I2R System Stabilization Tiger Team
Case Management and Communications Track
Summary Report

Author(s):	Melissa Liu
Contributors:	Chris Thomas, Igal Zadkovsky, Andrew Bulatowicz, Ryan Schmierer
Status:	Final
Date:	March 25, 2014

Table of Contents

1. Document Introduction

An analysis of P1 and P2 Alliance cases for I2R systems was conducted in the spring of 2006. The case analysis was focused on identifying causes for the level, increase, and volatility of P1/P2 cases for I2R systems. The case management process itself was not under direct examination at the time; however, issues with both case management and stability reporting were raised as a result of the analysis. Case management became a focus for improvement while the I2R system stabilization initiative was being formed to tackle other stability issues. During that time, the business experienced highly visible case management process failures; as a result, case management was added as a focus area for the program as well.

This document describes the work and results of the Case Management team.

2. Executive Summary

A systematic analysis of P1 and P2 Alliance cases for CACO-managed I2R systems was conducted in April/May 2006. The case data covered the period from August 2005 through March 2006. The case analysis identified key root cause factors behind the level of P1/P2 cases, the upward trend, and the volatility of the case load.

Due to schedule availability of key stakeholders, the P1/P2 case analysis readout was not conducted until the end of May. A "Tiger Team" to address critical stability issues was defined in June. Getting teams in place took a significant period of time; the initial Change Control and Case Management teams were staffed in late July; the C3 Performance team lacked critical resources until late August. Staffing remained a problem throughout the program duration as resources were shifted and replaced multiple times, delaying the work of the teams. The teams stayed in place until December, except for the Performance team, which stayed in place through the March 2007 C3 release.

Initial Situation

This team was created because of very visible case handling failures that were broadly communicated by TS business executives. Two highly business-impacting cases were "stalled" in resolution when they were not promptly routed to the correct support organization. These failures highlighted issues with the case management processes in place for I2R systems. Incident management issues were the impetus for the team; the team also focused on system stability reporting and problem management. The scope of the team was broadened early on to include all critical systems for TAC and CIN, regardless of whether I2R-IT was responsible for supporting each one. Identification of these critical systems therefore became part of the scope of the team.

Work Completed and Results

The Case Management team completed the following high-level work items:

- Instituted formal engagement with GTRC and the Fast Response Escalation Desk (FRED) to provide consistent incident creation and escalation

- Updated templates and aliases for incident communications to provide consistent communications to the right audiences

- Addressed issues preventing identified long-term fixes (LTFs) from being implemented, and got resources approved to begin working through the LTF backlog

- Identified the critical systems for TAC and CIN, as well as critical dependencies and infrastructure for those systems – supporting the work of this team, as well as the Change Control team

- Defined a System Stability Scorecard to provide consistent, business-oriented measurements of system stability for critical systems, regardless of IT ownership

- Improved the weekly I2R Health Report to include TACSUNS and non-I2R Critical Systems, as well as improved summary content and identification of change-related cases

Remaining Work

A complete list of remaining work can be found in Sections 5.5, 6.6, and 7.6. The items are summarized here:

- Implement guidelines for Incident Communications Aliases related to subscription, usage, and maintenance
- Establish process for reporting cost and impact of not deploying LTFs; ensure that LTFs are prioritized for delivery and process is in place for top IT priorities
- Extend SSC reporting to all CA-IT supported applications; baseline System Stability Scorecard
- Continue effort of integration of Non CA-IT supported tools into core operational processes; set up dependencies to ensure impacts are reported into I2R for case visibility and change control

Recommendations for Next Steps

Recommendations for further improvement that may not be currently funded include:

- Institute a Problem Management role within CACO
- Define SLAs for critical systems that formalize business requirements into SLA commitments and address any application priority discrepancies
- Define OLAs with internal IT groups and SLAs with external system vendors to ensure IT collaboration for incident and problem management response is adequate to meet business-facing SLA commitments
- Identify and implement improvements to problem management (RCA/LTF) process, in concert with the corporate IT effort (Critical Systems Resiliency Get Well Incident and Problem Management tracks)
- Align scorecard efforts with Critical Systems Resiliency Get Well Plan Metrics and Monitoring Track

3. Overview

The I2R System Stabilization program (also called the "I2R Get Well Plan") was defined in July 2006. The Case Management effort was a sub-team within that overall program. The background of both the program and the sub-team are described in the sections below.

3.1.   Introduction to the Stabilization Tiger Team

In late 2005 and early 2006, system outages for I2R systems were at a high level (e.g., above 10 during a number of weeks), increasing, and volatile. At the time, not much was known about key causes, areas of greatest problems, and improvements needed. Although root cause analysis (RCA) was and is still performed for each case, these conclusions tended to be focused on each specific case at hand, rather than looking across cases to identify key themes and trends.

An analysis of P1 and P2 Alliance cases was conducted in April 2006 to identify the causes of the level, trend, and volatility of these cases and they key actions needed to address them. The analysis used case data from August 2005 through March 2006. Due to scheduling constraints, the actual review of the results did not take place until late May.

3.1.1. Results of P1/P2 Case Analysis

In the spring 2006 case analysis, several major issues came to light:

- Change management issues caused 35% of the overall case load

- Lack of proactive maintenance policies and processes led to 16%, and probably contributed to another 8%

- Recurring application bugs accounted for 12% of the case load

In the original case analysis, two-thirds of the cases were on non-C3 systems (for example, Software Center). However, the business perceived only C3 to be unstable. The non-C3 applications with the most frequently-occurring outages were: Tablebuild (9% of the original caseload); <company>Live! (8%); SFA (7%); SIPS (5%); CaseKwery (6%); C3 business layer (not considered part of C3 by the support organization-5%); Topic/Google (5%). Of the C3 cases, the most frequently-occurring areas were: B2B (18% of C3 cases); SVO (11%); TSRT Query (9%). Seventy-two percent of the original cases were business-impacting, with two-thirds of those classified as case severity S3.

Case resolution times, which include both time to resolution of the immediate problem (or "short term fix") and time to long term fix implementation, were not studied in the original baseline. The Case Management focus emerged later as the I2R System Stabilization Program was being formed and specific, highly-visible case handling issues were encountered.

3.1.2. Objectives

The objective of the I2R System Stabilization program was to improve the stability of I2R systems by addressing key causes of outages.

3.1.3. Program Tracks

Two program tracks were initially defined: Change Control and C3 Performance. A third track was quickly added based on very visible failures in Case Management (for example, two P1/P2 case outages were delayed around 24 hours before even being routed to the right IT organization to address them).

Track leadership and team membership changed many times over the course of the program, extending the program's planned duration. Final team leadership was as follows:

- Change Control – Iain Campbell (SBS) and Danny Liu (I2R-IT)
    - o Formerly Logan Wilkins, Ed Freeman, Ryan Schmierer
- Case Management – Chris Thomas with Igal Zadkovsky (both CACO)
- Performance – Rajiv Wani (SIS) with Jyoti Sarin (I2R-IT)
    - o Formerly Ed Freeman
    - o This team was not staffed until late August
- Program – Stephen Liem (I2R-IT). Supported through September by Melissa Liu, then by Rodney Rowell

3.2.   Case Management Track

The Case Management track was the last track to be identified. This effort emerged as a formal improvement track after very visible case handling failures were experienced and were broadly communicated by TS business executives. Two highly business-impacting cases were "stalled" in resolution when they were not promptly routed to the correct support organization. These errors highlighted the fact that there were multiple routes to create Alliance cases for I2R systems and that, depending on the route chosen, the results may not be predictable. It was unclear how the business would know which process to use, or that the business was using the correct process for any given situation.

