IT Service Management
Process Assessment Report

Cornell University
Prepared by Third Sky, Inc.

DATE

John Worthington  Jeb McIntyre  Reg Lo
Director, Third Sky  Vice President, Third Sky  Vice President, Third Sky
(201) 826-1374  (248) 705-1390  (858) 926-6267
jworthington@thirdsky.com  jmcintyre@thirdsky.com  rlo@thirdsky.com
# TABLE OF CONTENTS

**Executive Summary** ............................................................................................................... 3  
Assessment Context ......................................................................................................................... 3  
Objectives ............................................................................................................................................. 4  
Benefits .................................................................................................................................................. 5  
Assessment Approach & Methodology ............................................................................................... 5  
Summary of Findings .......................................................................................................................... 9  
Summary Recommendations ............................................................................................................. 10  

**Consolidated Results** .............................................................................................................. 12  
Process Assessment Profile ............................................................................................................. 12  
Level Reached ................................................................................................................................... 15  
Reliability of Results .......................................................................................................................... 17  
Overall Findings & Recommendations .............................................................................................. 18  

**Per Process Findings** .................................................................................................................. 33  
Service Strategy .................................................................................................................................. 33  
Service Design ................................................................................................................................... 43  
Service Transition ............................................................................................................................. 81  
Service Operation ............................................................................................................................. 130  

**Appendix** .................................................................................................................................... 173  
Reading the Results of a TiPA Assessment ....................................................................................... 173
EXECUTIVE SUMMARY

This Assessment Findings Report is not a Road Map; it is intended to answer the question,

“Where Are We Now?”

in terms of ITSM process capability and maturity. It is a critical input to obtaining a consensus
on both a vision & strategy for IT@Cornell and a Road Map for adoption of IT service
management.

Answering this question does not always result in an epiphany, but it is a critical baseline point
for beginning an improvement journey. The assessment process is a first step, and continued
assessment must be part of the journey.

The demand for IT services continues to increase, along with greater technical complexity, a
desire for reduced costs and many more alternatives available for consideration than ever
before.

Fortunately, the organization seems to have a sense of urgency and is taking steps to solidify
governance structures, identify opportunities for immediate improvement, and control costs.

The assessment must remain part of these efforts.

ASSESSMENT CONTEXT

Cornell University has determined that adoption of IT Service Management is essential to the
strategic mission of the IT@Cornell organization, and ultimately the University.

The current organization is largely de-centralized, with IT Service Groups and other IT@Cornell
resources providing tailored support for specific customer needs (Type 1 Providers\(^1\)) and
Cornell IT (CIT) providing shared services across all customers (Type 2 Provider). All these
services fall under the IT@Cornell umbrella, and will benefit from standardized ITSM processes
(see Figure 1).

\(^1\) In fact, the ISGs may support more than one business unit making them duplicate Type 2 providers. This can blur
the boundaries between IT support organizations and confuse customers/users.
The intention of implementing IT Service Management is to enable the cohesive and integrated activities of CIT and the ITSG’s and eventually the entire campus in the delivery of end-to-end services to the Cornell community. In order to accomplish this an objective understanding of the current state is necessary.

Third Sky has been engaged to provide the following:

- An Assessment of ITSM Processes with SWOT Analysis
- A Vision & Strategy Workshop
- A Road Map for ITSM Adoption and next actions

**OBJECTIVES**

The specific objectives of the assessment activities include:

- Calibrate process maturity for the identified processes using the TIPA methodology
- Provide input into the Vision & Strategy workshop
- Provide a baseline against which ITSM process improvements are measured.
- Provide a vehicle for the establishment of ongoing communication and feedback about process capability and maturity among all IT@Cornell
- Prepare the organization to continue the assessment process via self-assessment
BENEFITS

The assessment provides the basis for answering the question, “where are we now?” and forms a beginning baseline upon which a Road Map for ITSM adoption may be developed. This enables more effective governance over improvement initiatives and improved ability to measure progress.

Conducting formal assessments demonstrates the organization’s commitment to improvement, and can focus improvement efforts where they are needed based on objective evidence. This can make more efficient use of scarce IT resources.

The approach used by Third Sky is based on the Tudor IT Process Assessment method (TIPA), which uses ITIL and ISO 15504 and establishes a Process Assessment Model based on industry and de facto standards. This provides the following additional benefits:

- Vendor-neutral, structured and repeatable evaluation method
- Process improvement through goal-setting and objective measurement, leading to improved ROI on ITSM projects
- Standardization to compare process maturity with other organizations in the industry

ASSESSMENT APPROACH & METHODOLOGY

The purpose of this assessment is to determine the Maturity Level of the processes at Cornell, to identify best practices that could be shared and to propose an action plan for improvement and alignment.

The assessment allowed for the determination of the Maturity Level of each of the assessed processes individually; it does not give any indication of the overall maturity of the organizational unit implementing the processes.

Processes were assessed using a Maturity Scale going from 1 to 5, with maturity Level 5 being the most mature. Each level is composed of two sublevels, except for level 1, which contains only one. To assess a process, these sublevels are rated using a 4-point rating scale, going from “Not” achieved to “Fully” achieved. For more details, go to the Appendix section Reading the Results of a TIPA Assessment.
**ASSESSMENT SCOPE**

**PROCESSES AND TARGET MATURITY LEVELS**

The Process Assessment Model (PAM) used for this assessment is the TIPA PAM based on ITIL v3.

This table presents the processes investigated within the organizational unit and the highest Maturity Level investigated for each individual process within the assessment. It is called the *target Maturity Level*.

<table>
<thead>
<tr>
<th>Process</th>
<th>Target Maturity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service Strategy</strong></td>
<td></td>
</tr>
<tr>
<td>Strategy Generation</td>
<td>N.A.</td>
</tr>
<tr>
<td>Financial Management</td>
<td>N.A.</td>
</tr>
<tr>
<td>Demand Management</td>
<td>N.A.</td>
</tr>
<tr>
<td>Service Portfolio Management</td>
<td>2</td>
</tr>
<tr>
<td><strong>Service Design</strong></td>
<td></td>
</tr>
<tr>
<td>Service Catalog Management</td>
<td>2</td>
</tr>
<tr>
<td>Service Level Management</td>
<td>2</td>
</tr>
<tr>
<td>Capacity Management</td>
<td>N.A.</td>
</tr>
<tr>
<td>Availability Management</td>
<td>2</td>
</tr>
<tr>
<td>IT Service Continuity Management</td>
<td>2</td>
</tr>
<tr>
<td>Information Security Management</td>
<td>N.A.</td>
</tr>
<tr>
<td>Supplier Management</td>
<td>N.A.</td>
</tr>
<tr>
<td><strong>Service Transition</strong></td>
<td></td>
</tr>
<tr>
<td>Transition Planning &amp; Support</td>
<td>2</td>
</tr>
<tr>
<td>Change Management</td>
<td>3</td>
</tr>
<tr>
<td>Service Asset &amp; Configuration Management</td>
<td>2</td>
</tr>
<tr>
<td>Release &amp; Deployment Management</td>
<td>2</td>
</tr>
<tr>
<td>Service Validation &amp; Testing</td>
<td>N.A.</td>
</tr>
<tr>
<td>Evaluation</td>
<td>N.A.</td>
</tr>
<tr>
<td>Knowledge Management</td>
<td>N.A.</td>
</tr>
<tr>
<td><strong>Service Operation</strong></td>
<td></td>
</tr>
<tr>
<td>Event Management</td>
<td>2</td>
</tr>
<tr>
<td>Incident Management</td>
<td>3</td>
</tr>
<tr>
<td>Request Fulfillment Management</td>
<td>2</td>
</tr>
<tr>
<td>Problem Management</td>
<td>2</td>
</tr>
<tr>
<td>Access Management</td>
<td>N.A.</td>
</tr>
<tr>
<td><strong>Continual Service Improvement</strong></td>
<td></td>
</tr>
<tr>
<td>Service Improvement</td>
<td>N.A.</td>
</tr>
</tbody>
</table>
The assessment took place at the following locations:

- CIT offices in the Computing & Communications Center (CCC)
- CIT offices in Rhodes Hall

The organizational units involved in the assessment (outside of CIT) included:

- Central Library and Mann Library
- College of Agriculture & Life Sciences
- College of Arts & Sciences
- Student & Academic Services
- Computing & Information Science and the College of Engineering
- School of Industrial & Labor Relations and the School of Hotel Administration
- Veterinarian School
- Facilities

- Assessment to be completed with final report by Thanksgiving 2011
- Vision and Strategy workshop will be delivered in December 2011.
- Roadmap will be created within 2 weeks of completion of the Vision and Strategy workshop.

Various roles were involved in the assessment that was outlined in the Project Charter for the assessment. Participants in the interview process are also found in the Project Charter.
CONFIDENTIALITY AGREEMENT

In accordance with the confidentiality agreement defined in the Assessment Project Charter and in accordance with the requirements defined in ISO/IEC 15504, this report does not include details of the assessment results of individual interviews. The Process Profile is the result of the consolidation of various interviews. It does not lead to any conclusion about the maturity of a particular individual.

Participants in the assessment have been assured of absolute confidentiality for the information they provide during the assessment interviews. The information obtained from participants cannot be attributed to a particular individual in this report. All discussions about the results have been held in private.

Involved parties have committed:

- To strictly keep confidential and not communicate directly or indirectly to any third party (in any form) any information or document that they have obtained or come across during the present assessment.
- Not to use any of this information or documents outside the scope of this assessment.
- On request, to return to the owner any document that was provided to the Assessors during the assessment.
SUMMARY OF FINDINGS

Processes that enable the definition, agreement, ongoing monitoring and reporting of customer-facing services do not achieve or only partially achieve their purpose.

In fact CIT may not spend sufficient time understanding customer segments, and may not be differentiating core services for varying customer needs. This may be a result of separation between CIT (who offers shared services to many customers), and other business units/ISGs (who focus on customer-specific requirements).

Similarly, processes that directly interface with users of IT services (i.e., Incident, Request) are highly fragmented and may only partially achieve their purpose. Multiple, independent Help Desks and toolsets provide high levels of support for local (business unit/ISG) issues but significantly complicate tracking, communication and resolution activities for cross-unit (often CIT) issues.

In the back office, gaps are mostly a reflection of a lack of high-level dependency data. Specific technical domains may have a good grasp of supporting service dependencies, but dependencies that span multiple technical and/or organizational domains are not captured or maintained.

This inhibits improvement in processes needed to assure service quality and manage risk. With the emergence of cloud computing and virtualization, these areas will increase in importance.

Out of the 13 processes in scope, 9 did not fully or largely achieve a performed (Level 1) maturity; as a result of the process purpose not being achieved, irregular or inconsistent performance (not systematic) and/or the absence of critical work products (inputs/outputs).

The collaboration tools in use for documentation do not necessarily provide an effective foundation for simple and effective document control, and management of process work products was not common across the entire organization.

The results of current levels of process capability and maturity are inconsistent and unpredictable process quality that perpetuates a negative perception of IT (and particularly CIT), and increased risks as customers demand new and more complicated IT service infrastructures.
SUMMARY RECOMMENDATIONS

The following summarizes the recommendations found in this assessment:

AGREE AND ESTABLISH ITSM GOVERNANCE AND PROCESS CONTROLS

The organization must be prepared to establish basic governance over the IT Service Management program, and the individual process improvement projects that drive adoption. This includes Process Ownership/Management, document management and program/project management.

The Vision & Strategy Workshop can help answer some of the questions typically raised about these issues, however they must be addressed in order to achieve sustained improvement and transformation.

CONSIDER KEY IT INITIATIVES WHEN PRIORITIZING PROCESS IMPROVEMENTS

The need for ITSM adoption and key IT initiatives are mutually interdependent. End User Support, Managed Desktop and Virtual Hosted Infrastructure services will demand effective and efficient processes. Conversely, failure or poor performance of these initiatives will make ITSM adoption all the more difficult.

Process improvement efforts must be effectively integrated with these initiatives. In addition, other activities already in progress can help ITSM adoption if leveraged properly:

- Service Catalog Re-Design
- Application Streamlining
- BCP/ IT Service Continuity Planning

The Assessment report elaborates on these efforts and they should be further explored during the Vision & Strategy Workshop.

FOCUS ON REQUIREMENTS DEFINITION AND USER SUPPORT

IT@Cornell, and particularly CIT, would benefit from greater focus on front-office ITSM processes. These include:
• Incident Management

• Service Portfolio, Service Catalog and Service Level Management

These are elaborated in the Assessment Report.

The Consolidated Results section provides graphs of the Process Profile and Levels Reached for all processes in scope, and may be suitable for distribution to all stakeholders in an effort to obtain feedback.

The Per Process Findings provide detail on the attributes and comments from the Assessment Team. This section is best reviewed by a limited number of stakeholders, and in fact may be most useful as a training aid for those who get formally trained in the TIPA/ISO 15504 methodology.

<table>
<thead>
<tr>
<th>Service Portfolio Management</th>
<th>Service Asset &amp; Configuration Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Catalog Management</td>
<td>Release &amp; Deployment Management</td>
</tr>
<tr>
<td>Service Level Management</td>
<td>Event Management</td>
</tr>
<tr>
<td>Availability Management</td>
<td>Incident Management</td>
</tr>
<tr>
<td>IT Service Continuity Management</td>
<td>Request Fulfillment</td>
</tr>
<tr>
<td>Transition Planning &amp; Support</td>
<td>Problem Management</td>
</tr>
<tr>
<td>Change Management</td>
<td></td>
</tr>
</tbody>
</table>
CONSOLIDATED RESULTS

An assessment is performed using information provided during interviews. The following assessment profile presents consolidated results.

PROCESS ASSESSMENT PROFILE

The figures that follow summarize the Process Profile for Cornell University.

