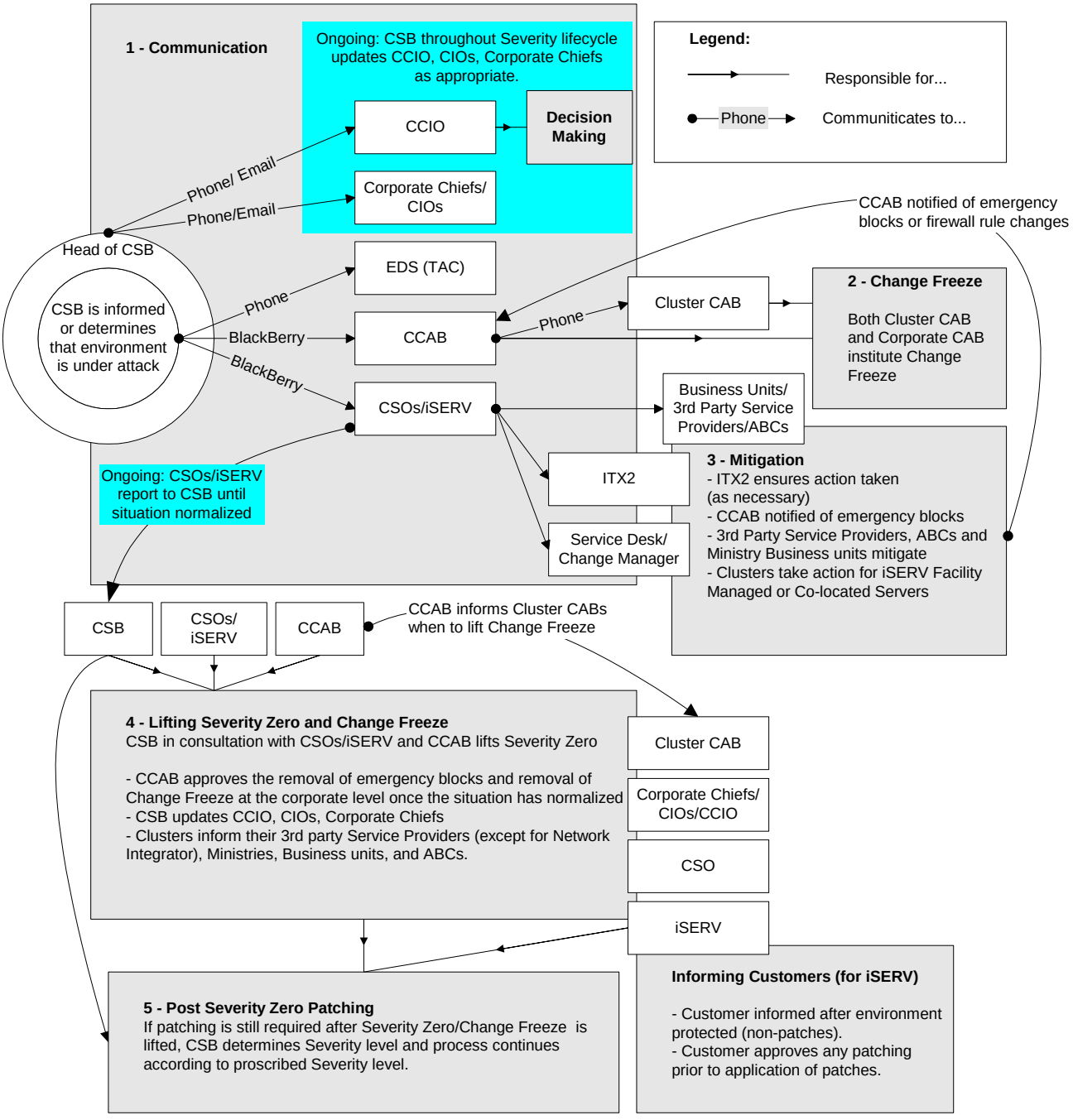

Figure 6 - Severity Zero Lifecycle

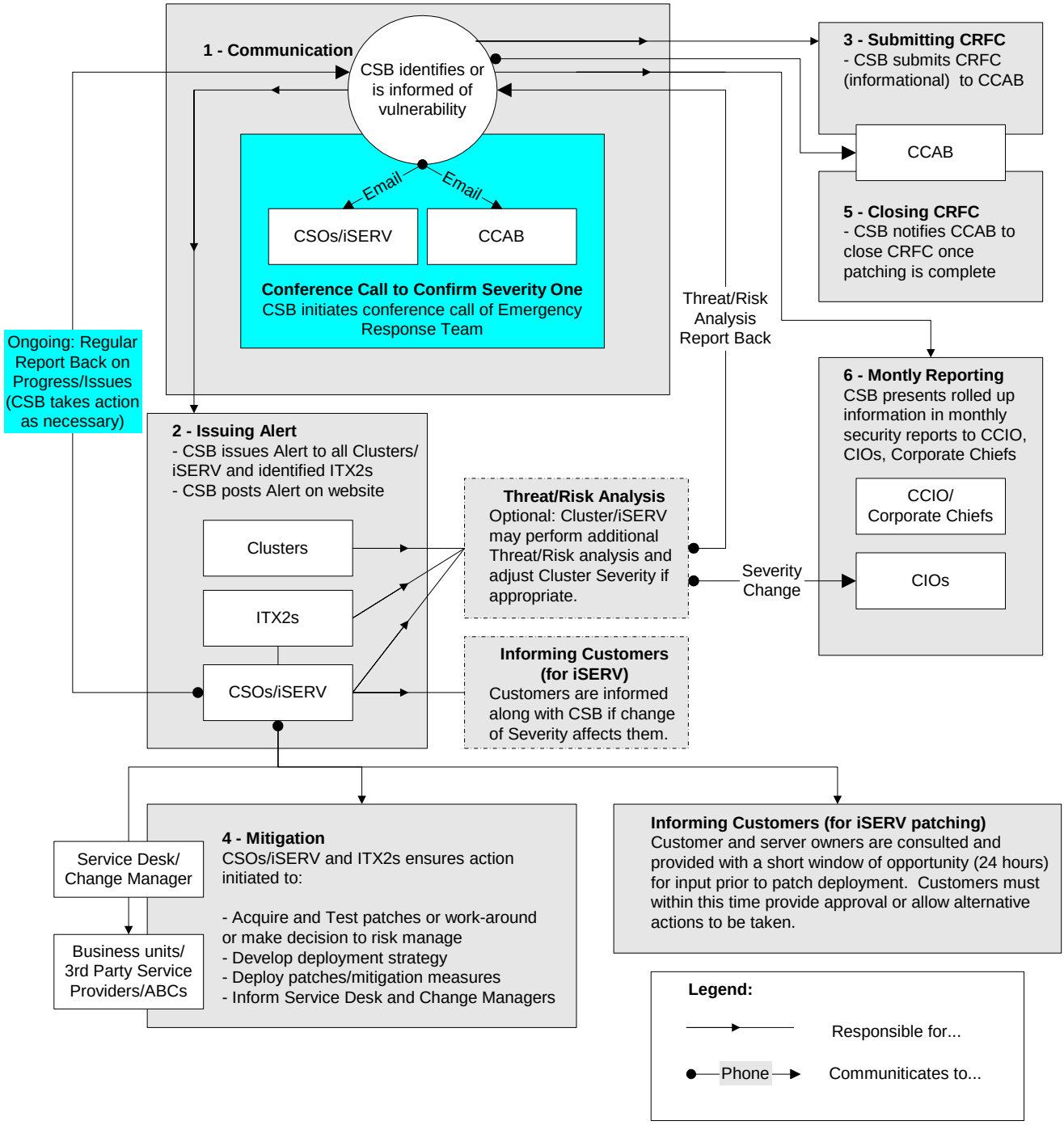

Figure 7 - Severity One Lifecycle