3.2.1. Team Objectives and Scope

The objectives of the Case Management team, as ratified in the August 17 Sponsors meeting were:

Address issues in the existing P1/P2 case management processes

Assess the Critical Systems to understand their full scope in the context of global operations, how they are being managed today, and any changes needed in to integrate them into core operational processes

Establish key metrics to support business evaluation of IT performance against SLA-based expectations

When the team was initially formed in July, the focus was on case management purely for I2R systems managed by CACO. With the addition of a new business sponsor in

August, the scope was broadened to include critical TS systems outside I2R control, such as MeetingPlace and <company> email.

The scope boundaries were revised to as follows:

Address issues in the existing P1/P2 incident management processes:

Scope includes "Top X" systems for TAC and CIN

Includes processes for opening, escalating, managing, performing root-cause analysis, and communicating case status

Establish key metrics to support business evaluation of IT performance against SLA-based expectations:

Scope includes "Top X" systems for TAC and CIN

The Case Management team drove the effort to define the systems that comprise the "Top X" critical systems list[1] for the TAC and CIN portions of the I2R business process, working with the SBS team to ensure the list matched actual business priorities. The Critical Systems list can be found in Section 7.

3.2.2. Guiding Factors

Several guiding factors guided the work of the team:

- The as-is case management processes should be reviewed to identify whether problems encountered are gaps in the process or in the *adoption* of the process, and should be addressed accordingly

- Business users do not necessarily know which IT organization supports which critical tool they use; where possible, any fragmentation of the IT support structure behind critical tools should be transparent to the business community

- The team should address case management issues and stability reporting for all critical TS tools

3.2.3. Team

The Case Management team was in place from late July through December 1, 2006. During that time, team membership changed several times, hindering the work of the team.

The team consisted of the following members:

Team Member	Role
Chris Thomas (CACO)	Lead
Igal Zadkovsky (CACO)	PM, co-lead
Nazia Ali (CACO)	Case management processes
Andrew Bulatowicz (CACO)	Case management processes

---

[1] The "Top X" systems list is now referred to as the "Critical Systems" list.

Team Member	Role
Scott Curtis (GTRC)	Case management processes
Dan McQueen (TACSUNS)	Case management processes
Zach May (TACSUNS)	Case management processes
William Mulhern (SBS)	Case management processes, system stability scorecard
Ryan Schmierer (CA Biz Ops)	Critical Systems analysis
Bob Keller (CA Biz Ops)	Critical Systems analysis, system stability scorecard
Ken Sharpe (SBS)	Critical Systems analysis
Kartik Jaggi (IT Global Ops)	Critical systems analysis
Tim Brown (IT Ops)	Critical systems analysis
Michael DeHaas (CACO)	System stability scorecard
Bob O'Connor (CA Biz Ops)	Team guidance and oversight
Melissa Liu (PRTM)	Final Report

3.2.4. Team Focus Areas

The team focused on three distinct areas of work:

- Incident management, problem management, and case communication processes (collectively, the "case management processes")

- System stability reporting (the stability "scorecard")

- Identification of critical TAC/CIN systems (initially called the "Top X" systems)

Each of these is described separately in the document.

4. Results

Results of the work of this track are described in the sections below.

4.1.   Case Handling Escalations

The specific quantitative metric affected by the work of this team is the number of case handling failures, measured as the number of times that clients escalate issues outside the normal case process. Prior to the work of this team, there were **1-2** escalations per week. **No** occurrences were seen once critical issues with the case creation, routing, escalation, and communication processes were improved.

	Before (Aug 05-Mar06)	After (Aug-mid Dec 06)
Client Escalation Failures[2]	• **1-2** per week	• **None**

4.2.   Incident Management

This section describes the qualitative effect of improvements to the handling of P1/P2 incidents as they occur.

	Before	After
Case Creation	Multiple processes for creating and escalating a case; different routes taken; inconsistent results and stalled cases. (3562 I2R/TACSUNS cases flowing through GTRC in 2006 – without a formal engagement or information on what to do with them)	Clearly defined processes using GTRC as the entry point; processes communicated to user community via revision to TAC engagement process
Case Routing	GTRC called for some cases, but no formal engagement with them or knowledgebase for how to route cases; routing delays	GTRC knowledgebase describing how to handle and route different types of cases Formal engagement for escalation through FRED Formal SLA with GTRC for escalation and routing of cases
Escalation	No path to escalate cases through GTRC Unclear decision process for escalation to management and engagement with vendors; delayed or no engagement for critical cases	Formal SLA with GTRC for escalation and routing of cases Prompt engagement with vendors Prompt escalation to management, including senior management involvement for critical cases
Leadership	No clear leader identified on P1 bridges; unclear who is making decisions and driving resolution	Leadership for the management bridge defined Senior management team defined for engagement in critical cases

---

[2] Situations where clients escalate issues outside the normal case process, due to case handling, routing, resolution failures

	Before	**After**
Communication	Case progress not always communicated to the business Case notes not always updated while cases resolution in progress	Active SBS participation to ensure stability status and progress broadly communicated, and that formal business approval received for needed short-term fixes that may impact user communities Formal and consistent communication format using standard templates for each of the steps in Incident Management Process CACO teams retrained to update case notes during case investigation and resolution – other IT groups still pending

4.3.   Problem Management

Qualitative effect of improvements to the identification and resolution of root cause issues are described below.

	Before	**After**
Issue / Trend Identification	RCA performed at case level; no broader analysis of themes and trends; no categorization to support identifying growing root cause areas	Periodic analysis of emerging issues and key cause areas, categorization in-place to support analysis
IT Coordination	Issues getting key infrastructure organizations engaged promptly; no formal or defined expectations for response with outside external vendors; issues with page response from other IT groups and support vendors	Improved coordination among IT teams to identify and resolve issues (both short-term case response and long-term problem resolution) Some issues still remain for page response <company> and external vendors still not completely aligned on analysis of root cause and long term actions needed
LTF Prioritization	No forum for ensuring LTFs get prioritized and resourced; enhancements prioritized over bug fixes; increasing long-term fix backlog	SBS as engagement point to ensure business prioritizes and funds fixes; clear priorities defined by executives of stability over enhancements; resources funded to work through LTF backlog Weekly process now implemented to review LTF backlog with SBS

4.4.   Stability Reporting

This section describes the qualitative effect of improvements to system health reporting.

	Before	**After**
Comprehensive view	No single view of stability for TS systems; no visibility into non-CACO managed systems health	Visibility and reporting of system health for critical systems, regardless of system ownership
		Health report includes TACSUNS and non-I2R Critical Systems
		RCA/LTF tracked for non-CACO tools as well as CACO tools
Business-orientation	System health metrics lack correlation to stability experience by business	Improved, business-oriented reporting through system stability scorecard
		End-to-end performance monitoring remains open

4.5.   Critical Systems

This section describes improvements to identification and management of critical systems.