All results are based on CIT as the service unit. Per process findings summarize process attributes that generated the findings.
### Cornell University

<table>
<thead>
<tr>
<th>Level 1 Performed</th>
<th>Level 2 Managed</th>
<th>Level 3 Established</th>
<th>Level 4 Predictable</th>
<th>Level 5 Optimizing</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strategy Generation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Demand Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Portfolio Management</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Service Catalogue Management</td>
<td>N</td>
<td>L</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Service Level Management</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Capacity Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability Management</td>
<td>P</td>
<td>N</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>IT Service Continuity Management</td>
<td>P</td>
<td>N</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Information Security Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supplier Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transition Planning and Support</td>
<td>P</td>
<td>N</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Change Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Asset &amp; Configuration Mgt</td>
<td>P</td>
<td>L</td>
<td>L</td>
<td>P</td>
</tr>
</tbody>
</table>

#### Legend
- "Fully"
- "Largely"
- "Partially"
- "Not"

#### Rules
- N: Not Assessed
- NA: Not Applicable
## Process Assessment Report

### CORNELL UNIVERSITY

<table>
<thead>
<tr>
<th>Profile</th>
<th>Level 1 Performed</th>
<th>Level 2 Managed</th>
<th>Level 3 Established</th>
<th>Level 4 Predictable</th>
<th>Level 5 Optimizing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release and Deployment Management</td>
<td>P</td>
<td>N</td>
<td>N</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Validation and Testing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evaluation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Knowledge Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event Management</td>
<td>L</td>
<td>L</td>
<td>N</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident Management</td>
<td>P</td>
<td>P</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Request Fulfillment</td>
<td>L</td>
<td>P</td>
<td>N</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Problem Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Improvement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Legend

- **F**: Fully
- **L**: Sufficiently
- **P**: Partially
- **N**: Not
- **N.A.**: Not Applicable
- **Not Assessed**: Not Assessed

### Rates

- **F**: Fully
- **L**: Sufficiently
- **P**: Partially
- **N**: Not
It is important to understand that at Level 1, a primary focus is on whether the process objectives and expected outcomes are achieved. The Assessment Team does not have to consider all Base Practice attributes of a process in order to determine that Level 1 has been achieved, and the results reflect this.

Where Level 1 is not achieved it may be the result of one or more of the following:

- The process does not achieve its purpose
- The process is performed, but so irregularly or inconsistently over time or in different organizational units it cannot be considered systematic
- Critical Work Products are missing

In these instances some aspect of the purpose of the process may not be fully understood by the organization. Improvement activities can focus on establishing a greater awareness of those needed process attributes.
Achieved Maturity Level

<table>
<thead>
<tr>
<th>Service Area</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategy Generation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Demand Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Portfolio Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Catalogue Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Level Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capacity Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT Service Continuity Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Security Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supplier Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transition Planning and Support</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Asset &amp; Configuration Mgt</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Legend:
- Level Achieved
- Level Not Achieved
- Not Assessed
RELIABILITY OF RESULTS

For each process in scope a minimum of 3 interviews were conducted. Evidence (documentation) was also made available on a Confluence site. Every attribute of every process was reviewed by two or more assessors and given a rating.

The attribute ratings were consolidated based on TIPA and ISO/IEC 15504 guidelines.

Organizational changes taking place during the assessment may have impacted the results; the assessors took every opportunity to orient questions around areas where stakeholders had understanding and experience even if their current position was new.
OVERALL FINDINGS & RECOMMENDATIONS

The per-process findings are consolidated in the Overall Findings section. The SWOT (Strengths, Weaknesses, Opportunities, Threats) for each process is consolidated in the Consolidated SWOT Analysis section, and the section Consolidated Recommendations provides a view of all recommendations contained in the Assessment Report.

OVERALL FINDINGS

SERVICE STRATEGY

**Portfolio Management** where performed, is based on projects and not services. While there is information indicating strategic intent, investments are not analyzed in terms of services. Defining IT services that are relevant to the business continues to be challenging.

There was no evidence of investments categorized into strategic categories (i.e., Run the Business, Grow the Business, Transform the Business). Investments are project oriented and no evidence of value-to-cost ratio of services was observed.

Communication regarding service portfolio decisions, particularly with regard to promoting these decisions to Service Design and other Lifecycle stages, is not in evidence.

SERVICE DESIGN

The significant efforts being made at establishing a **Service Catalog** tends to focus on catalog content and structure, rather than on customers and markets for services. While most of the activities are performed (see Results Analysis), weaknesses in Service Portfolio and Service Level Management may be hampering service definition.

While **Service Level Management** activities are partially performed and some Service Level Agreements (SLAs) are established, there are major weaknesses in key attributes and critical Work Products are absent.

**Availability Management** is largely restricted to technical domains. The process is reactive, fragmented and may be ineffective for Customer-Facing Services.

The principal hurdle to achieving the **IT Service Continuity Management** process purpose and outcomes is a lack of clear required and agreed business timescales for resolution of services, and scope that may be limited principally to the CIT organization.
SERVICE TRANSITION

The **Change Management** process is constrained by the absence and management of key Work Products and related process weaknesses in **Service Asset & Configuration Management**, Transition Planning & Support and Release & Deployment Management.

While there are configuration management activities taking place within technical domains, there is a significant lack of cross-domain dependency data. Configuration data contained in databases (CMDB) are not unified under a single Configuration Management System (CMS).

This results in controls that are not easily integrated with other ITSM processes.

**Transition Planning & Support** is dependent on Project Management, does not follow an accepted policy and does not consistently meet its objectives.

While the **Release & Deployment** process is partly performed, it is almost totally reliant on project management. Significant variations in the process take place due to inconsistencies across technical domains, business units and project management staff.

SERVICE OPERATION

There is **Event Management** process activities that occur, although they are restricted to technical domains.

Some non-CIT business units had slightly higher levels of **Incident Management** process maturity than CIT, however they were unable to leverage their process across domains when needed. The number and type of tools and different Help Desks varies significantly from one organizational unit to another. While process activities are performed, the resulting fragmentation significantly restricts process effectiveness and efficiency, particularly within CIT.

**Request Fulfillment** is not uniform but process activities are performed and it achieves its purpose, however procedures may not be well controlled.

**Problem Management** is ad hoc and reactive, and really an extension of Incident Management. Key inputs are absent and the purpose is not achieved.
## CONSOLIDATED SWOT ANALYSIS

### STRENGTHS

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Stakeholders indicated that some project portfolio management was taking place, so there is an awareness of portfolio management principles in the organization. In addition, the Application Streamlining initiative is using portfolio management techniques from an application perspective.</td>
</tr>
<tr>
<td>2</td>
<td>There is a high level of awareness of the importance of the Service Catalog at an organizational level.</td>
</tr>
<tr>
<td>3</td>
<td>Templates exist for SLAs and OLAs. Some services have SLAs defined.</td>
</tr>
<tr>
<td>4</td>
<td>There are process activities that occur in specific domains that are driven by requirements for high levels of availability (i.e., network, etc.).</td>
</tr>
<tr>
<td>5</td>
<td>The business (via EHS) is seems to be more aware of business continuity requirements and is driving the evolution of IT Service Continuity Management.</td>
</tr>
<tr>
<td>6</td>
<td>The Change Management process is the most mature and accepted process in the organization, and procedures may be well documented.</td>
</tr>
<tr>
<td>7</td>
<td>There were several domains that had a very good grasp of configuration management, including the use of discovery tools (one had written a discovery product) and effective configuration management techniques.</td>
</tr>
<tr>
<td>8</td>
<td>For larger projects, the organization has people with knowledge and experience in transition activities.</td>
</tr>
<tr>
<td>9</td>
<td>There was evidence of Release &amp; Deployment skills and experience in the organization, particularly for larger projects.</td>
</tr>
<tr>
<td>10</td>
<td>Most IT technical domains have a strong understanding of the importance of event management.</td>
</tr>
<tr>
<td>11</td>
<td>There are several organizational units that have strong Incident Management process capability.</td>
</tr>
<tr>
<td>12</td>
<td>Some business units showed significant process capability, including process supports (tools).</td>
</tr>
<tr>
<td>13</td>
<td>There are individual efforts being made to track Problems, and application groups are logging known errors (bugs).</td>
</tr>
</tbody>
</table>
## WEAKNESSES

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The primary weakness is generally poor awareness of business processes, how they serve external customers and what IT services underpin them. Service definition continues to be a challenge, particularly External/Internal Customer-Facing services.</td>
</tr>
<tr>
<td>2</td>
<td>The absence of Service Portfolio and Service Level Management inhibits effective Service Catalog Management.</td>
</tr>
<tr>
<td>3</td>
<td>Lack of Service Level Requirements (SLR) and Service Improvement Plans (SIP) and related policies are major weaknesses.</td>
</tr>
<tr>
<td>4</td>
<td>No Service Level Manager role is defined.</td>
</tr>
<tr>
<td>5</td>
<td>The lack of end-to-end dependency data and agreed service levels perpetuates the status quo.</td>
</tr>
<tr>
<td>6</td>
<td>Absence of Service Level Management and its key Work Products (SLR/SLA) is significantly hindering the effectiveness of the IT Service Continuity Management process.</td>
</tr>
<tr>
<td>7</td>
<td>The lack of documented Change Models, tailoring guidelines and related process areas inhibit the effectiveness of the process.</td>
</tr>
<tr>
<td>8</td>
<td>The principal weakness is a lack of inter-domain dependency data, and a lack of how one domain may impact another.</td>
</tr>
<tr>
<td>9</td>
<td>There is no transition policy, leaving room for variation from one project to another. Reliance on project management for all transition activities increases variation, and may be an inefficient use of project resources.</td>
</tr>
<tr>
<td>10</td>
<td>No dedicated Release Management resources for the project teams to work with.</td>
</tr>
<tr>
<td>11</td>
<td>There is a significant lack of cross-domain dependency data and monitoring intelligence.</td>
</tr>
<tr>
<td>12</td>
<td>The de-centralized nature of IT (multiple Help Desks, tools, etc.) significantly increases the complexity of the process from an IT@Cornell perspective.</td>
</tr>
<tr>
<td>13</td>
<td>There is no consistency across organizational units, and configuration management procedures may vary considerably.</td>
</tr>
<tr>
<td>14</td>
<td>Problems are treated like Major Incidents.</td>
</tr>
<tr>
<td></td>
<td>Opportunities</td>
</tr>
<tr>
<td>---</td>
<td>--------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>1</td>
<td>There are two strategic IT initiatives that may be leveraged in support of advancing the process, the re-development of Cornell’s Service Catalog and the Application Streamlining initiative.</td>
</tr>
<tr>
<td>2</td>
<td>The desire to benchmark IT service costs with other institutions is forcing a re-design of the Service Catalog, providing an opportunity to redefine IT services and supporting process interfaces with Service Catalog Management.</td>
</tr>
<tr>
<td>3</td>
<td>The desire to re-structure the Service Catalog and baseline service costs may present an opportunity to introduce formal Service Level Management.</td>
</tr>
<tr>
<td>4</td>
<td>Some services have clear input from the business regarding the need for high availability, presenting an opportunity to drive business-oriented improvements to availability.</td>
</tr>
<tr>
<td>5</td>
<td>The Business Continuity Planning activities may present opportunities to drive IT service management process improvement in conjunction with the business.</td>
</tr>
<tr>
<td>6</td>
<td>There may be existing procedures that can serve as the basis for Change Models and tailoring of the process.</td>
</tr>
<tr>
<td>7</td>
<td>Strong understanding of the importance of configuration data by staff provides a good foundation for process improvement.</td>
</tr>
<tr>
<td>8</td>
<td>Change Management is reasonably well deployed, providing a basis for improvements in this process area.</td>
</tr>
<tr>
<td>9</td>
<td>Change Management may provide a basis for process improvement.</td>
</tr>
<tr>
<td>10</td>
<td>Some application staff are working on compiling cross-domain dependency data, presenting an opportunity for process improvement.</td>
</tr>
<tr>
<td>11</td>
<td>Multiple organizational units expressed interest in process support (tool) improvement potential; presenting an opportunity for process improvement.</td>
</tr>
<tr>
<td>12</td>
<td>There may be opportunities to apply effective procedures as models for the organization.</td>
</tr>
<tr>
<td>13</td>
<td>There may be basic actions that can begin to raise the awareness of the process.</td>
</tr>
</tbody>
</table>
## THREATS

1. A driving force for the Service Catalog initiative is the desire to benchmark IT services with other institutions. While this may map well to supporting IT services, it may not map well to other (External/Internal Customer Facing) services.

2. While supporting services may be well aligned with other institutions, customer-facing services may not be. Adoption of ‘standard’ supporting services without aligning them to customer-facing services may actually complicate business alignment.

3. The performance of existing services may not be well known or understood, resulting in a poor understanding of customer perceptions.

4. Customers may continue to pursue external service provider relationships in pursuit of higher availability, even when they may not be warranted.

5. The most significant threat may be that the business seeks to ‘outsource’ key services to remove the burden of in-house continuity demands; this may (or may not) result in more efficient/effective IT service continuity and will require IT guidance and leadership.

6. Lack of related process areas will continue to inhibit maturity of the Change Management process.

7. Multiple disparate tools may limit effective integration with Change and other related processes.

8. Cultural factors and separation between applications and infrastructure present significant challenges to process adoption.

9. Domains outside the control of CIT may be hesitant to provide access to event information, and CIT may be unable to require this data or persuade them to provide.

10. Some organizational units continue to invest in the purchase and/or development of independent Incident Management toolsets and process initiatives.

11. Process maturity, where it exists, may be strongly tied to specific business unit needs and not easily transferable to other units.

12. There is low maturity in related process areas (Incident, Availability, Service Asset & Configuration, etc.)

13. There may be basic actions that can begin to raise the awareness of the process.
CONSORTIUM RECOMMENDATIONS

There was generally no management and review of process work products, and key policies around processes were not established.

The decentralized and independent culture at the University results in a lack of effective document control, and efforts should be taken to improve the management and control of process documentation.

More is not necessarily better, and separating policy, process, procedures, work instructions and forms/records may help simplify documentation.

CIT will need to be prepared to stand behind basic policies that enable process adoption; an area all stakeholders felt was a major weakness. This will require careful analysis of what policies can be established and the support of emerging IT governance structures.

One potential area for discussion may be alignment with University governance, risk and compliance units to clearly differentiate between University, IT@Cornell, CIT and departmental policies. There may also be some synergies with the business continuity plan (BCP) efforts in progress.