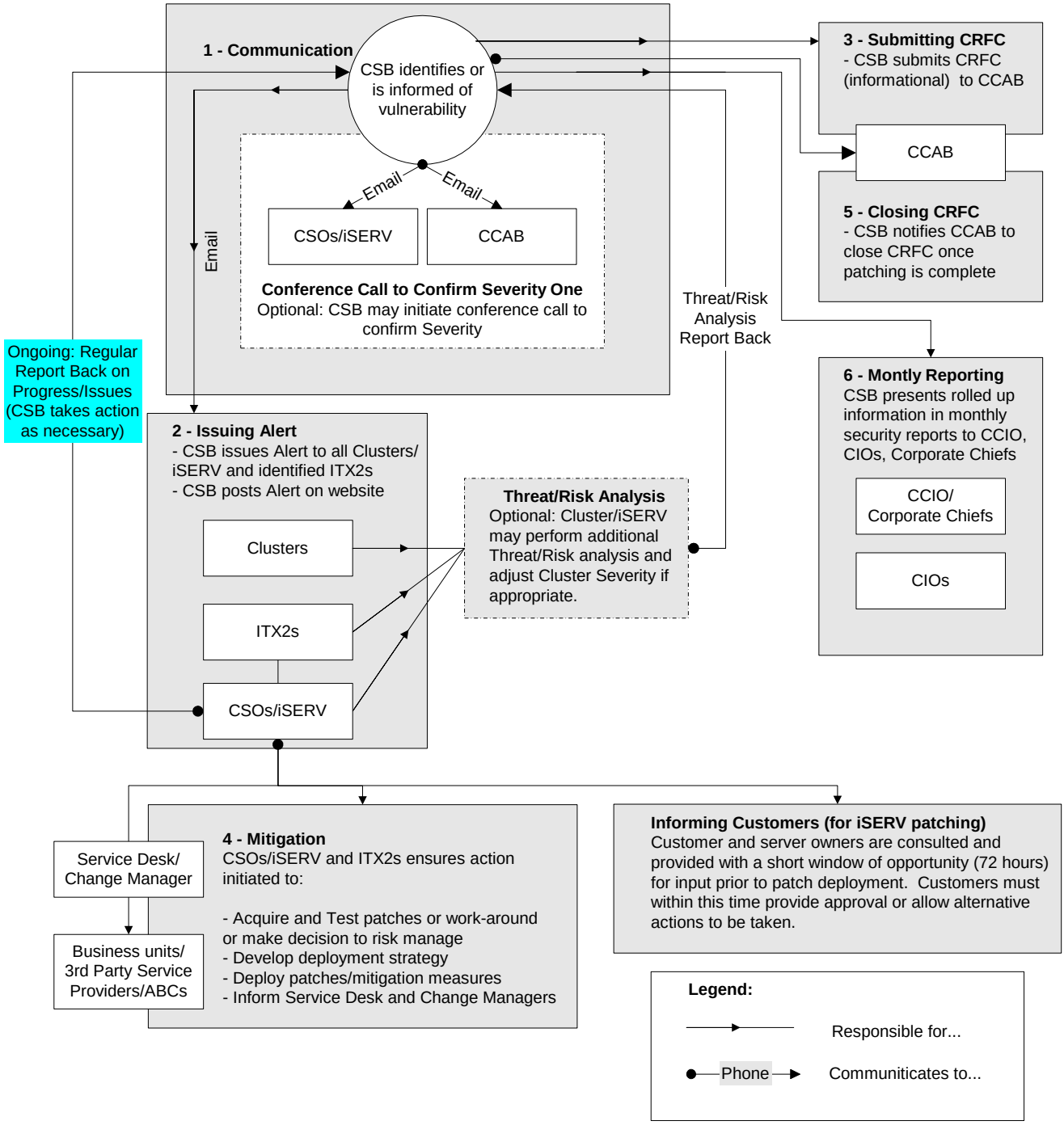

Figure 8 - Severity Two Lifecycle

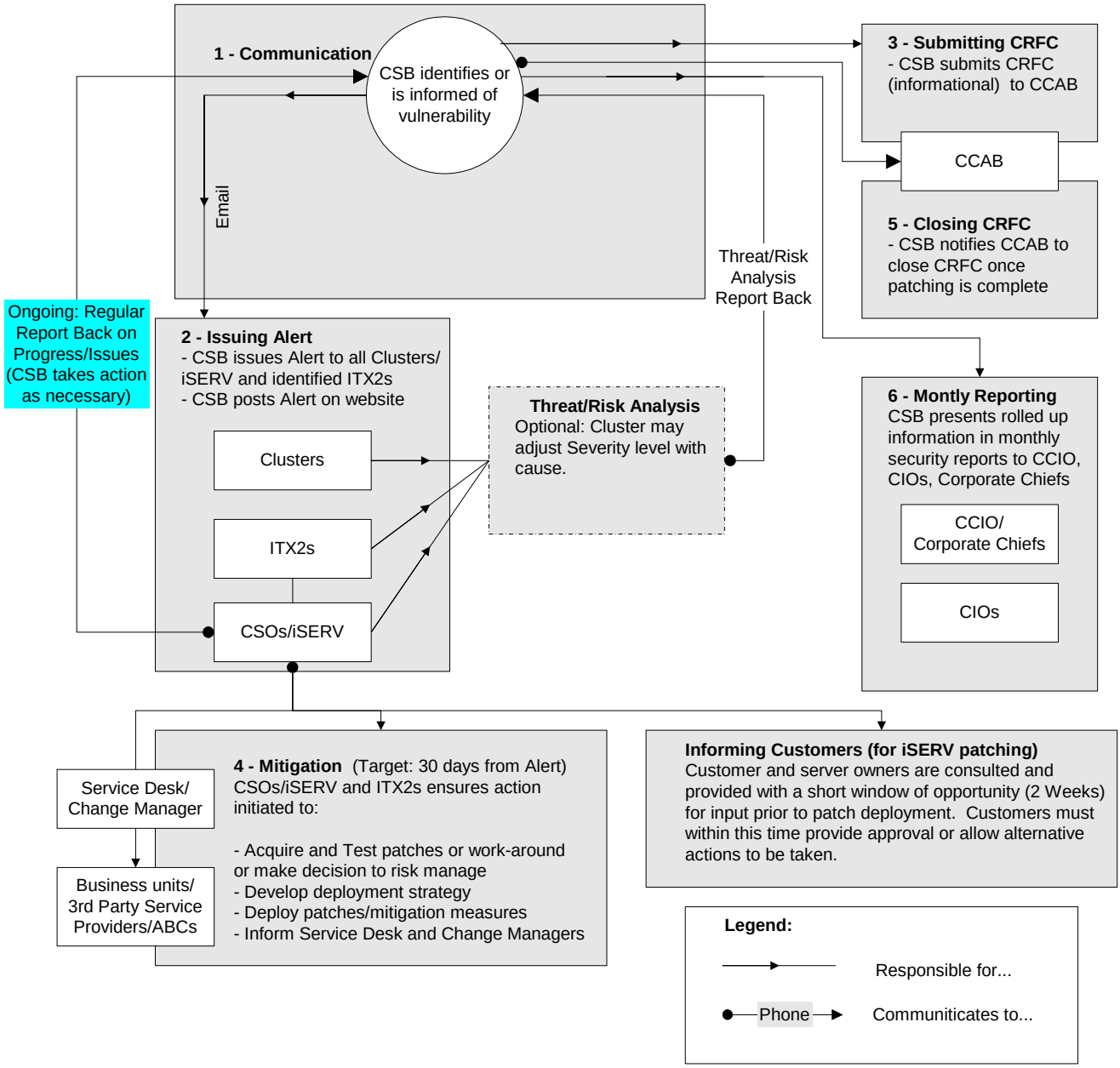

Figure 9 - Severity Three Lifecycle