	Before	**After**
Identification	Application priorities did not match business priority for key systems and dependencies	Identified critical systems list for TAC and CIN
	IT organizations did not know which systems were most critical to the business	Identified discrepancies between application priorities used to drive support and critical systems list
		Key discrepancies remain to be addressed for two applications
Visibility	IT organizations lacked visibility into some outages that were critical to the business and were only notified through non-standard communications (e.g., email from a VP)	Visibility into issues at the same time as the business
		Critical systems outages to non-I2R tools now included in the I2R health report
		Inclusion of some non-I2R critical systems in stability scorecard – some are still pending
Change Control	No visibility into or control over planned changes to critical TS systems outside of I2R direct control	Critical systems brought in to I2R change management processes

4.6.   System Health

The overall system health – not directly affected by this team – is shown in the table below. The metrics reflect a series of events during the Tiger Team execution that affected system stability, particularly in the September period. Multiple recurring issues were seen in this time frame – starting with a recurring site-specific performance issue in early September, followed by recurring Siteminder and other significant infrastructure-related issues. In addition, a new recurring issue from the September release (related to Workflow) has also caused a number of outages in the period. These issues *significantly* affected the number of cases, the severity of cases, and the number of recurrences, while also degrading the average availability.

The numbers should trend toward improvement in the coming weeks as the performance fixes from the December release, combined with the pending fix for the Workflow issue, make a positive impact on results.

	Before (Aug 05-Mar06)	**After (Aug-mid Dec 06)**
Average cases per week	• **5.7** per week	• **6** per week
Severity	• Severity 1: **0%** • Severity 2: **2%** • Severity 3: **66%** • Severity 4: **33%**	• Severity 1: **3%** • Severity 2: **21%** • Severity 3: **55%** • Severity 4: **22%**
Average Availability (against 99.5% SLA target)	• C3: **99.94%** • SVO: **99.32%** • TSRT: **99.42%** • B2B: **99.84%**	• C3: **99.73%** (99.87% in Q2) • SVO: **99.51%** (99.70% in Q2) • TSRT: **99.14%** (99.42% in Q2) • B2B: **98.84%** (99.65% in Q2)
Recurrences	• **28**% of P1/P2 cases	• **47**% of P1/P2 cases

5. Case Management Processes

Case management processes include the range of activities from opening a case to solving the root cause issue. The following diagram, adapted from IT Infrastructure Library (ITIL), shows the framework and taxonomy used for case management at <company>.
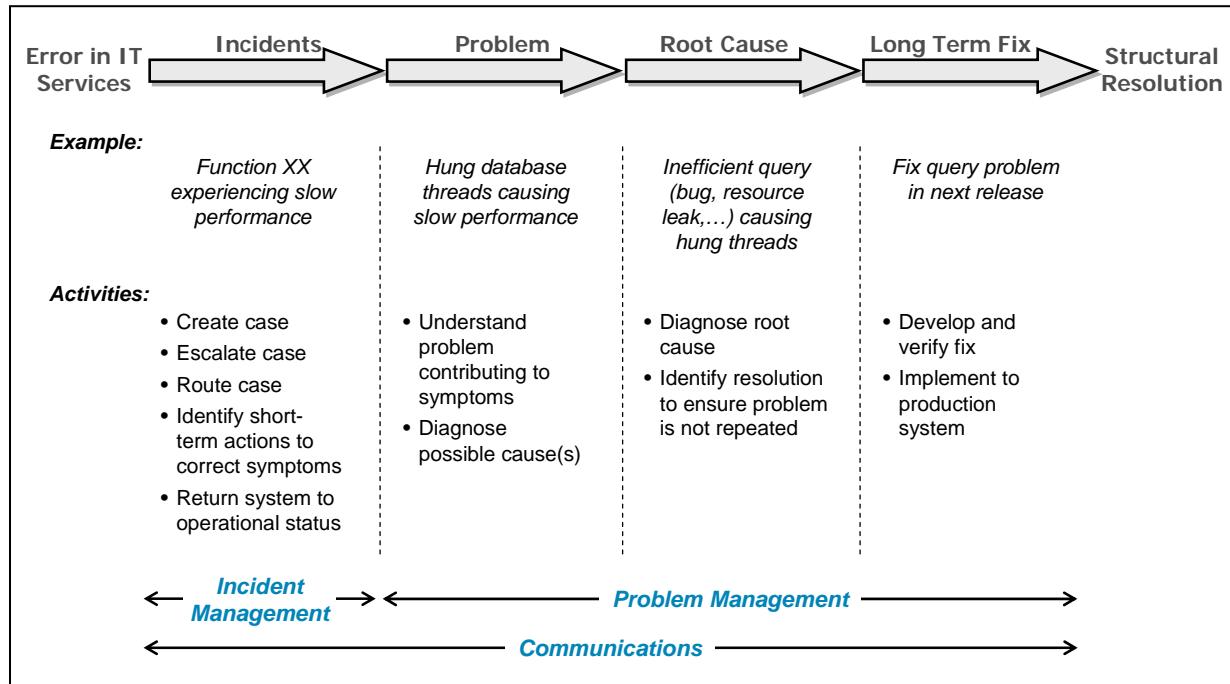
This framework is used to orient the remaining discussions of the baseline and revised case management processes.

5.1.   Starting Point for Process Improvement

This thread of work was begun due to issues with case routing and escalation processes within the incident management process. The team focused primarily on incident management processes, rather than problem management (i.e., RCA/LTF). However, some changes were made to address outstanding issues with the RCA/LTF processes as well.

5.1.1. Incident Management

There was no engagement with the Global Technical Response Center (GTRC), the organization that provides front line support services across <company>. Multiple routes were available to create and escalate a case, including:

- Using the web functionality (creating the case as a P4)
- Calling the GTRC to create and/or escalate a case
- Using the CACO FastTrack process (available to duty managers only)

Either of the first two methods initially routed the case through the GTRC. However, because there was no formal engagement with the GTRC, the routing for the case in either one of those scenarios was unpredictable. The GTRC did not have a knowledgebase for how and where to route cases of different types. If the business stakeholders did not take the FastTrack route, the cases could be delayed for up to 24 hours – even if the problem was of sufficient impact to merit designation as a P1. There was no way to escalate a case through the GTRC, as there was no engagement with the GTRC Fast Response Escalation Desk. The CACO Fast Track process was available for CACO-supported applications only.

The support structure for I2R applications was not necessarily clear to the business. For example, CACO supports a set of I2R critical systems, but not others such as MeetingPlace, email, etc. The FastTrack process was for CACO-managed applications specifically. Without a single-point-of-contact support structure, the business would have to know which IT organization supported which application, as well as the organization-specific procedures for prompt case escalation and response within each IT support group.

GTRC handled **3562** cases against I2R systems in 2006 – all without a process that defined how to handle the cases.

A second major gap in incident management processes at the outset of the Tiger Team was in communication of case status. In specific examples, the cases were not updated while the case was being worked, which gave business users the impression that no work was happening to address the issue. In other cases, the communication of case status was inadequate. Depending on complexity and duration there could have been multiple CACO support analysts responsible for managing incident communication. The format, content, and distribution were chosen by the CACO support analyst handling the case at the time, resulting in many inconsistencies in incident management communications.

The last key gap noted at the outset was a lack of leadership and formal decision-making for activities that occurred during P1/P2 incident management. For example, while many people may be on a P1 bridge, no one knew who owned the overall case and was in the driver's seat making the decisions. Also, formal decision-making for decisions such as restarting a server was not clear; in some cases, restarts were performed without business approval (e.g., from the functional duty manager) to ensure that the restart was performed at the best time for the business.