Process improvement efforts should be managed as projects. While the eventual Road Map will lay out a program over a period of time, each cycle of improvement must be treated as an improvement project. This includes a formal Project Charter that defines:

- Organizational, process and technical scope
- Key stakeholders including Process Ownership, Management, and Sponsorship
- Resources required
- Project Plan

SERVICE STRATEGY

**Service Portfolio Management** was the only process in scope whose primary activities take place at the strategic stage of the Service Lifecycle. Related processes such as Business Relationship Management, Strategy Generation for Services, Financial Management and Demand Management were not in scope.

The pending Vision & Strategy Workshop will help clarify Cornell’s internal/external environment, constraints and SWOT (Strengths, Weaknesses, Opportunities and Threats).
Based on the initial context/discovery process and the assessment findings, there are some clear market spaces that have been identified:

- Managed Desktop Services
- Virtualized Hosted Infrastructure Services
- ‘Core’ Application Services

In order for Service Portfolio Management to manage the portfolio for maximum value and minimum risk, an understanding of how customers within each market space define value is essential.

The Application Streamlining initiative presents an opportunity to build a portfolio of applications, as well as help validate the customer portfolio. When we begin to codify customer outcomes as well (even without formal SLAs), we have a basis for performing basic portfolio management as services become more defined.

Management of strategic change can be facilitated as decision points appropriate to the organization (Define, Analyze, Approve, Charter) are agreed. This also will help fine-tune cost models associated with services over time.

**SERVICE DESIGN**

With a revision to the existing **Service Catalog** already planned Cornell should take the time now to refresh the definition of Services to incorporate the new 2011 ITIL guidance, which identifies:

- **Customer-facing services** - IT services that are seen by the customer. These are typically services that support the customer’s business units/business processes, directly facilitating some outcome or outcomes desired by the customer.

- **Supporting services** - IT services that support or ‘underpin’ the customer-facing services. These are typically invisible to the customer, but essential to the delivery of customer-facing IT services.
Review the current structure and taxonomy of services with the proposed structure that will facilitate benchmarking of service costs with other institutions. Ensure that the new structure will allow alignment with Cornell’s customers, particularly for customer-facing services.

Agree on a standard Catalog Entry wherever possible to improve administration, make the catalog easier to use, and make sure that all services have the minimal information needed for customers and users. The Service Catalog is a marketing document and often the first place IT has to set expectations for services.

For this reason, interfaces with Service Portfolio Management and Service Level Management are essential, and the stakeholders involved in these processes (as well as Business Relationship Management) should participate in the design of the Service Catalog.

The desire to benchmark IT service costs may focus the Catalog on Supporting (Technical) IT services…

Development of Service Level Agreements without formal Service Level Management may be contributing to the negative perception of CIT having an internal focus and lack of service orientation.

The responsibilities for Service Level Management seem to fall on the Service Owners (who are sometimes managers of technical domains). A focus on customers is a secondary responsibility for Service Owners, and their primary technical focus may be re-enforcing traditional perceptions of CIT.
The Service Level Manager is also tasked with gathering service level requirements (SLR); a critical input that was not in evidence in the assessment. In fact, for customer-facing services these tasks may be outside of CIT, which only increases the distance between the organization and its customers.

As new services provided by CIT are defined and designed, it is essential that more emphasis on understanding the utility and warranty requirements of various customer segments be achieved. Placing this entire burden on the Service Owner (who for some services may actually be a Product Line Manager) can result in service offerings not adequately differentiated for critical customer segments.

The codification of desired customer outcomes (utility & warranty) does not imply that formal SLAs must be developed, but there must be some agreement on expectations (SLR) even if in an informal format.

The resulting information will enable the establishment of SLA structures (when the organization/service is ready for an SLA) and base lining current levels of service performance in the meantime.

Finally, there must be a mechanism for Service Improvement Plans (SIP) in order to foster continual improvement. The Service Portfolio Management process should review and approve the SIPs based on business priorities and available resources.

Investments in availability improvements should follow the identification and agreement of service level requirements (SLR) and a baseline of current availability. There may be opportunities as part of continuity management’s involvement in Business Impact Analysis (BIA) to identify vital business functions that can guide availability planning and reporting.

An Availability Plan template may help technical domains capture base level availability information that may facilitate broader-based availability reporting. In addition, the availability plans can identify measurement gaps in the Availability Management Information System (AMIS).
Reporting on availability to customers should be based on vital business functions and the end-to-end requirements from the customer’s perspective. Where this is not achievable, the Availability Plan should identify the gaps and propose improvements that will be collated, prioritized and analyzed through the Service Portfolio Management and Change Management process.

Availability Management staff should participate (along with other staff such as Capacity Management and Event Management) in Problem resolution activity when required.

Several activities associated with **IT Service Continuity Management** can be effectively leveraged for IT Service Management adoption, including Business Impact Analysis (BIA) and Risk Management.

The University has a Business Continuity Plan (BCP) initiative underway, which presents an opportunity for IT to develop greater alignment with the business. The BIA activities will identify and quantify the impact to the business of loss of service, thereby providing a documented source of the services most important to the University. Risk Assessment and Management can also help clarify business priorities and tolerance for risk.

These activities enable the mapping of critical elements of the end-to-end service infrastructure and can be leveraged by all ITSM process areas.

The eventual ITSM Road Map should attempt to maximize the work being done in this area; a few examples include:

- Ensuring Service Level Management is involved in BIA activities and analysis.
- Providing Incident and Change Management with Risk Management data for development of a Risk Matrix to focus priority on impact and urgency that are business relevant.
- Use the BIA and Risk data to aid decision making in Service Portfolio Management.

As the business has become more dependent on IT Services, it is essential that IT play an increasing role in the Business Continuity Plan. This may present opportunities for ongoing strategic dialog.
**Change Management** is the most mature process in CIT, in part due to the persistent efforts of key staff (principally the Change Manager) over the last two years. The establishments of a Process Owner, and steadfast effort over time have made progress.

While significant improvements in this process area may depend on related processes -- such as Service Asset & Configuration Management, Transition Planning & Support and Release Management -- there are some more immediate actions that could benefit the organization.

There is a significant amount of documentation associated with the process, including measurement and reporting on process performance. However policy and procedural information tends to be integrated into the overall documentation and may be unclear to stakeholders.

Separation of procedural information from policy and process documents may also enable existing procedures to be used to establish Change Models that become part of the overall process. This may present opportunities to streamline the approval process as well as ensure that remediation plans are incorporated into the various Change Models.

As the organization develops related process areas, Change Management can expand policy to identify lifecycle control points that satisfy project, transition and release management requirements for various changes.

This can improve consistency of service transition activity while providing flexibility for various requirements through tailored processes and procedures. These procedures, including an increasing library of tested Change Models, provide a foundation for automated actions as process interfaces are more fully understood.

**Service Asset & Configuration Management**, while a critical ITSM process, will require time to develop. In fact, within each technical domain there is a reasonable level of configuration management activity taking place and staff are very aware of the benefits (and pitfalls) of configuration management.

Most dependency data that is missing is high-level, cross-domain dependency information associated with end-to-end services. This is (more often than not) associated with customer-facing services. CIT should take steps to capture this high-level dependency information and establish logical models of the service infrastructure starting with the most critical services.

As these logical models are established, the specific Configuration Items (CI) associated with each service should be identified along with where the CI attribute information is stored.
With Managed Desktop Services a key CIT initiative a review of Asset Management policies and procedures, including software assets, should be conducted. The location and use of secure libraries and secure stores should be identified.

The shift away from dedicated QA and transition resources, and adjustments to the project management methods within CIT may make future transition activities more inconsistent and unreliable. Efforts should be made to clarify Transition Policies in conjunction with Project Management, Change Management and Release Management.

The Change Management, **Transition Planning & Support** and Release Management policies must allow for tailoring in much the same way that project management tailors methods for small, medium and large projects. In fact, greater integration between the Project Management Life Cycle (PMLC) and the Service Lifecycle is highly desirable.

The Service Lifecycle and Project Management processes can incorporate process models (i.e., Change Models, etc.) and predefined templates to make related artifacts more consistent. There may be opportunities to consolidate artifacts and agree on key base line points based on the models and project tailoring guidelines.

This can provide the basis for the establishment of Lifecycle controls that can help customers and staff understand what is required as project move through the service lifecycle. Monitoring these control points can identify improvement opportunities not always readily apparent from a pure process control perspective.

Recommendations for **Release & Deployment Management** mirror those of Transition Planning & Support.

There are three aspects of **Event Management**  1) Detecting Events, 2) Making sense of Events, and 3) Taking the appropriate control action.

CIT’s technical domains seem to do a reasonable job at all three, which are performed to varying degrees and with toolsets (monitors) tuned to domain-specific needs. However, service infrastructures increasingly span multiple technical domains that can complicate ‘making sense of events’ beyond the capability of any single individual (or even a room full of experts).

CIT seems to recognize this, and roles have been piloted to accelerate the capture of end-to-end dependency data. Past efforts have included attempts at automating discovery development of a real time CMIS (Capacity management Information System).
Nowhere will this be more important than in the Virtual Hosted Services area, a key initiative of the CIT. The need to establish end-to-end service views is shared by other ITSM process areas as well:

- Financial Management, to prepare accurate cost models for services
- Service Level Management, to understand end-to-end requirements
- Service Asset & Configuration Management, to establish logical models of the service infrastructure

CIT should continue these efforts, perhaps combining them with other activities in progress such as Continuity efforts (BIA, etc.), Service Level Requirement (SLR) definition and Availability Management.

In addition, greater integration between the Event Management process and Incident Management is needed. The understanding of Events, both as they unfold and after action is taken, is an opportunity to raise the level of expertise of Level 1 staff. Building and validating a knowledge base that can be used in the Service Desk is a shared responsibility between the Service Desk and Level 2/3 support staff, and event management intelligence can help facilitate collaborative management.

For this reason, the organization should evaluate correlation technologies that can make sense of cross-domain events, particularly in virtual environments.

The Service Desk is the ‘face of IT’ and is highly dependent on the Incident and Request Fulfillment processes. CIT’s Incident Management process is significantly constrained due to fragmentation across multiple business units, multiple diverse tools in use, and the use of temporary staff.

This exacerbates the perception of CIT as ‘not having the ability to deliver quality, reliable services’\(^2\). CIT should take steps to increase the number of full time, professional staff on the Help (Service) Desk.

Less clear is the degree to which consolidation of various Help Desks would be beneficial, however significant duplication of effort exists. There needs to be a discussion about the scope of a University-wide Incident Management process and the appropriate structure of the Service Desk based on real customer requirements and cost constraints.

\(^2\) Report of the Ad Hoc Review Committee for IT@Cornell
Cornell should implement a formal Incident Management process across the University, perhaps starting with CIT but expanding its scope to other units as defined and agreed during the scoping and chartering of the process.

Steps should be taken as soon as possible to compile a resolution and/or knowledge base for use by front line staff in Incident handling. Requests should be separately categorized from Incidents in areas where this is not already occurring, and volume data for both Incidents and Requests should be compiled. Self-service capabilities that exist should be leveraged if possible.

Most business units have established procedures (Request Models) to handle Request Fulfillment, although they are documented in different ways and maintained to varying degrees on different systems. Capturing and cataloging these Request Models is recommended.

As the structure for the Service Desk is understood and evolves, it will be important that these procedures (Request Models) are validated, maintained and communicated to the Service Desks that will require them. Boundaries for those business units that have isolated fulfillment processes and procedures will need to be understood and defined.

The timeframes for handling requests should be reviewed by Service Level Management and agree by all stakeholders in order to set proper expectations with customers and users.

An important element of Problem Management is both its separation from, and relationship with, Incident Management. Performing root-cause analysis after a Major Incident is not the objective of the process; it is preventing Incidents in the first place (or reducing their impact).

Level 2/3 staff should be encouraged to provide workarounds for Level 1 staff, to minimize the impact of Incidents to users and reduce the number of escalations to Level 2/3 staff.

Correctly identifying Problems (the unknown cause of one or more Incidents) and establishing a log of the ‘top 10’ is one way to highlight the need for Problem Management resources to be assigned. These teams should include informal benefit statements in problem resolution data to help justify the commitment to the process.

The Service Level Management process should ensure integration between the Service Improvement Plan (SIP) procedures and the Problem Management process when needed.
PER PROCESS FINDINGS

SERVICE STRATEGY

SERVICE PORTFOLIO MANAGEMENT

PROCESS PURPOSE

Service Portfolio Management is the process for managing the value of services in the pipeline (under development), in production and the services being retired. It analyzes the value to the business of each service and aligns the investment into the service according to business priorities.

EXPECTED OUTCOMES

As a result of successful implementation of the Service Portfolio Management process:

1. The strategic intent of the service provider is crafted;
2. The service investments are analyzed and authorized in accordance with the service provider’s strategic intent;
3. The service portfolio is defined and regularly refreshed to take into account the market and regulatory changes;
4. The service portfolio is approved and the service portfolio related decisions are promoted to Service Design (and to other service life-cycle phases).

FINDINGS

The process is at level 0. Process activities are not performed significantly. Overall, the process does not achieve its purpose and outcomes.
The consolidation of assessment interviews results in the following profile:

### Process Profile

#### Portfolio Management

<table>
<thead>
<tr>
<th>Level 1: Performed</th>
<th>Level 2: Managed</th>
<th>Level 3: Established</th>
<th>Level 4: Predictable</th>
<th>Level 5: Optimizing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessed</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>N.A.</td>
</tr>
<tr>
<td>Target</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>N.A.</td>
</tr>
<tr>
<td>Rating scale</td>
<td>Fully</td>
<td>Largely</td>
<td>Partially</td>
<td>Not</td>
</tr>
</tbody>
</table>

#### Results Analysis

Portfolio management where performed, is based on projects and not services. While there is information indicating strategic intent, investments are not analyzed in terms of services. Defining IT services that are relevant to the business continues to be challenging.

There was no evidence of investments categorized into strategic categories (i.e., Run the Business, Grow the Business, Transform the Business). Investments are project oriented and no evidence of value-to-cost ratio of services was observed.