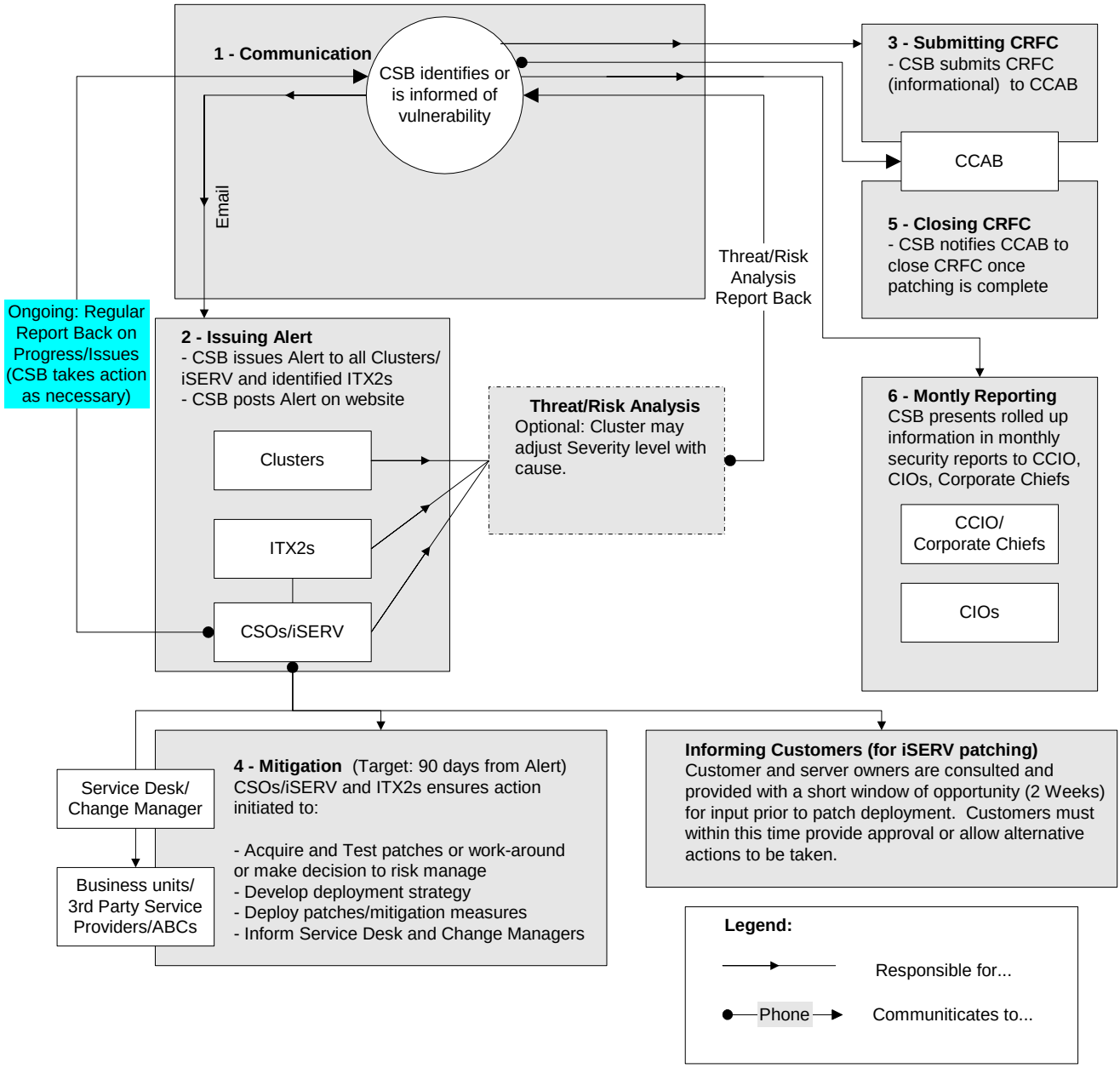

Figure 10 - Severity Four Lifecycle

5.2 Appendix B: Severity Case Examples

5.2.1 Alerts from 2003

1. Blaster
   Initial Assessment
   Extent – *High* – Affects Windows 2000, Windows NT, Windows Server 2003, Windows XP – potential for large number of sites, geographic distribution
   Impact – *Medium* - Causes system instability, compromises security settings
   ⇒Severity 2