The as-was P1 and CACO Fast Track processes are shown in Sections 11.1 and 11.2.

5.1.2. Problem Management

There were acknowledged issues with the RCA/LTF processes as well, some of which were noted in the original P1/P2 case analysis.

The RCA process is and was most effective at identifying technical problems. The RCA process is not suited to identifying either process issues (particularly cross-organization gaps) or technical issues of a more strategic nature (e.g., performance trends that are starting to cause an increasing number of issues and need to be addressed). RCA is performed at a case level only – looking across cases to identify contributing factors is not part of the RCA process. Some CACO analysis does attempt to do this (the "CACO

RCA process"); however, the organization has not traditionally been successful getting identified issues addressed, as most of these types of issues have cross-organizational impact.

Long-term fix (LTF) implementation had significant gaps. Immediate issues could be addressed under the emergency bug fix (EBF) process. However, once operational status was restored, any needed changes were routed through the LTF process. LTFs were generally tactical (minor) changes that could have been included in major or minor releases – BUT, the prioritization process tended to exclude these improvements in favor of enhancements. The Business Approval Committees (BACs) were the prioritization forums; there was no formal or identified communication channel from the CACO client support organization into these forums to get the changes reviewed for inclusion. This gap existed despite the fact that the organization running minor releases (the tactically-focused releases) was also under the CACO umbrella. The CACO release management sub-group looked to the BACs for identification of needed changes; there was no attempt to get candidate changes from the support part of the organization. As a result, a large LTF backlog was created over time. And, the business perception – largely correct, given these gaps – was that, once a case was moved to LTF, "nothing else happened."

At the outset of this program, CACO was responsible for both bug fixes and enhancements. As the prioritization was owned by the business, CACO resources were used to deliver enhancements not fixes. Enhancements were transitioned to IT teams (SRM is still pending); however, during the program there were still insufficient resources to work through the built-up LTF backlog. Those resources have now been allocated.

5.2. Goals

The goal of the Case Management process improvement portion of the initiative was to:

Address issues in the existing P1/P2 case management processes

The scope was defined as including:

- *Critical systems for TAC and CIN*
- *Processes for opening, escalating, managing, performing root-cause analysis, and communicating case status*

5.3. Improvements Made during Team Execution

The following is a summarized list of improvements made to Case Management processes during the Tiger Team:

- Replaced I2R CACO Fast Track process with GTRC engagement and Fast Response Escalation Desk (FRED) process – single point-of-contact for escalation, regardless of IT group supporting an application

- Updated email aliases and communications templates for P1/P2 case communications to provide consistent communications to the appropriate audiences

- Identified communication channel through SBS for LTF prioritization to ensure that LTFs can be prioritized into releases
- Allocated / funded resources to work through LTF back log

The revised case management process is shown in Section 11.3.

5.4. Roles and Responsibilities

This section documents the current (revised) roles and responsibilities for Case Management.

Role Name	Responsibilities
Business User	• Detect and report problems • Work with functional Duty Manager for escalation of critical issues
CACO Duty Manager	• Send page notifications (for CACO-supported applications) • Participate in P1 bridges • Drive incident post-mortem and send incident summary email within 10 days of resolution
Functional (e.g., TAC) Duty Manager	• Detect and report problems • Contact GTRC to escalate cases as needed • For TAC DM, communicate case summary information, support processes to be used during an outage, workarounds (e.g., temporary use of WebTickets) to TAC organization
GTRC	• Open and escalate cases at business request • Determine priority and escalate to IT Ops
Infrastructure Organizations	• Participate in technical and management bridges as needed • Participate in resolution of P1/P2 cases as needed
IT Ops	• Identify outages via EMAN monitors • Identify severity for cases • Page appropriate individuals for case handling • Open technical and management bridges
Management	• Participate in management bridges as needed
SBS	• Send partner, customer, and business leadership communications

Role Name	Responsibilities
Support Teams (I2R and non-I2R teams)	• Send incident notification, update, and resolution communications to specified email alias(es) or users • Troubleshoot and resolve issues • Capture request for change information for needed LTFs

5.5.   *Continuing Work*

The following items are continuing activities past the conclusion of the Tiger Team:

Action	Owner	Contributors	Timing
Identify and implement improvements to problem management (RCA/LTF) process, in concert with corporate IT effort	Chris Thomas (CACO), Kartik Jaggi (EIO)	CSR Problem Management team	Dec-Mar
Implement guidelines for subscription & usage of the Incident Communication Aliases	Chris Thomas	Andrew Bulatowicz, Igal Zadkovsky	December
Implement Process for adding / changing application / group aliases as a result of re-orgs / new apps & maintaining integrity of the alias structure	Chris Thomas	Andrew Bulatowicz, Igal Zadkovsky, William Mulhern	December
Establish Process of reporting cost/impact of not deploying LTFs	Chris Thomas	Iain Campbell, Igal Zadkovsky	January
Ensure that LTFs are prioritized for delivery and process is in place for top IT priorities	Chris Thomas	Iain Campbell	Ongoing
Ensure that all incidents have a PIR / post mortem	Chris Thomas	CSR Problem Management team	January

6. System Stability Reporting and Scorecard

The system stability scorecard portion of the effort aimed to better reflect the system stability experienced by the business, and to provide an integrated view into stability across critical TS systems, regardless of IT support organization.

6.1.   Starting Point for Improvement

At the outset of the program, there was no comprehensive system stability report for TS-impacting systems. The I2R Health Report, produced weekly, showed P1 and P2 cases for CACO-managed I2R applications, availability metrics for a small number of systems, and some summary information for P3-P6 cases. There was no visibility into health data for TACSUNS systems or other IT-managed systems, or into critical TS tools managed outside of the I2R organization.

The Health Report was widely acknowledged to have significant shortcomings in its ability to measure the stability actually experienced by the business.

The number of weekly P1/P2 incidents for CACO-managed I2R systems was the key metric tracked and trended at that time. However, the number of P1/P2 cases did not correspond to the number of actual outages experienced by the business. Automated EMAN monitoring created P1/P2 cases whenever monitored systems went down or became slower than defined as acceptable in the defined monitors. When critical infrastructure components went down (e.g., an outage in a network component or key server), cases were created for all the system elements dependent on that component. As a result, the *case counts* for some outages were magnifications of the root problem (however, they *were* accurate reflections of the degree of systems impacted by the issue).

Although EMAN monitors indicated outages during some peak load periods (due to delays in the monitor responses), it was not clear whether the business actually experienced any degradation in performance during those times. No reliable monitors or systems were in place to measure user-experienced performance. EMAN-reported outages due to slow monitor response, where the reported system was still operational, were generally not considered meaningful. (Examination of trends in EMAN-reported outages most likely *could* have been used as leading indicators of future performance problems, however.)

Cases were categorized as business-impacting or non-business impacting. Quantification of the degree of impact, such as number of users impacted, total duration of outages experienced during the period, criticality of functions impacted, or number of business functions impacted, was not calculated or reported.

The priority of the case (i.e., its existence as a P1 or P2) carried more weight than the severity of the case. However, the priority of the case was significantly tied to the priority of the application, rather than the priority or impact of the actual issue. An issue affecting a single user could potentially be accorded P1 status and be included in highly-visible metrics. The severity was used to indicate the degree of actual impact. However, in practice, most P1 and P2 cases did indicate critical stability issues.