Communication regarding service portfolio decisions, particularly with regard to promoting these decisions to Service Design and other Lifecycle stages, is not in evidence.
In this section, we measure the extent to which the process is performed, achieves its purpose, and produces its outcomes.

The process is not performed.

The following practices have been reviewed during assessment interviews:

SPM.BP1 - Identify long-term goals of the service organization.

Identify the long-term goals of the service organization. [ITIL v3 - Service Strategy: p126] [Expected Result 1]

*Discussions are held regarding where they need to be (i.e., next year), but the strategic plan is still under development. Long-term goals are being developed over a 3-5 year timeline working with (Bain).*

SPM.BP2 - Determine relevant IT services.

Determine what IT services are required to meet the long-term goals of the service organization. [ITIL v3 - Service Strategy: p126] [Expected Result 1]

*Services have not yet been reviewed in the context of long-term strategy, with some possible exceptions at a technology level (i.e., virtualization, managed desktop, etc.)*

SPM.BP3 - Document a strategic plan.

Document how the service organization will achieve those services by taking into account the capabilities and resources required for them. [ITIL v3 - Service Strategy: p126] [Expected Result 1]

*While there is project portfolio management taking place, there is limited ability to obtain a 'roll-up' view of demand for IT resources and capabilities. This is currently limited to larger projects only, rather than an entire portfolio (and not of services).*

SPM.BP4 - Split investments into strategic categories.

Split IT investments between three strategic categories:

- Run the Business investments are centered on maintaining service operations
- Grow the Business investments are intended to grow the organization's scope of service
- Transform the Business investments are moves into new market spaces
- [ITIL v3 - Service Strategy: p127]

*There was no evidence of investments categorized into strategic categories (i.e., Run the Business, Grow the Business, Transform the Business). Investments are project oriented and no evidence of value-to-cost ratio of services was observed.*

SPM.BP5 - Divide strategic categories into budget allocations.

Divide strategic categories into budget allocations, for example: Venture, Growth, Discretionary, Non-discretionary, Core. [ITIL v3 - Service Strategy: p127] [Expected Result 2]

- Venture: create services in a new market space
- Growth: create new services in existing market space
- Discretionary: provide enhancement to existing services
- Non-discretionary: maintain existing services
- Core: maintain business critical services

[ITIL v3 - Service Strategy: p127]

*The organization is re-evaluating categories such as Systems Enhancement, Support, Rebuild, etc. at this time.*

SPM.BP6 - Authorize service investments.

Determine the value-to-cost ratio of services and consider other relevant factors (mission imperatives, compliance, trends, social responsibilities, innovation, ...) to authorize (or not) service investments. [ITIL v3 - Service Strategy: p128] [Expected Result 2]

*This is mostly limited to larger projects via a business case.*
SPM.BP7 - Make inventory of services.

Collect information from all existing services as well as every proposed new service in order to document what service provider is able to do. [ITIL v3 - Service Strategy: p125] [Expected Result 3]

NOTE: A Service portfolio should include the service pipeline, the service catalogue and the retired services.

[ITIL v3 - Service Strategy: p251]

*There is a catalog of services that is being re-evaluated, but it is unclear to what degree this can be effectively used for strategic decision making.*

SPM.BP8 - Document a business case for each service.

Document a model of what each service is expected to achieve in order to enable the service provider to assess its services in terms of potential benefits and the resources required to provision and maintain it. [ITIL v3 - Service Strategy: p125] [Expected Result 3]

*Business case data, when available, is not based on end-to-end services and may not clearly establish the value of the service in customer terms.*

SPM.BP9 - Make decision on the future of existing services.

Approve the future state of the existing services in accordance with the strategic plan. [ITIL v3 - Service Strategy: p128] [Expected Result 4]

The future state for existing services fall into six categories:

- Retain
- Replace
- Rationalize
- Refactor
- Renew
- Retire

[ITIL v3 - Service Strategy: p128]

*Service Owners may make a case for retirement of services, but most decisions may not incorporate formal analysis (option space tools, etc.) due to a lack of enabling information.*

SPM.BP10 - Allocate resources for service investments.

Allocate resources to make effective the authorized service investments and the decisions on the future of existing services. [ITIL v3 - Service Strategy: p128] [Outcome 4] [Expected Result 4]

*While they do consider operational requirements, Total Cost of Ownership (TCO) and similar analysis is not performed.*

SPM.BP11 - Communicate the service portfolio and related decisions.

Promote the service portfolio content, future of existing services and service investment decisions in order to establish a common vision of the current and future service provider’s activities. [ITIL v3 - Service Strategy: p128] [Expected Result 4]

*Communication regarding service portfolio decisions, particularly with regard to promoting these decisions to Service Design and other Lifecycle stages, is not in evidence.*

SPM.BP12 - Refresh service portfolio.

Monitor, measure, reassess and rebalance the investments based on changing conditions, markets and business needs. [ITIL v3 - Service Strategy: p129] [Expected Result 3]

*Adjustments to the portfolio tend to be reactive and based on projects.*
PROCESS INPUTS & OUTPUTS

The following lists standard process inputs and outputs and indicates whether or not they exist and in which form in the assessed organizational unit.

INPUTS

Key inputs such as service-oriented financial information, customer business plans, service investment analysis and Total Cost of Utilization (TCU) were not identified in the organization.

OUTPUTS

While a portfolio of services existed, it tends to favor supporting services and applications rather than end-to-end services in support of identified business processes. Additional outputs including service investment analysis were not observed.
SWOT ANALYSIS

STRENGTHS

The analysis of assessment results resulted in the identification of the following main strengths:

Stakeholders indicated that some project portfolio management was taking place, so there is an awareness of portfolio management principles in the organization. In addition, the Application Streamlining initiative is using portfolio management techniques from an application perspective.

WEAKNESSES

The analysis of assessment results resulted in the identification of the following main weaknesses:

The primary weakness is generally poor awareness of business processes, how they serve external customers and what IT services underpin them. Service definition continues to be a challenge, particularly External/Internal Customer-Facing services.

OPPORTUNITIES

The analysis of assessment results resulted in the identification of the following main opportunities:

There are two strategic IT initiatives that may be leveraged in support of advancing the process, the re-development of Cornell’s Service Catalog and the Application Streamlining initiative.

THREATS

The analysis of assessment results resulted in the identification of the following main threats:

A driving force for the Service Catalog initiative is the desire to benchmark IT services with other institutions. While this may map well to supporting IT services, it may not map well to other (External/Internal Customer Facing) services.
RECOMMENDATIONS

Service Portfolio Management was the only process in scope whose primary activities take place at the strategic stage of the Service Lifecycle. Related processes such as Business Relationship Management, Strategy Generation for Services, Financial Management and Demand Management were not in scope.

The pending Vision & Strategy Workshop will help clarify Cornell’s internal/external environment, constraints and SWOT (Strengths, Weaknesses, Opportunities and Threats). Based on the initial context/discovery process and the assessment findings, there are some clear market spaces that have been identified:

- Managed Desktop Services
- Virtualized Hosted Infrastructure Services
- ‘Core’ Application Services

In order for Service Portfolio Management to manage the portfolio for maximum value and minimum risk, an understanding of how customers within each market space define value is essential.

The Application Streamlining initiative presents an opportunity to build a portfolio of applications, as well as help validate the customer portfolio. When we begin to codify customer outcomes as well (even without formal SLAs), we have a basis for performing basic portfolio management as services become more defined.

Management of strategic change can be facilitated as decision points appropriate to the organization (Define, Analyze, Approve, Charter) are agreed. This also will help fine-tune cost models associated with services over time.
At the end of the assessment, we have identified the following recommendations:

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPM.1</td>
<td>Create an Application Portfolio</td>
<td>Applications are not the same as services, and the Application Portfolio should be clearly distinguished from the Service Portfolio. A single application may enable multiple applications, and a service may be only one of many application outputs. Applications in the Application Portfolio should be linked to services in the Service Portfolio. Nothing should be in the Application Portfolio without first going through the Service Portfolio Management process.</td>
</tr>
<tr>
<td>SPM.2</td>
<td>Create a Customer Portfolio</td>
<td>The customer portfolio is a database or structured document used to record all customers of the IT service provider. The customer portfolio is the business relationship manager’s view of the customers who receive services from the IT service provider. Service portfolio management uses the customer portfolio to ensure that the relationship between business outcomes, customers and services is well understood. The service portfolio documents these linkages and is validated with customers through business relationship management.</td>
</tr>
<tr>
<td>SPM.3</td>
<td>Create a Customer Agreement Portfolio</td>
<td>Until formal SLAs can be created, document and link customer expectations to the services provided and obtain customer agreement.</td>
</tr>
<tr>
<td>SPM.4</td>
<td>Map to Service Portfolio</td>
<td>Link the Application, Customer and Agreement Portfolios to the Service Portfolio.</td>
</tr>
<tr>
<td>SPM.5</td>
<td>Identify strategic change baseline points</td>
<td>Identify the basic phases of Portfolio Management (Define, Analyze, Approve, Charter) within the organization and establish key process inputs to facilitate further improvement.</td>
</tr>
<tr>
<td>SPM.6</td>
<td>Establish Cost Models for Services</td>
<td>As part of the Service Catalog initiative, begin creating standard Service Cost Models suitable for the organization.</td>
</tr>
</tbody>
</table>
SERVICE DESIGN

SERVICE CATALOG MANAGEMENT

PROCESS PURPOSE

The purpose of the Service Catalogue Management process is to provide a single source of consistent information on all agreed services that is widely available to those who are approved to access it.

Service Catalog Management is the process of publishing and maintaining a description of the services that are in production or readily available. The Service Catalog can help set expectations without the rigor of a formal Service Level Agreement (SLA) and can clarify how the business should interact with IT.

EXPECTED OUTCOMES

As a result of successful implementation of the Service Catalogue Management process:

1. Service Catalogue management policies and principles are developed;
2. NOTE: A unique policy can be developed for both the Service Portfolio and Service Catalogue.
3. Each service (being run or being prepared to run in the live environment) is described in detail and recorded in the Service Catalogue;
4. A Service Catalogue, including the business and the technical service catalogues, is produced, agreed and maintained;
5. The Service Catalogue and its content are available to those who need it.
FINDINGS

The process reaches level 1. Process activities are performed. The process achieves its purpose but in a non-repeatable way and with few controls. During each instance, the process is not implemented in a managed fashion (planned, monitored, and adjusted). Work Products are not appropriately established, controlled, and maintained. Moreover, the way the process is managed is not uniform throughout the organization.

The significant efforts being made at establishing a catalog of services tends to focus on catalog content and structure, rather than on customers and markets for services. While most of the activities are performed (see Results Analysis), weaknesses in Service Portfolio and Service Level Management may be hampering service definition.

PROCESS PROFILE

The consolidation of assessment interviews results in the following profile:
LEVEL 1

In this section, we measure the extent to which the process is performed, achieves its purpose, and produces its outcomes.

The process is largely performed.

The following practices have been reviewed during assessment interviews:

SCM.BP1 - Document and agree a service definition.

Document and agree a service definition with all relevant parties to ensure a common understanding of what is a service within the service provider organization. [ITIL v3 - Service Design: p63] [Expected Result 1]

*Cornell has promoted the ITIL definition of a service however there may not be a clear consensus within IT@Cornell. This may inhibit the establishment of effective policies and principles surrounding both Service Catalog and Service Portfolio Management.*

SCM.BP2 - Define service hierarchy.

Define the service hierarchy used to represent the relationships (i.e. dependencies) between all the IT services and supporting services. [ITIL v3 - Service Design: p62] [Expected Result 1]

For example:

- supporting services: infrastructure/network/application services
- shared services
- commodity services

*The use of the terms ‘supporting services’ has not been established. Use of the term ‘shared service’ is well established; the term ‘commodity service’ is in use but may be limited to applications.*

*We did not observe service dependency data being recorded or maintained between IT and supporting services.*
SCM.BP3 - Define service details and statuses to be recorded.

Define details of each IT service that will be recorded in the service catalogue and the different statuses for a service. [ITIL v3 - Service Design: p61] [Expected Result 1]

NOTE: A balance is necessary between too detailed information to maintain accurately and information at a too high level to be of any value.

*The Catalog has reasonable details about services, including status information. Status information in the catalog may be too detailed.*

SCM.BP4 - Collect services information.

Collect information from service portfolio management, service level management and the business in order to populate the service catalogue. [ITIL v3 - Service Design: p63, p64] [Expected Result 2]

*Data is collected from the business however there is little to no information being collected from either Service Portfolio Management or Service Level Management.*

SCM.BP5 - Describe and record all services in the Service Catalogue.

Record the descriptions of services being run or being prepared to run in the live environment, with their default service level and their relationships, in the Service Catalogue. [ITIL v3 - Service Design: p64] [Expected Result 2, 3]

NOTE: The relationships should be:

- to the business units and business processes that rely on the IT services for the Business Service Catalogue
- to the supporting services, technical components and CIs necessary to the provision of the service for the Technical Service Catalogue

*There is information about future and retired services in the Catalog. Service Levels and business process dependency information was largely absent, although there was information about technical dependencies for certain services.*
SCM.BP6 - Agree the Service Catalogue.

Agree the service catalogue and its content, in conjunction with the service portfolio management. [ITIL v3 - Service Design: p63] [Expected Result 3]

*The pending re-design of the Catalog is being driven by a desire to benchmark the costs of services with other institutions; it is not clear to what degree contents are agreed and portfolio management weaknesses may be a contributing factor.*

SCM.BP7 - Maintain the Business Service Catalogue.

Maintain the business service catalogue regularly, in conjunction with service level management, to ensure that the information contained in the business service catalogue is aligned to the business and the business processes. [ITIL v3 - Service Design: p63] [Expected Result 3]

*The Catalog is regularly maintained, however not in conjunction with Service Level Management and not in alignment with business processes.*

SCM.BP8 - Maintain the Technical Service Catalogue.