   Revised Assessment
   Extent and Impact became high in August, 2003, when the exploit published and further ports to exploit the vulnerability were added to the alert.
   ⇒ Revise to Severity 1

2. Slammer
   Initial Assessment
   Extent of Threat – *High* – affects Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP – potential for large number of sites, geographic distribution
   Impact – *Medium* - degrades performance
   ⇒ *Severity 2*

   Revised Assessment
   Impact increased to high
   ⇒Revise to *Severity 1*

3. Nachi
   Extent of Threat – *High* – affects Microsoft IIS, Windows 2000, Windows XP - potential for large number of sites, geographic distribution
   Impact – *High* – deletes files, causes system instability, compromises security settings
   ⇒ *Severity 2 until exploit published*

4. Possible Denial of Service (DoS) with respect to the H.323 protocol for Microsoft Internet Security and Acceleration Server 2000
   Extent – *Low* – Affects Windows 2000 Advanced Server
   Impact – *High* - Successful exploitation of this vulnerability may allow a remote attacker to execute arbitrary code in the context of Microsoft Firewall Service running on ISA Server 2000. This may lead to complete control of the vulnerable system.
   ⇒ *Severity 2*

5. Cisco PIX Firewall Vulnerabilities
   Extent – *High* - All Cisco PIX firewall devices running the affected software
   Impact – *High* – can crash firewall **No exploit**
   ⇒ *Severity 2*

6. Expiration of VeriSign Global Server ID Intermediate Root CA
   Extent – *Medium* - Internet Information Server (IIS) 4.0 and IIS 5.0
   Impact – *Low* - *Some* users may not be able to establish SSL connections
   ⇒ *Severity 3*

5.2.2 Alerts from 2004

7. MS04-012 - Cumulative Update for Microsoft RPC/DCOM (remote procedure call).

Description:
This update resolves several newly discovered vulnerabilities in RPC/DCOM. An attacker who successfully exploits the most severe of these vulnerabilities could take complete control of the affected system. An attacker could then take any action on the affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges. Microsoft recommends that customers apply the update immediately.

Risk Definition:
Number and types of systems affected: High
Impact and damage: High
⇒ *Severity 1*

Expected Action:
Installation of Microsoft Updates dealing with the affected Software.

8. W32/Nachi.worm.D

Description:
W32/Nachi-D is a worm which spreads to computers at random IP addresses that are infected with W32/MyDoom-A or are vulnerable to the following Microsoft buffer overflow vulnerabilities: DCOM RPC, WebDAV, IIS5/WEBDAV and Locator Service. Computers that do not have the following Microsoft patches installed are vulnerable:
MS03-007, MS03-026, MS-03-039, MS03-049

The worm connects to random IP addresses on port 135 or 445 and exploits these buffer-overflow vulnerabilities to execute a small amount code on computers that have not been patched. The buffer overflow code downloads the worm and runs it. The worm allows itself to be downloaded via a random port above 1024.
The worm spreads to computers at random IP addresses that are infected with W32/MyDoom-A via a backdoor component installed by W32/MyDoom-A that provides access on port 3127.

Risk Definition:
Number and types of systems potentially affected: High
Impact and damage: High
⇒ *Severity 1*

Expected Actions:
Ensure that computers are updated with the patches described in MS-03-007, MS03-026, MS03-039 and MS03-049.
Ensure that computers are updated with the latest anti-virus files.