When the P1/P2 case analysis was conducted in the spring of 2006, it was acknowledged that the rate of P1/P2 cases was not a business experience oriented metric. A true DMAIC approach would have started by gathering clearly articulated needs statements with respect to system availability from the business users and defining appropriate metrics from that effort. However, the level of instability was unacceptable to the business and the causes and solutions needed to be diagnosed urgently; gaps in stability measurement were identified as an area to which the team should return later. (A more "typical" DMAIC effort would also have started by putting a particular process under examination for possible improvements, beginning with as-is process documentation. However, many different processes comprise I2R systems operations; it was not known that that time which processes had gaps that contributed most heavily to system instability.)

The stability reporting portion of the effort was kicked off as a result of business sponsor input that significantly improved reporting was needed, and that the reporting should measure stability and performance as experienced by the business.

6.2.   Goals

The goal of the System Stability Scorecard portion of the initiative was to:

Establish a mechanism to support business evaluation of IT performance against SLA-based expectations

Supporting this goal required the following actions:

- Understanding the business requirements for system stability
- Defining metrics that measured outcomes compared to those requirements
- Defining service level agreements (SLAs) that formalize and document the requirements

The focus of the Tiger Team portion of this effort was on the first two items; the third item remains as continuing work for sustaining members of the effort.

6.3.   System Stability Scorecard

The new System Stability Scorecard is organized by IT Service Management process and includes the following metrics:

IT Service Management Process	Critical Success Factor	Proposed Tier 1 Metric
Incident Management	*Minimize Short-term Business Impact*	Number of business-impacting P1/P2 Incidents
		Business impact total score (severity x duration)
	Resolve Incidents within Established Service Times	SLA Rate for P1/P2 Incidents (percentage of incidents resolved within SLA)

IT Service Management Process	Critical Success Factor	Proposed Tier 1 Metric
Problem Management	*Avoid Repeat Incidents*	Number of repeat incidents/recurring problems
	Minimize Long-term Impact of Problems	LTF Cycle Time (case open to fix implemented)
Change Management	*Protect Services when Making Changes*	Number of P1/P2 incidents caused by Request For Change (RFC) implementation
Availability Management	*Maintain Availability and Reliability of IT Services*	Average Availability vs. Target Availability for Critical Business Systems
		Outage Duration and Frequency for Critical Business Systems
		End to End Performance (User Experience)

The business impact score may need to be revised to take into account the number of users affected by the outage, in addition to the current severity and outage duration factors.

End-to-End Performance metrics are not currently available. A centralized IT effort is exploring performance management and monitoring (the "Monitoring" track of the "Critical Systems Resiliency Get Well Plan" program).

The System Stability Scorecard is produced monthly. The stability scorecard pilot can be accessed at the following location: http://ams-filer01a-web.<company>.com/users-m/mdehaas/published/caco/Projects/SSC/SSC_Pilot_v2.html. One tab of the stability scorecard is included as an example below:
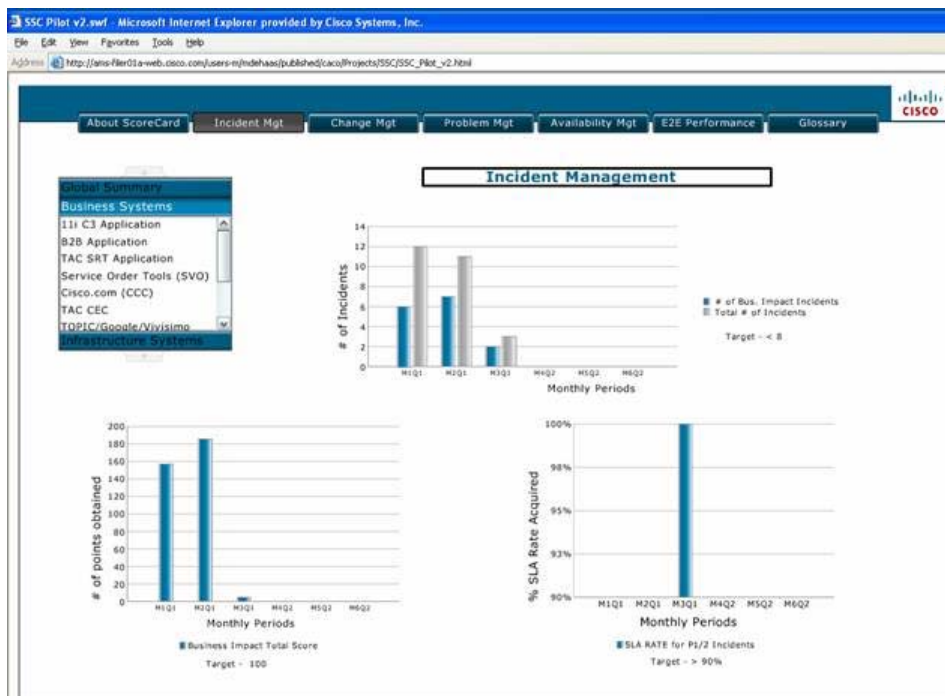
6.4. I2R Health Report Improvements

The I2R Health Report is produced weekly and summarizes the system stability experienced during the week (as well as including some information on the LTF backlog). The following improvements were made to the I2R Health Report during the program:

- Added a case summary table to provide a management-level summary of the specific cases encountered over the week. The summary includes the application, IT owner, summary case data, priority, severity, outage duration, business impact, indicate of recurrence or not, source of the outage, and case owner

- Added summary metrics for stability over the last four weeks compared to target (the target was defined in Q406 prior to launching of the I2R System Stability program)

- Included case counts for non-I2R Critical Systems

- Included case data for TACSUNS systems

- Added indication of which cases were change-related

6.5. Roles and Responsibilities

Roles and responsibilities for gathering and reporting system stability scorecard information are documented below:

Role Name	Responsibilities
CACO	• Gather all system stability scorecard metrics • Produce a quarterly system stability scorecard • Review metrics quarterly with SBS; revise and update scorecard • Produce weekly I2R Health Report
TACSUNS IT	• Provide input for TACSUNS critical systems (currently Email only) to quarterly scorecard • Provide TACSUNS health data for I2R Health Report
Non-I2R Tools IT (e.g., MeetingPlace)	• Provide input for non-I2R TAC/CIN Critical Systems to quarterly scorecard (future – part of broader IT initiative: monitoring track) • Provide health data for I2R Health Report
SBS	• Review quarterly scorecard with CACO • Review quarterly scorecard with key business stakeholders; gather feedback and communicate to CACO
Business	• Review quarterly scorecard

6.6.   Continuing Work

The following items are continuing activities past the conclusion of the Tiger Team:

Action	Owner	Contributors	Timing
Implement an ongoing process of collection, review, distribution & administration of SSC for all P1/P2 I2R-IT Supported applications	Bob O'Connor	William Mulhern, Mahesh Bhumralkar, Michael DeHaas	Quarterly review (tied in with Ops reviews)
Extend SSC reporting to all CA-IT supported applications and to non-I2R Critical Systems for TAC and CIN	Bob O'Connor	Michael DeHaas	**TBD**
Define I2R impacts of non-I2R Critical Systems (e.g., "<company>.com"); set up dependencies to ensure impacts are reported into I2R	Chris Thomas	Ryan Schmierer, Andrew Bulatowicz	January
Baseline stability scorecard results (including all critical tools)	Bob O'Connor	Michael DeHaas	January
Align with Critical Systems Resiliency Get Well Plan Monitoring Track, which will focus on providing key metrics for both critical infrastructure and business systems components	Bob O'Connor	Michael DeHaas	December - March
Align with IT metrics program	Bob O'Connor	Michael DeHaas	**TBD**
Identify a refined approach for integrating user impact factors into stability score card metrics	Michael DeHaas	William Mulhern	January