Maintain the technical service catalogue regularly, in conjunction with change management and service asset and configuration management, to ensure that the information contained in the technical service catalogue is align to the supporting services, technical components and CIs [ITIL v3 - Service Design: p63] [Expected Result 3]

*Change Management is involved in the maintenance of the Catalog, however Service Asset & Configuration Management is fragmented. Combined with low levels of service dependency information, the Catalog is maintained from a cosmetic rather than from a dependency perspective.*

SCM.BP9 - Make available the Service Catalogue.

Make the service catalogue, and its content, available all the time to all relevant parties: customer, Service Level Management, support teams, suppliers, ... [ITIL v3 - Service Design: p] [Expected Result 4]

*The Catalog is generally available to all relevant stakeholders, however Service Level Management is not established.*
PROCESS INPUTS & OUTPUTS

The following table lists standard process inputs and outputs and indicates whether or not they exist and in which form in the assessed organizational unit.

<table>
<thead>
<tr>
<th>INPUTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key inputs to the process were not in evidence, including:</td>
</tr>
<tr>
<td>- Service Portfolio</td>
</tr>
<tr>
<td>- Configuration Management System (CMS)</td>
</tr>
<tr>
<td>- Supplier and Contract Database (SCD)</td>
</tr>
<tr>
<td>- Service Reports</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OUTPUTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>The following Work Products were in evidence, however in some cases were not controlled or were fragmented:</td>
</tr>
<tr>
<td>- Service Definition documentation</td>
</tr>
<tr>
<td>- Service Catalog communication plan</td>
</tr>
</tbody>
</table>
**LEVEL 2 – PERFORMANCE MANAGEMENT**

Process performance is **not** managed.

In this section, we measure the extent to which process performance is planned and managed within time and resource constraints. We assess whether the following points are covered:

a) Objectives for the performance of the process are identified.
b) The performance of the process is planned and monitored.
c) The performance of the process is adjusted to meet plans.
d) Responsibilities and authorities for performing the process are defined, assigned, and communicated.
e) The resources and information necessary for performing the process are identified, made available, allocated, and used.
f) Interfaces between the involved parties are managed to ensure both effective communication and clear assignment of responsibility.

**The Assessment Team collected the following findings:**

The key elements inhibiting effective performance management are a lack of supporting processes and roles, specifically Service Portfolio and Service Level Management.

**LEVEL 2 – WORK PRODUCT MANAGEMENT**

Work Products (process inputs and outputs) are **not** managed.

In this section, we measure the extent to which the Work Products produced by the process are appropriately managed. We assess whether the following points are covered:

a) Requirements for the Work Products of the process are defined.
b) Requirements for documentation and control of the Work Products are defined.
c) Work Products are appropriately identified, documented, and controlled.
d) Work Products are reviewed in accordance with planned arrangements and adjusted as necessary to meet requirements.

**The Assessment Team collected the following findings:**

While there were some templates in use, the process was not formally documented and some key Work Products (inputs/outputs) were not defined. Where process Work Products were established, reviews and controls were largely ad hoc.
SWOT ANALYSIS

STRENGTHS

The analysis of assessment results resulted in the identification of the following main strengths:

There is a high level of awareness of the importance of the Service Catalog at an organizational level.

WEAKNESSES

The analysis of assessment results resulted in the identification of the following main weaknesses:

The absence of Service Portfolio and Service Level Management inhibits effective Service Catalog Management.

OPPORTUNITIES

The analysis of assessment results resulted in the identification of the following main opportunities:

The desire to benchmark IT service costs with other institutions is forcing a re-design of the Service Catalog, providing an opportunity to redefine IT services and supporting process interfaces with Service Catalog Management.

THREATS

The analysis of assessment results resulted in the identification of the following main threats:

While supporting services may be well aligned with other institutions, customer-facing service may not be. Adoption of ‘standard’ supporting services may actually complicate business alignment.
RECOMMENDATIONS

With a revision to the existing Service Catalog already planned Cornell should take the time now to refresh the definition of Services to incorporate the new 2011 ITIL guidance, which identifies:

- **Customer-facing services** - IT services that are seen by the customer. These are typically services that support the customer’s business units/business processes, directly facilitating some outcome or outcomes desired by the customer.

- **Supporting services** - IT services that support or ‘underpin’ the customer-facing services. These are typically invisible to the customer, but essential to the delivery of customer-facing IT services.

Review the current structure and taxonomy of services with the proposed structure that will facilitate benchmarking of service costs with other institutions. Ensure that the new structure will allow alignment with Cornell’s customers, particularly for customer-facing services.

Agree on a standard Catalog Entry wherever possible to improve administration, make the catalog easier to use, and make sure that all services have the minimal information needed for customers and users. The Service Catalog is a marketing document and often the first place IT has to set expectations for services.

For this reason, interfaces with Service Portfolio Management and Service Level Management are essential, and the stakeholders involved in these processes (as well as Business Relationship Management) should participate in the design of the Service Catalog.

At the end of the assessment, we have identified the following recommendations:
<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCM.1</td>
<td>Update the definition of Service</td>
<td>Refresh the definition of a Service to include the new guidance relating to Supporting, Internal Customer-Facing and External Customer-Facing Services. Include this definition in all future training.</td>
</tr>
<tr>
<td>SCM.2</td>
<td>Agree on Service Taxonomy</td>
<td>Establish a hierarchy/taxonomy of services that is appropriate for the organization and agreed by key stakeholders.</td>
</tr>
<tr>
<td>SCM.3</td>
<td>Agree on standard Catalog Entries</td>
<td>Create a standard template for entries into the Service Catalog, and place this Work Product under document and process control.</td>
</tr>
<tr>
<td>SCM.4</td>
<td>Re-architect the Catalog</td>
<td>As part of the Service Catalog initiative, leverage the mapping of Application and Customer Portfolio information to rationalize the Service Portfolio and Service Catalog based on:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Supporting Service requirements and consistency with benchmarking partners</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Internal Customer-Facing Services and consistency with Internal Customers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• External Customer-Facing Services and consistency with these customers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This may identify Service Improvement Plans (SIP) that can differentiate services for specific customer segments. These SIPs would be prioritized by the Service Portfolio Management process.</td>
</tr>
<tr>
<td>SCM.5</td>
<td>Bridge SCM with SPM and SLM</td>
<td>Identify key process interfaces with Service Portfolio Management and Service Level Management. Include Business Relationship Management if possible as well.</td>
</tr>
</tbody>
</table>
SERVICE LEVEL MANAGEMENT

PROCESS PURPOSE

The purpose of the Service Level Management process is to ensure that an agreed level of IT services is provided for all current IT services, and that futures services are delivered to agreed achievable targets.

Service Level Management is the process of negotiating, documenting and agreeing on appropriate IT service targets with representatives of the business, and then monitoring and reporting on the service provider’s ability to deliver the agreed level of service.

EXPECTED OUTCOMES

As a result of successful implementation of the Service Level Management process:

1. Requirements for new IT services are defined, maintained and documented in SLRs;
2. The service level of IT services provided is defined and agreed by customers (business);
3. The service level of IT services provided is monitored, reported and reviewed;
4. Internal service levels (OLA) and supplier contracts are defined into line with SLA targets;
5. Customer relationships and satisfaction are developed and improved;
6. Service level breaches are addressed in Service Improvement Plan (SIP).
FINDINGS

The process is at level 0. Process activities are not performed significantly. Overall, the process does not achieve its purpose and outcomes.

While Service Level Management activities are partially performed and some Service Level Agreements (SLAs) are established, there are major weaknesses in key attributes and critical Work Products are absent.

PROCESS PROFILE

The consolidation of assessment interviews results in the following profile:
RESULTS ANALYSIS

LEVEL 1

In this section, we measure the extent to which the process is performed, achieves its purpose, and produces its outcomes.

The process is not performed.

The following practices have been reviewed during assessment interviews:

SLM.BP1 - Identify requirements for IT services.

Identify requirements for existing IT services and for new services being developed. [ITIL v3 - Service Design: p69] [Expected Result 1]

*Service levels are not defined in a systematic way. While there may be project artifacts that document requirements we did not observe a standard Service Level Requirements document. Variations in documenting requirements exist.*

SLM.BP2 - Consult other ITSM processes for defining realistic targets.

Consult others ITSM processes in order to define realistic service level targets that can be effectively achieved. [ITIL v3 - Service Design: p70] [Expected Result 1]

    NOTE: The main processes to be consulted are: incident, capacity and availability management.

*Most process interfaces are ad hoc and not well established. Service Owners drive the setting of service level targets.*

SLM.BP3 - Establish and maintain monitoring capabilities.

Establish, review and update service levels monitoring capabilities. [ITIL v3 - Service Design: p70] [Expected Result 3]

    NOTE: It is essential that monitoring matches the customer's true perception of the service but it is often very difficult to achieve.
Targets are often a reflection of what they should measure but do not reflect what can be measured. Where formal Service Level Agreements exist, it is not clear that the organization can effectively monitor, report and review on these measurements.

SLM.BP4 - Define, negotiate and agree SLAs.

Document IT service levels in a draft SLA, and based on it, negotiate and agree service levels with customers. [ITIL v3 - Service Design: p69, p67, p68] [Expected Result 2, 5]

NOTE: SLA should also identify relationships and contacts between the service provider, the customer and the other stakeholders.

It is not known how many SLAs or customers there are. No formal policy on SLA reviews was observed however there were template SLAs in evidence.

SLM.BP5 - Measure service performance against SLA targets.

Measure service performance against SLA targets [ITIL v3 - Service Design: p71] [Expected Result 3, 6]

There is no consistency in the way Service Levels are measured and reported. Dashboards exist, but may be isolated. Little information on related ITSM processes is collected and used as part of service reporting.

SLM.BP6 - Provide service reporting to customer.

Provide service reporting to customer, based on agreed service report and intervals, to demonstrate service achievement against SLA targets. [ITIL v3 - Service Design: p73] [Expected Result 3,5]

Service reporting is inconsistent and driven independently by Service Owners.

SLM.BP7 - Review SLA with customer.

Review SLA contents and targets on a regular basis with customer to keep aligned with business needs [ITIL v3 - Service Design: p74] [Expected Result 3, 5]
NOTE: SLRs should be reviewed in accordance with the SLA reviews.

*Service reporting is inconsistent and driven independently by Service Owners.*

SLM.BP8 - Monitor and improve customer satisfaction.

Monitor customer perception on service delivery and take it into account in the SLA reviews and the Service Improvement Plan (SIP). [ITIL v3 - Service Design: p72] [Expected Result 3, 5]

*While there are customer satisfaction surveys conducted, they are not driven by Service Level Management and not tied to SLA achievements.*

SLM.BP9 - Define and maintain internal service levels and supplier contracts.

Define and maintain Operational Level Agreements (OLA) with internal units and supplier contracts with external suppliers, in order to underpin the existing SLA targets. [ITIL v3 - Service Design: p73] [Expected Result 4]

*Templates for Operational Level Agreements (OLAs) exist, but OLAs are in very limited use, if at all. The definition and maintenance of internal service levels and contracts is informal and ad hoc. OLAs are not maintained on a regular basis.*

SLM.BP10 - Record and manage complaints and compliments.

Record all complaints and compliments and communicate them to the relevant parties for actions and resolution [ITIL v3 - Service Design: p75] [Expected Result 5, 6]

*The handling of compliments and complaints is fragmented across Remedy (Help Desk), e-mail and Account Management. This sometimes results in a ‘loudest voice’ approach to complaints.*

SLM.BP11 - Address service level breaches in SIP.

Identify and prioritize improvement actions, in order to avoid recurrence of service level breaches, into the Service Improvement plan (SIP). [ITIL v3 - Service Design: p73] [Expected Result 6]
There is no formal policy for initiating Service Improvement Plans (SIP) and in fact there may not be management support for doing so. Prioritizing service improvements remains ad hoc.
PROCESS INPUTS & OUTPUTS

**INPUTS**

Service Level Requirements (SLR) are not in evidence and may not be in use, even when project requirements are identified. Other process Work Products such as OLAs and Contracts exist but are not well managed or not in use.

**OUTPUTS**

Updated SLRs not an output; Service Reports, Service Improvement Plans (SIP) are not in evidence.

SWOT ANALYSIS

**STRENGTHS**

The analysis of assessment results resulted in the identification of the following main strengths:

Templates exist for SLAs and OLAs. Some services have SLAs defined.

**WEAKNESSES**

The analysis of assessment results resulted in the identification of the following main weaknesses:

Lack of Service Level Requirements (SLR) and Service Improvement Plans (SIP) and related policies are major weaknesses.

No Service Level Manager role is defined.

**OPPORTUNITIES**

The analysis of assessment results resulted in the identification of the following main opportunities:

The desire to re-structure the Service Catalog and baseline service costs may present an opportunity to introduce formal Service Level Management.

**THREATS**

The analysis of assessment results resulted in the identification of the following main threats:

The performance of existing services may not be well known or understood, resulting in a poor understanding of customer perceptions.
RECOMMENDATIONS

Development of Service Level Agreements without formal Service Level Management may be contributing to the negative perception of CIT having an internal focus and lack of service orientation.

The responsibilities for Service Level Management seem to fall on the Service Owners (who are sometimes managers of technical domains). A focus on customers is a secondary responsibility for Service Owners, and their primary technical focus may be re-enforcing traditional perceptions of CIT.

The Service Level Manager is also tasked with gathering service level requirements (SLR); a critical input that was not in evidence in the assessment. In fact, for customer-facing services these tasks may be outside of CIT, which only increases the distance between the organization and its customers.

As new services provided by CIT are defined and designed, it is essential that more emphasis on understanding the utility and warranty requirements of various customer segments be achieved. Placing this entire burden on the Service Owner (who for some services may actually be a Product Line Manager) can result in service offerings not adequately differentiated for critical customer segments.

The codification of desired customer outcomes (utility & warranty) does not imply that formal SLAs must be developed, but there must be some agreement on expectations (SLR) even if in an informal format.

The resulting information will enable the establishment of SLA structures (when the organization/service is ready for an SLA) and base lining current levels of service performance in the meantime.

Finally, there must be a mechanism for Service Improvement Plans (SIP) in order to foster continual improvement. The Service Portfolio Management process should review and approve the SIPs based on business priorities and available resources.