7. Critical Systems for TAC and CIN

This portion of the initiative emerged from the addition of a new business sponsor[3]. This sponsor brought a much-needed business-centric, rather than IT-centric, view of systems stability. Prior to this point, each IT organization operated independently and provided independent views of their own results. However, the sponsor indicated that the business does not necessarily know – or care – which IT group is responsible for any particular outage. They just want the systems to work, and they want to know who to call when they do not. From these discussions, the scope of this team was broadened to include non-I2R-managed systems that were critical to the TS business community, specifically the TAC and CIN organizations. In order to include those systems in scope, it was necessary to identify which systems actually *were* critical to the business – information not previously well-understood by the IT organizations supporting them.

The focus of this thread of work was to identify those critical "Top X" systems[4]. This analysis supported other work within the case team (Stability Scorecard, Case Management Processes), as well as the work of the Change Control team (to bring critical non-I2R tools into the I2R change control process).

7.1.   Goals

The goal of the Critical Systems Analysis portion of the initiative was to:

Assess the TAC/CIN Critical Systems to understand their full scope in the context of global TAC/CIN operations, how they are being managed today, and any changes needed in to integrate them into core operational processes

The scope spanned across Operational Processes including:

- Incident Management
- Change Management (this analysis supported work by the Change Control team to bring critical tools into scope for I2R change management)
- Communications Management (specifically, communications for P1/P2 cases)
- Problem Management
- Reporting and Metrics

7.2.   Critical Business Systems

Critical Business Systems are Applications, Tools, and Platforms that reside in a data center and are accessed by users to perform core business functions.

The TAC & CIN organizations depend most heavily on systems for case tracking, product ordering, knowledge management, and customer interaction.

---

[3] Steve Gordon, added August 2006
[4] Called the "Top X" systems at that time, because it was not clear how many systems would end up on the critical systems list.

The critical systems for TAC and CIN are listed below. Critical infrastructure supporting TAC and CIN follows in the next section.

System	Function(s)	Key Components
C3	Oracle 11i CRM system	Oracle Forms Interface Core Transactional Modules
TSRT – Create	Web interface for opening C3 Cases	
SVO – Submit	Replacement product ordering tool	
Software Center	Customer software download tool	GLA Tablebuild
<company>.com	Entry site to key functionality	CCO Infrastructure CCx Infrastructure User Profile Authentication
TAC Internal Websites	TAC content and tools	WWW-TAC web content Key eServices Tools
Topic/Google/Vivisimo	TAC search tool	TAC Search Engine Knowledge Content Collections
SALT/CSCC	Contract Entitlement Lookup	
DDTS/CDETS	Engineering Bug Database	

7.3. *Critical Infrastructure Elements*

The TAC & CIN operations are built on a distributed call center business model involving 21 internal and 16 outsourced teams in various global locations. These teams are wholly dependent on core infrastructure services in order to process customer transactions.

Critical Infrastructure components span the globe and form a web of connections between distributed teams, global customers, and centralized business systems.

Critical infrastructure elements for the TAC and CIN are listed below:

Network Connectivity:
- Partner Extranet Connections
- Corporate WAN Links

Telephony:
- Telephones
- Voicemail
- IPCC Call Mgrs

Email:	• Corporate Exchange System
	• TACSUNs Outsourcer Email
MeetingPlace:	• Corporate MeetingPlace Clusters
	• TAC MeetingPlace Systems in SJ

7.4.   Critical Systems Dependencies and Implications

Of the 14 systems identified as critical to the business, a large number of dependencies were identified, complicating the task of providing a holistic view and integrated processes to the business. These 14 systems include over 385 components, each managed and monitored independently, including:

- 9 Meeting Place Clusters w/ 80+ components
- 4 IPCC Clusters w/60+ components
- 128 Email Servers
- 78 WAN Links
- 32 Web Servers
- 6 Databases
- 12 IT Support Organizations

7.5.   Critical Systems Priority Gaps

Based on the analysis of critical systems and dependencies, the following systems need updated priority levels:

- **Distributed Director** devices in the www-tac environment:
    - Current Priority: **P3**
    - Recommended Priority: **P2**

- **MeetingPlace** Components:
    - Current Priority: **P1 or P2**, depending on component
    - Recommended Priority: **P1 for all components**

7.6.   Continuing Work

There is follow-on work for this thread. The analysis identified gaps between defined application priorities used to drive support SLAs and priorities identified by the business. In addition, SLAs and OLAs need to be defined or revised for all critical systems to ensure SLA commitments are aligned with business expectations and needs. Key continuing activities are listed below.

Action	Owner	Contributors	Timing
Identify plan for resolving most critical application priority discrepancies, including funding impact if any	TBD – OpEx	TBD	TBD
Define/revise SLAs for Critical Systems	TBD – OpEx	TBD	TBD
Define OLAs with partners (Infra) to match SLA expectations	TBD – OpEx	TBD	TBD
Add the TAC/CIN critical system dependencies into the report used by CCB for change control.	Iain Campbell	Wendy Middleton	January
Clarify filtering criteria used by IT Operations to identify I2R Incidents and ensure filtering triggers are in place for all of the critical system components and dependencies	Chris Thomas	Ryan Schmierer, Andrew Bulatowicz	January
Modify rules used for Daily I2R P1 Recap reports to include the TAC/CIN critical systems	Chris Thomas	Ryan Schmierer, Andrew Bulatowicz	January
Clarify expectations of CACO Duty Mgrs in managing incidents for non-CACO supported critical systems	Chris Thomas	Igal Zadkovsky	January

8. Findings and Recommendations

Remaining issues discovered over the course of the program, or not addressed by the program, are documented in this section.

8.1.   Findings

Incident Management Gaps

- **Mismatches between Expectations and Support Provided.** Business expectations for issue resolution on critical systems are not always consistent with the I2R-IT support provided. There are some SLA commitments in place between I2R-IT and Business, but SLAs have gaps with respect to performance. In some cases, there are discrepancies between business requirements and the application priority level used to drive support. In addition, the ITIL support process methodology (breaking problems into incident management versus problem management) does not correspond to the support model used by TS with <company> customers.

- **Expectations not Documented for Critical Transactions.** There are limited SLAs that define expected system performance for critical business transactions. SLAs defining required end user experience do not exist.

- **Challenges in Obtaining Prompt Response from Other IT Resources for Incident Investigation and Resolution.** Collaboration among <company> IT organizations and between <company> IT and external vendors has improved since program launch. However, getting internal (e.g., WebMaster, Global IT Ops) and external vendor (e.g., WebMethods, Oracle) support to respond quickly remains a challenge. Internal IT support does not consistently respond when paged out for P1/P2 incidents. External vendor support agreements are not sufficient to meet SLAs established with I2R business stakeholders. P1 bridges still lack a defined "quarterback" calling plays and directing the players.