At the end of the assessment, we have identified the following recommendations:
<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SLM.1</td>
<td>Identify SLM Roles &amp; Responsibilities</td>
<td>Establish roles and responsibilities for SLM as it applies to Supporting, Internal Customer-Facing and External Customer-Facing Services.</td>
</tr>
<tr>
<td>SLM.2</td>
<td>Participate in Catalog Development</td>
<td>Have Service Level Managers assist with the re-design of the Service Catalog.</td>
</tr>
<tr>
<td>SLM.3</td>
<td>Document Customer Service Level Expectations</td>
<td>Begin documenting Service Level Requirements (SLR).</td>
</tr>
<tr>
<td>SLM.4</td>
<td>Agree on an SLA Structure</td>
<td>Establish a structure for Service Level Agreements based on predefined templates that minimizes administrative overhead and simplifies negotiation.</td>
</tr>
<tr>
<td>SLM.5</td>
<td>Baseline Service Levels</td>
<td>Based on current monitoring capabilities, begin baselining current service levels.</td>
</tr>
<tr>
<td>SLM.6</td>
<td>Establish a procedure for Service Improvement Plans (SIP)</td>
<td>Ensure that all Service Level Managers and Customers understand the need for regular reporting and review. Agree on procedures for addressing Service Improvements, both for new/changed requirements and service level breach.</td>
</tr>
</tbody>
</table>
AVAILABILITY MANAGEMENT

PROCESS PURPOSE

The purpose of the availability management process is to ensure that the level of service availability delivered in all services is matched to (or exceeds) the current and future agreed needs of the business, in a cost effective manner.

The availability management process does not include Business Continuity Management and the resumption of business processing after a major disaster. The support of BCM is included within IT Service Continuity Management.

IT Service Continuity Management and Availability Management have a close relationship, particularly in the management of risks and in the implementation of risk reduction and resilience measures.

EXPECTED OUTCOMES

As a result of successful implementation of the Availability Management process:

1. The current and future service availability requirements are identified and addressed;
2. An appropriate availability plan is produced, maintained, reviewed annually, and executed as required;
3. Performance and availability of all services and resources are monitored against agreed targets and reported;
4. Unavailability-related events are investigated and corrected;
5. Advice and guidance on availability and performance issues are provided to all other business and IT areas.
FINDINGS

The process is at level 0. Process activities are not performed significantly. Overall, the process does not achieve its purpose and outcomes.

Availability Management is largely restricted to technical domains. The process is reactive, fragmented and may be ineffective for Customer-Facing Services.

PROCESS PROFILE

The consolidation of assessment interviews results in the following profile:

![Availability Management Profile](image-url)
RESULTS ANALYSIS

LEVEL 1

In this section, we measure the extent to which the process is performed, achieves its purpose, and produces its outcomes.

The process is partially performed.

The following practices have been reviewed during assessment interviews:

AVA.BP1 - Determine current and future availability requirements.

Identify and document current and future availability requirements based on SLAs and SLRs. [ITIL v3 - Service Design: p102] [Expected Result 1]

*Availability targets are typically dictated by management, rather than by an analysis of SLR/SLA data. Even when formal analysis is performed, it may not include OLA and Contract dependencies.*

AVA.BP2 - Identify Vital Business Functions (VBFs).

Identify and document all business functions that are critical for the business operations of its customers. [ITIL v3 - Service Design: p102] [Expected Result 1]

*There is little to no formal Business Impact Analysis (BIA) performed as part of Availability Management, however Business Continuity efforts may be conducting BIA. Resiliency focus is on technical components rather than vital business functions.*

AVA.BP3 - Develop an availability plan.

Produce an availability plan that enables the service provider to continue to provide service of quality defined in SLAs (current availability requirements) and that covers a sufficient planning timeframe to meet future availability requirements. [ITIL v3 - Service Design: p102] [Expected Result 2]

NOTE: Each improvement should be quantified in terms of resource required, cost, benefits and impact.
Availability Plans, if present, are informal, limited to technical domains and not the result of SLAs.

AVA.BP4 - Maintain the availability plan.
Assess impacts of all changes on the availability plan, update it accordingly, and review completely at least annually the availability plan. [ITIL v3 - Service Design: p102] [Expected Result 2]

There is no proactive availability management undertaken, and no evidence of annual reviews of availability plans.

AVA.BP5 - Negotiate budget for availability plan execution.
During budget accounting cycle, negotiate the budget necessary to be able to put the availability plan into operation during the next periods. [ITIL v3 - Service Design: p112, p124] [Expected Result 2]

Stakeholders felt there was limited financial information to facilitate effective planning of availability; no downtime costs are calculated, etc. Capacity data is domain focused and provides little benefit to planning end-to-end availability requirements.

AVA.BP6 - Test resilient and fail-over components and mechanisms.
Perform tests on resilient and fail-over components and mechanisms at planned intervals to ensure that they will be effective in case of necessity. [ITIL v3 - Service Design: p120, p121] [Expected Result 2]

There is regular testing of failure and resiliency mechanisms.

AVA.BP7 - Define service and resource availability measures and targets.
Document and agree availability measures for all services and critical resources, and define related availability targets. [ITIL v3 - Service Design: p103] [Expected Result 3]

NOTE: The availability measures should be incorporated into SLAs, OLAs and underpinning contracts
While component availability is tracked and monitored, it is not clear if specific targets are established for critical components. No evidence of these being incorporated into SLAs on a regular basis.

AVA.BP8 - Measure service availability from a business perspective.

Measure the availability of IT services in terms of business operations in order to keep aware of the business and customer perception on the service availability. [ITIL v3 - Service Design: p103] [Expected Result 3]

Few end-to-end services are defined, and there is no mapping to business processes. Customer perceptions of availability are not understood in business terms, but focused on individual Incidents.

AVA.BP9 - Measure service availability from an IT component perspective.

Measure the service availability in terms of IT components, in order to both react promptly when unavailability events occur and provide input for service availability improvements. [ITIL v3 - Service Design: p105] [Expected Result 3, 4]

Component availability is actively monitored but not reflected in service availability metrics. The tendency is to increase component availability by adding redundancy, which may actually increase complexity and may not always be the most efficient approach to realizing business availability goals.

AVA.BP10 - Identify, analyze and resolve any unavailability related events.

Identify, investigate and correct unacceptable availability levels that impact or could impact the customers (i.e. SLAs breaches). [ITIL v3 - Service Design: p106] [Expected Result 4]

NOTE: Usually the identification of unavailability events is done by raising an availability exception report from the monitoring activity. The unavailability-related events should be recorded as an incident or a problem and so should be treated through the incident, problem and change management processes.
When significant unavailability occurs, steps are taken to perform root-cause analysis. Some trending analysis takes place, mostly on a domain-specific basis. Lack of Service Level Management tends to make these activities inconsistent and reactive.

AVA.BP11 - Provide advice and guidance on availability and performance issues.

Contribute to SLRs/SLAs definition and change evaluation; perform application sizing and design impact analysis models...[ITIL v3 - Service Design: p97, p106] [Expected Result 5]

The lack of a defined SLM process limits the effective use of service design principles and techniques such as application sizing and impact analysis; there is not always clear SLR data upon which to base design decisions.
PROCESS INPUTS & OUTPUTS

**INPUTS**

Inputs to the process are fragmented across technical domains or not in use. Most inputs are based on components and/or domain-specific information rather than end-to-end IT services:

- Customer business Plan [AVA.BP1, 2] [Expected Result 1]
- Risk analysis report [AVA.BP1, 2] [Expected Result 1]
- Availability Plan [AVA.BP4] [Expected Result 2]
- Availability Management information System (AMIS) [AVA.BP1, 3, 4] [Expected Result 1, 2]
- Availability recovery design criteria, measures, targets and alerts [AVA.BP8] [Expected Result 3]
- Availability exception report
- Forecast and predictive report [AVA.BP4] [Expected Result 2]
- Availability test schedule [AVA.BP6] [Expected Result 2]
- Availability test report [AVA.BP4, 10] [Expected Result 2, 4]

**OUTPUTS**

Similarly, outputs are component and/or domain oriented:

- Availability Management information System (AMIS) [AVA.BP7, 8, 9] [Expected Result 3, 4]
- Availability Plan [AVA.BP1, 3, 4] [Expected Result 1, 2]
- Availability recovery design criteria, measures, targets and alerts [AVA.BP7] [Expected Result 3]
- Availability exception report [AVA.BP8, 9] [Expected Result 3, 4]
- Ad hoc availability and performance report [AVA.BP11] [Expected Result 5]
- Forecast and predictive report [AVA.BP11] [Expected Result 5]
- Availability test schedule [AVA.BP6] [Expected Result 2]
- Availability test report [AVA.BP6] [Expected Result 2]
SWOT ANALYSIS

STRENGTHS

The analysis of assessment results resulted in the identification of the following main strengths:

There are process activities that occur in specific domains that are driven by requirements for high levels of availability (i.e., network, etc.).

WEAKNESSES

The analysis of assessment results resulted in the identification of the following main weaknesses:

The lack of end-to-end dependency data and agreed service levels perpetuates the status quo.

OPPORTUNITIES

The analysis of assessment results resulted in the identification of the following main opportunities:

Some services have clear input from the business regarding the need for high availability, presenting an opportunity to drive business-oriented improvements to availability.

THREATS

The analysis of assessment results resulted in the identification of the following main threats:

Customers may continue to pursue external service provider relationships in pursuit of higher availability, even when they may not be warranted.
**RECOMMENDATIONS**

Investments in availability improvements should follow the identification and agreement of service level requirements (SLR) and a baseline of current availability. There may be opportunities as part of continuity management’s involvement in Business Impact Analysis (BIA) to identify vital business functions that can guide availability planning and reporting.

An Availability Plan template may help technical domains capture base level availability information that may facilitate broader-based availability reporting. In addition, the availability plans can identify measurement gaps in the Availability Management Information System (AMIS).

Reporting on availability to customers should be based on vital business functions and the end-to-end requirements from the customer’s perspective. Where this is not achievable, the Availability Plan should identify the gaps and propose improvements that will be collated, prioritized and analyzed through the Service Portfolio Management and Change Management process.

Availability Management staff should participate (along with other staff such as Capacity Management and Event Management) in Problem resolution activity when required.
At the end of the assessment, we have identified the following recommendations:

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| AVA.1 | Identify Vital Business Functions | Leverage Business Impact Assessment (BIA) activities associated with continuity planning to understand and capture vital business functions for each customer.  
This should be part of Service Level Requirement (SLR) capture. |
| AVA.2 | Begin Availability Planning | Establish a simple template for an Availability Plan that can be used by multiple stakeholders to begin capturing critical availability plan data. |
| AVA.3 | Report on Availability      | Where current monitoring capabilities allow, begin regular reporting on availability. Identify gaps based on critical business drivers and prioritize availability improvement opportunities via SIP and SPM. |
IT SERVICE CONTINUITY MANAGEMENT

PROCESS PURPOSE

The purpose of the IT Service Continuity Management process is to support the overall Business Continuity Management process by ensuring that the required IT technical and service facilities can be resumed within required and agreed business timescales.

EXPECTED OUTCOMES

As a result of successful implementation of the IT Service Continuity Management process:

1. An IT service continuity strategy is defined and implemented in accordance with the business continuity objectives;
2. A set of IT Service Continuity Plans and IT recovery plans is produced, based on the overall Business Continuity Plans, available all the time, maintained, reviewed and executed as required;
3. Continuity tests are performed at planned intervals;
4. Continuity tests failures are investigated and corrected;
5. Advice and guidance on continuity and recovery issues are provided to all other business and IT areas.

FINDINGS

The process is at level 0. Process activities are not performed significantly. Overall, the process does not achieve its purpose and outcomes.

The principal hurdle to achieving the IT Service Continuity Management process purpose and outcomes is a lack of clear required and agreed business timescales for resolution of services, and scope that may be limited principally to the CIT organization.
The consolidation of assessment interviews results in the following profile:

### IT Service Continuity Management

<table>
<thead>
<tr>
<th>Level 1 Performed</th>
<th>Level 2 Managed</th>
<th>Level 3 Established</th>
<th>Level 4 Predictable</th>
<th>Level 5 Optimizing</th>
</tr>
</thead>
</table>

**Assessed**

- P
- N
- N

**Target**

- F
- P
- P

**Rating scale**

- Fully
- Largely
- Partially
- Not
- N.A.

**Legend**

- Level achieved
- Level not achieved
- Not assessed

---

**Edit Note:**

The assessment results are as follows:

- Level 1: Partially achieved
- Level 2: Not achieved
- Level 3: Not assessed
- Level 4: Not assessed
- Level 5: Not assessed

---

**Follow-up:**

A detailed analysis of each component is required to improve the current level of maturity in IT Service Continuity Management.
RESULTS ANALYSIS

LEVEL 1

In this section, we measure the extent to which the process is performed, achieves its purpose, and produces its outcomes.

The process is **partially** performed.

The following practices have been reviewed during assessment interviews:

SCO.BP1 - Identify and agree the scope of the ITSCM process.

Determine and agree the scope of IT service continuity management with the customers into line with its business continuity strategy. [ITIL v3 - Service Design: p128] [Expected Result 1]

*While work is in progress to establish linkages to the business continuity strategy (SAIC, EHS), much of the IT focus is on establishing redundancy rather than continuity. In addition, the scope is focused on CIT and may not adequately encompass other business units.*

SCO.BP2 - Perform Business Impact Analysis and Risks Analysis.

Perform Business impact analysis to prioritize IT service recovery accordingly, and perform risk analysis to define risk reduction measures and continuity (recovery) options. [ITIL v3 - Service Design: p131] [Expected Result 1,2]

NOTE: The priority of IT services recovery can change according to the time of day, day of the week and monthly and annual variations.

NOTE: A balanced approach should be adopted where risk reduction and recovery are complementary and both are required.

*Impact analysis is informal and not well documented. Minimum service levels and/or resource requirements may not be known.*

SCO.BP3 - Implement risk reduction measures.