Problem Management Gaps

- **No Forum for Identifying Process, rather than Technical, Root Cause Issues.** The historical focus is on technology, not process. The technical team that responded to the case also performs the RCA/LTF analysis, which tends to lead to technical RCA identification only. In addition, cases are root-caused at a case level, not across cases to identify recurring themes and trends (e.g., "we can't get a long-term fix for this recurring bug implemented because enhancements keep getting prioritized over fixes"). The CACO case analysis that uses the RCA/LTF process output and then performs additional analysis provides some visibility into these types of issues. But, traditionally – outside of the I2R Stabilization Program – these identified core process and organization issues do not get resolved.

- **Few LTFs Address Broader Technical Issues.** Again, since the RCA/LTF is performed on a case-by-case basis, technical issues that require broad resolution – for example, capacity management, data archiving, architecture gaps – do not get identified as root causes or long term fixes needed. A proactive, ongoing review of issues encountered, themes, and trends is needed. While the ITIL case management process decomposition into incident management versus problem management is intended to solve underlying problems like these, in practice at <company> it does not.

- **No Formal Tracking for Problem Status.** LTF implementation is tracked on an ad-hoc basis. The I2R Health report shows the LTF backlog, but there is no process or owner defined currently for tracking each case through LTF implementation.

- **Not all Incidents Have a Post Incident Review (PIR).** Only Severity-1 and -2 incidents have a PIR. A PIR brings the case response team back together after incident resolution to identify lessons learned and to properly identify the RCA. In other cases, the case owner alone is responsible for RCA/LTF. Bringing the case response team back together post-incident may be more effective at identifying the correct RCA and LTF for the incident.

8.2.   Recommendations

The following recommendations are in priority order.

1. **Recommendation:** *Institute a Problem Management role*
   Priority: High
   Owner: CACO
   Key Organizations and Roles: CACO, Infrastructure, SBS, DLT
   The Problem Manager role can ensure adequate focus on both process issues as well as broader technical issues. Part of the role (an analyst role) would include proactive, ongoing review of issues and resolutions needed. The Problem Manager role is planned to be responsible for identifying trends and reviewing the data on a monthly basis with the SBS and I2R-IT organizations. In addition, the Problem Manager would be responsible for LTF reporting, tracking, and escalation. Part of this role could include driving post-incident reviews to ensure accurate RCA and LTF identification.

2. **Recommendation:** *Define SLAs for critical systems and services that formalize business requirements into SLA commitments and address any application priority discrepancies.*
   Priority: High
   Owner: Operational Excellence
   Key Organizations and Roles: CACO, Business, SBS, IT Tracks
   SLAs must be defined (or revised) to ensure IT support commitments reflect business requirements for support of critical systems. Gaps between existing priority level and business requirements must be investigated and resolved.

Longer term, SLAs defining required system performance for critical business transactions must also be defined; however, implementation requires methods and tools that can monitor and measure system performance at a business transaction level.

3. **Recommendation:** *Define OLAs with internal IT groups and SLAs with external system vendors to ensure IT collaboration for incident and problem management response is adequate to meet business-facing SLA commitments.*

Priority: High

Owner: Operational Excellence

Key Organizations and Roles: CACO, Infrastructure

Response from both internal IT groups and external vendors has improved but is still not always adequate to meet business expectations for response.

Formalization of these requirements – with associated incentives or penalties – is needed to ensure I2R-IT can meet its business users' expectations for support.

9. Metrics

The System Stability Scorecard defines the metrics that will be used to measure case management processes and overall stability. No additional metrics have been defined. The System Stability Scorecard may continue to be revised through the Monitoring track of the Critical Systems Resiliency program. The current stability scorecard pilot can be accessed at the following location: http://ams-filer01a-web.<company>.com/users-m/mdehaas/published/caco/Projects/SSC/SSC_Pilot_v2.html.
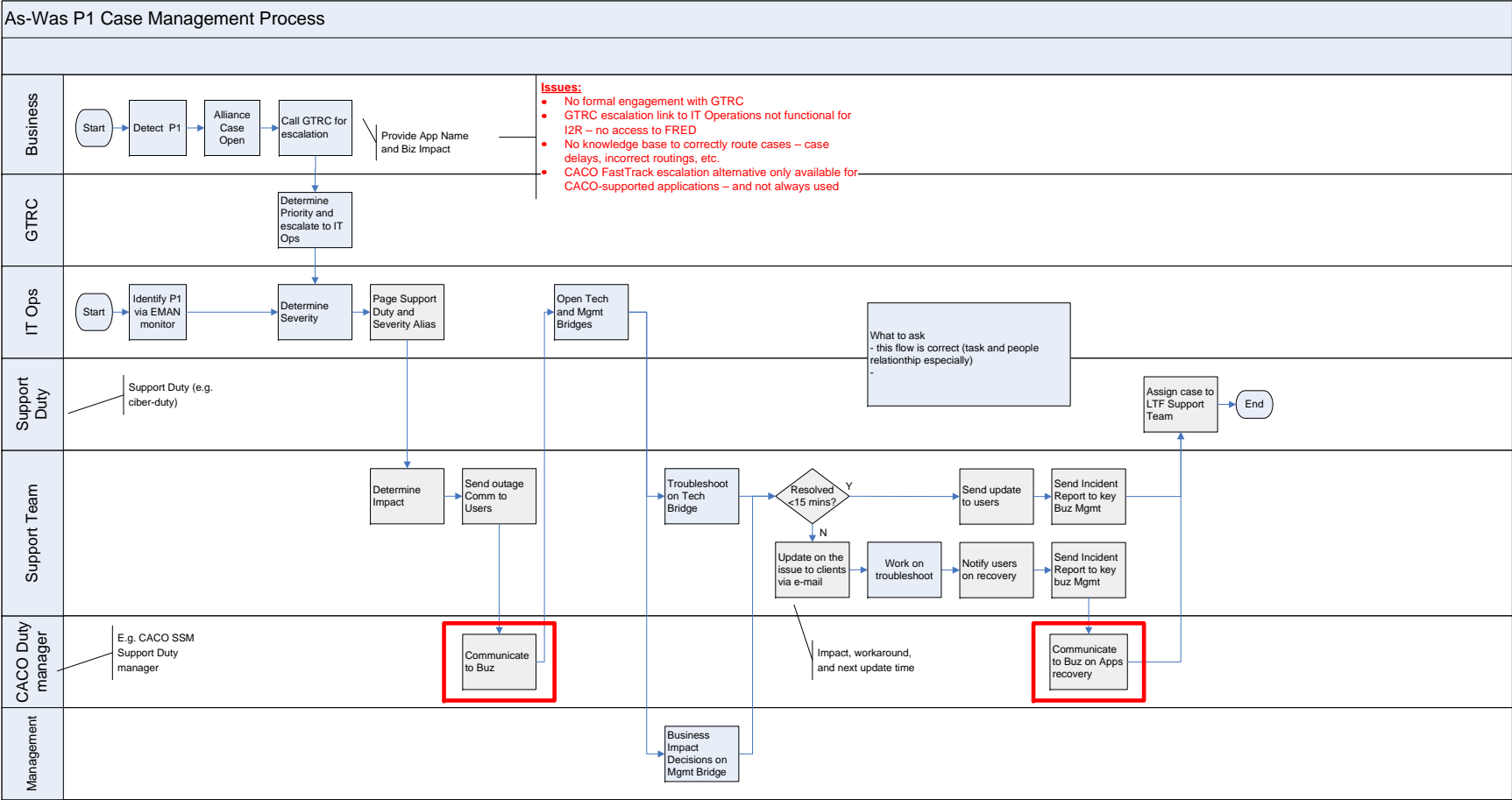
10. Lessons Learned

Lessons learned from the conduct of this effort are listed below:

- **P1 support responsibilities affect commitment predictability.** During specific periods (e.g., early September), the CACO support team spent significant periods of time on P1 case response. Because the Case Management team was driven by CACO, the Tiger Team program commitments during that time were impacted and needed to be re-planned. The notion that a Tiger Team is a "drop everything else and focus on the initiative" type of effort does not work in practice for organizations that have fast-response responsibilities that are not lifted during Tiger Team mode.