Implement risk reduction measures resulting from risk analysis in order to reduce continuity risks exposure. [ITIL v3 - Service Design: p133] [Expected Result 1]
NOTE: The risk reduction measures should be instigated in conjunction with availability management as many of these measures also impact the service availability.

*Risk reduction measures are ad hoc and informal.*

SCO.BP4 - Obtain facilities for the provision of the necessary recovery capability.

Implement information backup facilities and negotiate contracts for the provision of the recovery capability necessary to put the IT service continuity strategy into practice. [ITIL v3 - Service Design: p135] [Expected Result 1, 2]

*There are some contracts with external parties (i.e., quick ship agreements, etc.) and standby agreements within campus.*

SCO.BP5 - Develop a set of IT Service Continuity Plans.

Produce IT Service Continuity plans, in line with the Business Continuity Plans and ensuring that the required services, facilities and resources are delivered in a acceptable operational state and are ‘fit for purpose’ when accepted by the business [ITIL v3 - Service Design: p136] [Expected Result 2]

*The continuity plan is fragmented; teams are identified as well as some tasks, elements of the plan are under control, however each group may have different versions of recovery procedures that could result in some inconsistencies.*

SCO.BP6 - Maintain the set of IT Service Continuity Plans.

Review annually the IT Service Continuity Plans and assess impacts of all changes of the IT Service Continuity Plans [ITIL v3 - Service Design: p137] [Expected Result 2]

*Plans are reviewed at least annually. Service Owners are involved in updating service-by-service plans, with links to the EHS master plan; no defined policy for additional reviews to meet specific business unit requirements.*

SCO.BP7 - Manage the distribution of the IT Service Continuity Plans.
Manage the distribution of IT Service Continuity plans to ensure that copies are available to key staff at all times [ITIL v3 - Service Design: p135] [Expected Result 2]

**Key stakeholders have copies of the plan and copies are also maintained off-site.**

SCO.BP8 - Train involved staff.

Train everyone involved in the continuity plans in how to put their assigned tasks into action in case of invocation. [ITIL v3 - Service Design: p137] [Expected Result 2, 3]

**People are aware of their responsibilities, although no formal training has been conducted.**

SCO.BP9 - Perform continuity plans tests.

Define continuity test scenarios and objectives, plan and conduct tests of the IT Service Continuity Plans. [ITIL v3 - Service Design: p137] [Expected Result 3]

**Elements of the plan are tested (selected services and domains), however the overall plan has not been tested.**

SCO.BP10 - Resolve Continuity tests failures.

Investigate the continuity test failures and correct them by instigate remedial action. [ITIL v3 - Service Design: p137] [Expected Result 4]

**These actions tend to be ad hoc and reactionary (i.e., Peoplesoft testing as a result of audit request).**

SCO.BP11 - Provide advice and guidance on continuity and recovery issues.

Contribute to SLRs/SLAs definition and change evaluation; perform application sizing and design impact analysis models...[ITIL v3 - Service Design: p139] [Expected Result 5]

**There is no significant presence of SLR/SLA data for use by the IT Service Continuity process.**
PROCESS INPUTS & OUTPUTS

INPUTS

The key input that was not in evidence was the Service Level Agreement (SLA).

OUTPUTS

The following process outputs were fragmented and/or not in evidence:

- IT service continuity strategy [SCO.BP4, 1, 3] [Expected Result 1, 2]
- Business impact analysis report [SCO.BP2] [Expected Result 1, 2]
- Risk analysis report [SCO.BP2] [Expected Result 1, 2]
- IT service continuity plans [SCO.BP5, 6] [Expected Result 2]
- Continuity test schedule [SCO.BP9] [Expected Result 3]
- Continuity test report [SCO.BP9] [Expected Result 3]
- Service Level Agreement (SLA) [SCO.BP11] [Expected Result 5]
- Ad hoc continuity and recovery report [SCO.BP11] [Expected Result 5]
SWOT ANALYSIS

STRENGTHS

The analysis of assessment results resulted in the identification of the following main strengths:

The business (via EHS) is seems to be more aware of business continuity requirements and driving the evolution of IT Service Continuity Management.

WEAKNESSES

The analysis of assessment results resulted in the identification of the following main weaknesses:

Absence of Service Level Management and its key Work Products (SLR/SLA) is significantly hindering the effectiveness of the IT Service Continuity Management process.

OPPORTUNITIES

The analysis of assessment results resulted in the identification of the following main opportunities:

The Business Continuity Planning activities may present opportunities to drive IT service management process improvement in conjunction with the business.

THREATS

The analysis of assessment results resulted in the identification of the following main threats:

The most significant threat may be that the business seeks to ‘outsource’ key services to remove the burden of in-house continuity demands; this may (or may not) result in more efficient/effective IT service continuity and will require IT guidance and leadership.
Several activities associated with IT Service Continuity Management can be effectively leveraged for IT Service Management adoption, including Business Impact Analysis (BIA) and Risk Management.

The University has a Business Continuity Plan (BCP) initiative underway, which presents an opportunity for IT to develop greater alignment with the business. The BIA activities will identify and quantify the impact to the business of loss of service, thereby providing a documented source of the services most important to the University. Risk Assessment and Management can also help clarify business priorities and tolerance for risk.

These activities enable the mapping of critical elements of the end-to-end service infrastructure and can be leveraged by all ITSM process areas.

The eventual ITSM Road Map should attempt to maximize the work being done in this area; a few examples include:

- Ensuring Service Level Management is involved in BIA activities and analysis.
- Providing Incident and Change Management with Risk Management data for development of a Risk Matrix to focus priority on impact and urgency that are business relevant.
- Use the BIA and Risk data to aid decision making in Service Portfolio Management.

As the business has become more dependent on IT Services, it is essential that IT play an increasing role in the Business Continuity Plan. This may present opportunities for ongoing strategic dialog.
At the end of the assessment, we have identified the following recommendations:

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCO.1</td>
<td>Leverage BIA activities and data</td>
<td>Maximize the efforts with the Business related to BIA activities by including other ITSM process areas, such as Service Level Management and Availability Management.</td>
</tr>
<tr>
<td>SCO.2</td>
<td>Understand Risk tolerance associated with customers</td>
<td>Update University Audit on ITSM plans; evaluate opportunity to create a ‘seat at the IT table’ to improve the management of risk and improve SPM as trade-offs between schedule, quality and cost are considered.</td>
</tr>
<tr>
<td>SCO.3</td>
<td>Re-evaluate Impact &amp; Urgency in light of BIA analysis</td>
<td>Use the BIA data to re-evaluate guidelines for determining business impact and urgency. Use this data, tailored as appropriate for customer segments, when establishing guidelines for setting priority.</td>
</tr>
</tbody>
</table>
The purpose of the Change Management process is to control the life cycle of all changes in such a way as to maximize business value while minimizing IT service disruptions.

As a result of successful implementation of the Change Management process:

1. Changes Management policies and principles are defined
2. Remediation planning is defined and assessed
3. Each change is documented
4. Changes/RFCs are filtered and authorized
5. Changes are implemented
6. Changes are finished
7. Emergency changes are handled.
**FINDINGS**

The process reaches level 1. Process activities are performed. The process achieves its purpose but in a non-repeatable way and with few controls. During each instance, the process is not implemented in a managed fashion (planned, monitored, and adjusted). Work Products are not appropriately established, controlled, and maintained. Moreover, the way the process is managed is not uniform throughout the organization.

The Change Management process is constrained by the absence and management of key Work Products and related process weaknesses in Service Asset & Configuration Management, Transition Planning & Support and Release & Deployment Management.

**PROCESS PROFILE**

The consolidation of assessment interviews results in the following profile:

<table>
<thead>
<tr>
<th>Process</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance</td>
<td>L</td>
<td>L</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Work Product</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process Definition</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process Deployment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process Prevention</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process Control</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process Innovation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process Optimization</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Assessed: L

Target: F


Legend: Level achieved, Level not achieved, Not Assessed.
RESULTS ANALYSIS

LEVEL 1

In this section, we measure the extent to which the process is performed, achieves its purpose, and produces its outcomes.

The process is **largely** performed.

The following practices have been reviewed during assessment interviews:

- CHA.BP1 - Define Change Management policies and principles.
- Define Change Management policies and principles including:
  - the scope of change to services
  - roles and responsibilities
  - procedures
  - change process models
  - emergency/standard changes definition
  - remediation/back-out [ITIL v3 - Service Transition: p45] [Expected Result 1]

  **NOTE:** Different types of change may need different types of RFC with specific procedures

  **NOTE:** Define which changes are standard and how to treat them.

  **NOTE:** A standard change is a change that has been pre-authorized by Change Management

*While Change Management is well established, policies are embedded in procedures. Process models are ad hoc and not defined as part of the process.*

CHA.BP2 - Document back-out plan or a workaround for each change.

To have a plan in order to restore the service to its original situation in case the change fails during implementation.
If a change is not reversible, therefore making a back-out plan unavailable, a workaround should be identified in order to restore the service in the best possible way. [ITIL v3 - Service Transition: p48] [Expected Result 2]

*The RFC field for back-out plans is free form text and not mandatory. These are not always provided for in RFPs and changes are frequently approved without sufficient back out plans in place.*

CHA.BP3 - Assess remediation prior to change authorization.

The existence of remediation (either back-out plan or workaround) has to be one of the criteria to be considered to approve a change [ITIL v3 - Service Transition: p56, 57] [Expected Result 2, 4]

*While the CCAB may occasionally ask remediation questions, the approval process is such that chain of command authorizations mask the absence of remediation plans.*

CHA.BP4 - Record change details in RFC and update RFC documentation throughout its lifecycle

Changes are recorded in Requests for Change (RFC). The RFC has to be kept up to date as it progresses through the Change process. [ITIL v3 - Service Transition: p50] [Expected Result 3]

*RFCs are established for all production system changes, and some development environments. Change records are routinely updated during the lifecycle of changes.*

CHA.BP5 - Review and filter RFCs.

Review the RFCs filtering out those that seem to be impractical, duplication of previous RFCs, or incomplete [ITIL v3 - Service Transition: p53] [Expected Result 4]

*The Change Manager reviews all RFCs. All changes are e-mailed to 100+ people who can review at their discretion; changes are routinely pre-approved by supervisors.*

CHA.BP6 - Assess, evaluate, and prioritize RFCs.

Consider the potential impact of changes (successful and unsuccessful) on the services or infrastructure and allocate a priority to each RFC. [Expected Result 4, 7]
For example, use the seven Rs of Change Management: Raised, Reason, Return, Risks, Resources, Responsible, Relationship [ITIL v3 - Service Transition: p53]

*Changes are assessed based on the risk field of the RFC; priority is not always set. Adherence to ITIL's "7 Rs" may be subject to free form fields being filled out by change requestors.*

CHA.BP7 - Approve RFC by the Change authority (CAB/ECAB) and communicate the decision with all relevant stakeholders.

Changes (through their associated RFCs) need to be authorized by a Change Authority. Examples of this Change Authority are:

- CAB: Change Advisory Board
- ECAB: Emergency CAB
- Board of directors  [ITIL v3 - Service Transition: p56] [Expected Result 4]

**NOTE:** The levels of authorization for a particular change should be judged by the type, size or risk of the change.

**NOTE:** The decision of the change authority with the regards to the go/no go of the change is communicated to all stakeholders.  [ITIL v3 - Service Transition: p57]

*Changes are approved in several ways:*

- **Record Only** – *Changes that CAB has no authority over, such as facilities downing power in a building, etc.*
- **Minor** – *No outage to production systems, CAB does not specifically address (supervisor approves)*
- **Major** – *Outage to production system; approval requires immediate supervisor, service owner and project manager. CAB approval contingent on these approvals.*
- **Significant** – *Same basic procedure as Major Changes (only impacts a single system)*

*Communication about change approvals is via service owner to his/her users, notification from Change Management, network administration list e-mail or Help Desk communication.*

CHA.BP8 - Schedule authorized changes with the business.
Coordinate that the schedule is respected. [ITIL v3 - Service Transition: p57] [Expected Result 5]

NOTE: The implementation is done by other teams outside Change Management

[ITIL v3 - Service Transition: p57]

*Changes are scheduled by the service owner and implementers, involving the customer as required. Some complex changes are actually scheduled in advance of approval.*

CHA.BP9 - Coordinate the change implementation.

Change management is responsible for ensuring that the changes are implemented i.e., it is responsible for the coordination NOT for the implementation itself. [ITIL v3 - Service Transition: p57] [Expected Result 5]

Change implementation includes building and testing the change before implementation in the live environment. [ITIL v3 - Service Transition: p57]

*Implementer, identified in the RFC, is responsible for coordinating change implementation. Sometimes project management does the coordination. Updates to change records occasionally need policing by the CAB.*

CHA.BP10 - Review change implementation (PIR) and check completeness of change documentation.

Review the results of the change and verify that all the documentation related to the change is available in the RFC. If necessary, update the Configuration Management System (CMS) [ITIL v3 - Service Transition: p57] [Expected Result 6]

PIR = Post-Implementation Review  [ITIL v3 - Service Transition: p58]

*We did not observe procedures for updating documentation, reviewing attachments to the change record or updating configuration records.*

CHA.BP11 - Close the RFC.

RFCs must be formally closed no matter the result (implemented or abandoned) of the change. [ITIL v3 - Service Transition: p58] [Expected Result 6]
All RFCs are closed, even if abandoned. Change Manager will close at monthly review when/if needed.

CHA.BP12 - Document, authorize, and coordinate emergency changes in a specific way.

Emergency changes require specific procedures in order to be executed as fast as possible. [ITIL v3 - Service Transition: p60] [Expected Result 7]

The amount of emergency changes should be kept to a minimum. Too many emergency changes might be a symptom of an uncontrolled Change Management process. [ITIL v3 - Service Transition: p60]

There are an estimated 3-5 emergency changes per week. There is a documented procedure for emergency changes.
**PROCESS INPUTS & OUTPUTS**

**INPUTS**

The Work Products most absent are those that are also related to Service Asset & Configuration Management, Transition Planning & Support and Release & Deployment Management, including:

- Transition plan
- Release and deployment plans
- Test plan
- Evaluation plan
- Remediation plan
- Configuration Items (CI)
- Configuration baseline

**OUTPUTS**

Key outputs not in evidence included:

- Policy and strategies for change and release
- Configuration Items (CI)

**LEVEL 2 – PERFORMANCE MANAGEMENT**

Process performance is **largely** managed.