- **Shifting scope affects progress and timing.** Early on in the program, the Case Management team had multiple shifts in scope as a new sponsor became engaged (the most notable being the inclusion of non-I2R-supported Critical Systems for TS; focus on as-is process diagnosis was an additional example). The forward momentum of the team was affected a few times as scope changed; however, the scope changes were valuable re-directs for the team.

- **Consistent team membership.** The efforts of the overall program suffered repeatedly due to turnover of key resources.

- **Formal time commitment by all key parties.** Some critical team members were not available to the degree needed. Escalations and re-prioritizations were needed to get participation at the needed level.

- **Strong sponsorship**. This program has benefited since its inception from strong executive backing as to the importance of the program. Despite recurring resource and budget issues – including both resource limits as well as resource decision process shortcomings – the team was always able to eventually get to a solution.

- **Individual contributions**. As always, team outcome is the sum of the collective efforts of all the involved individuals. After all the resource churning was complete, the final team was a very strong team, with significant contributions across the team members both individually and as a group.

- **Streamlined decision processes**. Issues encountered over the course of program were painful, bureaucratic, and time-consuming to address. For example, resource decisions needed (due to turnover or identified shortfalls) required a large number of people, and in most cases multiple discussions, to identify a resolution. A fair amount people-hours during the program was spent trying to get to resolutions for resource issues. The turnover in IT organization leadership (e.g., lack of both a director and a VP for specific periods) probably contributed in part to complexity of the discussions and decisions.

11. Process Flows

Relevant process flows are included in this Appendix. Flows are in MS Visio format in Livelink; locations are specified in References.

11.1. As-Was P1 Process

11.2. *As-Was CACO Fast Track Process*

CACO Fast Track Process

Legend:
Business/CS Duty Manager/Lead: Business Duty Manager
CACO SSM/AS Duty Manager: CACO Duty Manager
Support Team: respective support teams not limited SSM

Business Duty Manager

Start → Detect P1 event → new P1? — N — Open Alliance case → epage CACO Duty Manager, or call GTRC and request to page him/her → End

Confirm resolution

CACO Duty Manager

Problem has not yet been reported (use ITS page)?

if missed, respond in 10 min

Right contact? — Y — Ensure all info is in the case → Can solve in CACO quickly? — Y — Call SSM support team contact → Contact IT Ops

Identify as the support manager for the application team, request IT Ops to create an Alliance case and provides the priority and severity

Facilitate communication (e.g. every hour but depending on the severity)

Distribute final status update (e.g. root cause, STF, LTF) → End

- Duty Manager Name, UserID
- Location/Site (impacted)
- Contact Number
- P1 Event description
- Start time of P1 Event
- Business Impact statement (How the event impacting the business, number of users being impacted at the site?)

Right contact? — N

Can solve in CACO quickly? — N

Valid P1? — N — Request to follow normal case open process → End

Valid P1? — Y

IT Ops

Refer Business Duty Manager to GTRC priority definitions

CACO support, DBA teams, Business or CS duty manager

Set up a bridge and engage with appropriate teams

Support Team (*)

Troubleshoot

11.3. To-Be Incident Management Process

I2R Incident Management Process

Legend:
Detection & Recording | Classification & Initial Support | Investigation & Diagnosis | Tactical (N/Y) | Resolution & Recovery | Tactical Request Process | Incident Closure

Business
Start → Detect P1 → TAC User → (Y) → TAC DM
(N)
TAC DM's have direct access to FRED to expedite escalation process

GTRC / FRED
GTRC Fronline will assess Priority and escalate to FRED → P1/ P2 ? → (Y) → FRED Fast Response Escalation Desk → P3 – P6 Case management process → End
(N)

IT Ops
Start → Identify P1 via EMAN monitor → Determine Severity → Page Support Duty and Severity Alias → Open Tech and Mgmt Bridges

Support Team
Start → Detect P1
Determine Impact
Troubleshoot on Tech Bridge → Resolved <15 mins? → (N) → Investigation & Diagnosis → Resolved? → (N) → Tactical Request → (N) → Assign case to LTF Support Team → CM / Downtime → (N) → End
(Y) ... (Y) ... (Y) ... (Y)
Within 30 min's
Within 30 min's of Resolution
Every 30 – 60 min's
Initial Incident Email (A) Notification
Resolution Email (E) Notification
Incident Update email (C) Notification
CM / Downtime email (H) Notification

CACO Duty manager
CACO I2R Support Duty manager @ts-escalation-duty
Start → Detect P1
CACO Incident Communication Process
Within 15 min's
Initial Incident Page (B) Notification
Within 15 min's of Resolution
Resolution Page (F) Notification
Every 30 – 60 min's
Incident Update Page (D) Notification
Post Mortem → Incident Summary email (G) Notification
Within 10 Days of Resolution
1) Upon Approval
2) One Bus Day prior to execution of CR

CACO Support Delivery manager
Engage with Tactical Delivery Process

Management
Business Impact Decisions on Mgmt Bridge

12. Appendix A. Glossary

Term	Definition
Incident	System issue that resulted in an Alliance case
Incident Management	The process used to address outages and other system issues as they occur
Problem	A system flaw (application, network, hardware, software, etc.) that that produced one or more identified incidents
Problem Management	The process used to ensure that the root cause of system issues is identified and addressed
Short-term Fix (STF)	Change needed to restore a system to operational status
Long-term Fix (STF)	Change needed to address a the root issue for an experienced problem so that it does recur
Root Cause Analysis (RCA)	Process used to identify the core issue that resulted in an Alliance case
Service Level Agreement (SLA)	Formal documentation and agreement between organizations (service providers and service consumers) that reflects the services to be provided and the commitments for those services. SLAs formalize what should become the consumers' expectations for services and service levels
Global Technical Response Center (GTRC)	Centralized <company> help-desk and front-line support organization
Fast Response Escalation Desk (FRED)	Centralized <company> process for escalating cases handled by GTRC

13. Appendix B. References

Reference	Link
System Stability Scorecard Pilot	http://ams-filer01a-web.<company>.com/users-m/mdehaas/published/caco/Projects/SSC/SSC_Pilot_v2.html
Incident Management and Communications Final Report	http://workspace/Livelink/livelink.exe?func=ll&objId=18807119&objAction=Open
Critical Systems Summary Report	http://workspace/Livelink/livelink.exe?func=ll&objId=17493631&objAction=Open
Electronic version of this document	http://workspace/Livelink/livelink.exe?func=ll&objId=18993516&objAction=browse&sort=name

14. Revision History

Date	Author	Version	Change Description
21Dec06	Melissa Liu	1.0	Initial Version