In this section, we measure the extent to which process performance is planned and managed within time and resource constraints. We assess whether the following points are covered:

- Objectives for the performance of the process are identified.
- The performance of the process is planned and monitored.
- The performance of the process is adjusted to meet plans.
- Responsibilities and authorities for performing the process are defined, assigned, and communicated.
- The resources and information necessary for performing the process are identified, made available, allocated, and used.
• Interfaces between the involved parties are managed to ensure both effective communication and clear assignment of responsibility.

The Assessment Team collected the following findings:

The process is largely managed considering the absence of related process areas. While process supports (tools) could improve performance, roles and responsibilities are defined and metrics are tracked on a regular basis.

LEVEL 2 – WORK PRODUCT MANAGEMENT

Work Products (process inputs and outputs) are partially managed.

In this section, we measure the extent to which the Work Products produced by the process are appropriately managed. We assess whether the following points are covered:

• Requirements for the Work Products of the process are defined.
• Requirements for documentation and control of the Work Products are defined.
• Work Products are appropriately identified, documented, and controlled.
• Work Products are reviewed in accordance with planned arrangements and adjusted as necessary to meet requirements.

The Assessment Team collected the following findings:

The process is missing Work Products, partly as a result of low maturity of related process areas.

However, a common finding across all processes is generally poor management of key process Work Products. This may be a result of policy deficiencies, document management inconsistencies and/or lack of regular review of process Work Products.

LEVEL 3 – PROCESS DEFINITION

The reference process is partially defined.

In this section, we measure the extent to which a standard process is maintained to support the deployment of the defined process. We assess whether the following points are covered:

• A standard process, including appropriate tailoring guidelines, is defined, which describes the fundamental elements that must be incorporated into a defined process.
• The sequence and interaction of the standard process with other processes are determined.
Required competencies and roles for performing a process are identified as part of the standard process.
Required infrastructure and work environment for performing a process are identified as part of the standard process.
Suitable methods for monitoring the effectiveness and suitability of the process are determined.

The Assessment Team collected the following findings:

There are no documented tailoring guidelines for the process. The sequence and interaction of the process with related processes are not defined.

LEVEL 3 – PROCESS DEPLOYMENT

The standard process is partially deployed.

In this section, we measure the extent to which the standard process is effectively deployed as a defined process to achieve its process outcomes. We assess whether the following points are covered:

- A defined process is deployed based on an appropriately selected and/or tailored standard process.
- Required roles, responsibilities, and authorities for performing the defined process are assigned and communicated.
- Personnel performing the defined process are competent based on appropriate education, training, and experience.
- Required resources and information necessary for performing the defined process are made available, allocated, and used.
- Required infrastructure and work environment for performing the defined process are made available, managed, and maintained.
- Appropriate data is collected and analyzed as a basis for understanding the behavior of, and to demonstrate the suitability and effectiveness of, the process and to evaluate where continuous improvement of the process can be made.

The Assessment Team collected the following findings:

Tailoring guidelines are required to effectively deploy the process. The supporting infrastructure may need improvement in order to successfully deploy the process across the organization as a standard process.
SWOT ANALYSIS

STRENGTHS

The analysis of assessment results resulted in the identification of the following main strengths:

The Change Management process is the most mature and accepted process in the organization, and procedures may be well documented.

WEAKNESSES

The analysis of assessment results resulted in the identification of the following main weaknesses:

The lack of documented Change Models, tailoring guidelines and related process areas inhibit the effectiveness of the process.

OPPORTUNITIES

The analysis of assessment results resulted in the identification of the following main opportunities:

There may be existing procedures that can serve as the basis for Change Models and tailoring of the process.

THREATS

The analysis of assessment results resulted in the identification of the following main threats:

Lack of related process areas will continue to inhibit maturity of the Change Management process.
Change Management is the most mature process in CIT, in part due to the persistent efforts of key staff (principally the Change Manager) over the last two years. The establishments of a Process Owner, and steadfast effort over time have made progress.

While significant improvements in this process area may depend on related processes -- such as Service Asset & Configuration Management, Transition Planning & Support and Release Management -- there are some more immediate actions that could benefit the organization.

There is a significant amount of documentation associated with the process, including measurement and reporting on process performance. However policy and procedural information tends to be integrated into the overall documentation and may be unclear to stakeholders.

Separation of procedural information from policy and process documents may also enable existing procedures to be used to establish Change Models that become part of the overall process. This may present opportunities to streamline the approval process as well as ensure that remediation plans are incorporated into the various Change Models.

As the organization develops related process areas, Change Management can expand policy to identify lifecycle control points that satisfy project, transition and release management requirements for various changes.

This can improve consistency of service transition activity while providing flexibility for various requirements through tailored processes and procedures. These procedures, including an increasing library of tested Change Models, provide a foundation for automated actions as process interfaces are more fully understood.
At the end of the assessment, we have identified the following recommendations:

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHA.1</td>
<td>Improve document management</td>
<td>Consider more formal management and control of documentation. This does not mean <em>more</em> documentation! See global recommendations under document controls.</td>
</tr>
<tr>
<td>CHA.2</td>
<td>Establish Change Models</td>
<td>Use existing procedures and document control improvements to establish Change Models as part of the process. This would include the establishment of a library of Standard Changes, preauthorized by the CCAB.</td>
</tr>
<tr>
<td>CHA.3</td>
<td>Evaluate Remediation Plans</td>
<td>Change Models present an opportunity to standardize back-out plans, providing greater rigor for higher risk changes and more complex remediation planning is needed.</td>
</tr>
<tr>
<td>CHA.4</td>
<td>Evaluate Change Approvals</td>
<td>As libraries of Change Models are established that include remediation plans, evaluate opportunities to streamline the approval process (for low risk changes) and focus greater attention on high-risk changes.</td>
</tr>
<tr>
<td>CHA.5</td>
<td>Prioritize process interfaces</td>
<td>Some analysis of supporting processes (i.e., Service Asset &amp; Configuration, Transition Planning &amp; Support, Release &amp; Deployment Management) is needed. One example may be reviewing Transition and Release policies in line with Project Management, and identifying basic lifecycle baseline points and controls. These points and required artifacts must allow tailoring for small, medium and large efforts as well as leverage existing Change Models. Another would be integration with existing (domain-based) configuration data, including an overall architecture for configuration management as process maturity improves.</td>
</tr>
<tr>
<td>CHA.5</td>
<td>Document process interfaces</td>
<td>Process documentation should be updated over time to reflect changes and improvements to supporting processes.</td>
</tr>
</tbody>
</table>
CONFIGURATION MANAGEMENT

PROCESS PURPOSE

The purpose of the Service Asset and Configuration Management process is to define and control the components of services and infrastructure by maintaining accurate configuration information on the historical, planned, and current state of the services and infrastructure.

EXPECTED OUTCOMES

As a result of successful implementation of the Service Asset and Configuration Management process:

1. Service asset and configuration management policies and principles are defined
2. The configuration is identified and base lined
3. The Configuration Management System (CMS) is implemented
4. The Configuration Management System (CMS) is controlled
5. Service Assets and Configuration Items (CIs) are identified
6. Service Assets and Configuration items (CIs) are classified and documented
7. Service Assets and Configuration Items (CIs) are reported, audited, and verified

FINDINGS

The process is at level 0. Process activities are not performed significantly. Overall, the process does not achieve its purpose and outcomes.

While there are configuration management activities taking place within technical domains, there is a significant lack of cross-domain dependency data. Configuration data contained in databases (CMDB) are not unified under a single Configuration Management System (CMS).

This results in controls that are not easily integrated with other ITSM processes.
The consolidation of assessment interviews results in the following profile:

### Service Asset and Configuration Management

<table>
<thead>
<tr>
<th>Level</th>
<th>Level 1 (Performed)</th>
<th>Level 2 (Managed)</th>
<th>Level 3 (Established)</th>
<th>Level 4 (Predictable)</th>
<th>Level 5 (Optimizing)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessed</td>
<td>P</td>
<td>N</td>
<td>N</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Target</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rating scale</td>
<td>Fully</td>
<td>Largely</td>
<td>Partially</td>
<td>Not</td>
<td>N.A.</td>
</tr>
</tbody>
</table>

### Legend
- Level achieved
- Level not achieved
- Not assessed

---

Copyright © 2010 and Confidential to Cornell University
RESULTS ANALYSIS

LEVEL 1

In this section, we measure the extent to which the process is performed, achieves its purpose, and produces its outcomes.

The process is **partially** performed.

The following practices have been reviewed during assessment interviews:

SAC.BP1 - Define the framework and key principles against which assets and configurations are developed and maintained.

- Define configuration management plan
- Defines roles and responsibilities

[ITIL v3 - Service Transition: p66] [Expected Result 1]

*Service Assets and Configurations are locally driven and oriented around technical domains. Roles and responsibilities vary based on organizational unit and technical domain; there is wide variation in the process from one unit to another.*

SAC.BP2 - Define the configuration breakdown model identifying relevant Configuration Items (CIs), granularity levels and relationships among the CIs.

The Configuration Management's logical model of the services and infrastructure is the single common representation used by all parts of IT Service Management, and beyond, such as HR, finance, suppliers and customers. CIs should be selected by applying a top down approach, considering if it is sensible to break down a CI into component CIs. Relationships describe how the CIs work together to deliver the services. [ITIL v3 - Service Transition: p66] [Expected Result 2]

CI information is valuable only if it facilitates the management of change, the control of incidents and problems or the control of assets that can be independently moved, copied or changed. Choosing the right CI level is a matter of achieving a balance between information availability, the right level of control and the resources and effort needed to support it.

Examples of types of relationships:

- a CI is a part of another CI
- a CI is connected to another CI
- a CI uses another CI
- a CI is installed on another CI [ITIL v3 - Service Transition: p77]

The capture of relationships between CIs is locally driven and technically oriented (domain-based). There is rarely a logical model of the infrastructure, particularly for customer-facing services.

SAC.BP3 - Review the relevance of the CIs and granularity level regularly.

The organization should plan to review the CI level regularly to confirm that information down to a low level is still valuable and useful. [ITIL v3 - Service Transition: p74] [Expected Result 2]

While CI granularity varies based on technical domain, there were indications that several domains regularly reviewed CI data. In some cases there was automated discovery in use and generally effective configuration controls, although limited to specific technical domains.

SAC.BP4 – Establish Configuration Baselines.

A configuration baseline is the configuration of a service, product or infrastructure that has been formally reviewed and agreed on, that thereafter serves as the basis for further activities and can be changed only through formal change procedures. It captures the structure, contents and details of a configuration and represents a set of configuration items that are related to each other. [Expected Result 2, 3]

Fragmentation of configuration data between technical domains and multiple independent tools in support of the process make establishing end-to-end service baselines difficult, however there was evidence of an ability to establish domain-based configuration baselines.

SAC.BP5 - Implement a CMS, including one or more CMDBs and a DML.

The CMS is a set of tools and databases that are used to manage an IT Service Provider's Configuration data.

The CMDB(s) store(s) attributes of CIs, and relationships with other CIs.
The DML is one or more locations where the definitive and approved versions of all software CIs are securely stored. Only software from the DML is acceptable to use in Release.

[ITIL v3 - Service Transition: p230, p232] [Expected Result 3]

- CMS = Configuration Management System
- CMDB = Configuration Management Data Base
- DML = Definitive Media Library
- CI = Configuration Items

*There are different approaches to CMDBs and DMLs that vary by business unit and technical domain. The resulting CMS is limited when cross-domain dependency data is required.*

SAC.BP6 - Control access, addition, modification, replacement and removal of CIs.

Configuration control ensures that there are adequate control mechanisms over CIs while maintaining a record of changes to CIs, versions, location and custodianship/ownership. [ITIL v3 - Service Transition: p79] [Expected Result 4]

This includes access and changes in the physical world to avoid mismatch between CMS and physical world.

- CMS = Configuration Management System
- CMDB = Configuration Management Data Base
- DML = Definitive Media Library
- CI = Configuration Items

*Integration of Service Asset & Configuration Management with Change Management is limited by multiple diverse tool sets in use and fragmented configuration management policies and methods across the organization.*

SAC.BP7 - Define categories and lifecycle of CIs.

Typical CIs types include service, hardware, software, documentation, and staff.
Each asset or CI will have one or more discrete states through which it can progress. These status compose the CI's lifecycle. [ITIL v3 - Service Transition: p77] [Expected Result 4, 6]

Example of a lifecycle:

- Development or draft: It means that the CI is under development
- Approved: The CI may be used as a basis for further work
- Withdrawn: Not usable anymore

[ITIL v3 - Service Transition: p80]

*There are lifecycle categories in use, however they may vary across domains.*

SAC.BP8 - Define and use a naming convention for the Service Assets and CIs and identify their attributes.

Individual CIs should be uniquely identifiable by means of the identifier and version. The physical Service Assets and CIs should be labeled with this unique identifier. Attributes describe the characteristics of a CI that are valuable to record. [ITIL v3 - Service Transition: p74] [Expected Result 5]

Typical attributes: [ITIL v3 - Service Transition: p75]

- Unique identifier
- CI type
- Name/description
- Version
- Location
- Supply date
- License details
- Owner/custodian
- Status
- Supplier/source
- Related document masters
- Related software masters
- Historical data
- Relationship type
- Applicable SLA

*CI attribute data is locally driven and domain-based, with no evidence of policy or guidelines to maintain consistency of information.*

SAC.BP9 - Assign types to CIs and maintain status.

In order to facilitate the documentation, components should be classified into assets or CIs types and their status should be kept up to date. [ITIL v3 - Service Transition: p77, p80]

[Expected Result 6]

Typical CIs types are service, hardware, software, documentation, and staff. Typical CI status are drafted, accepted, installed, and withdrawn.

[ITIL v3 - Service Transition: p77, p80]

*CI attribute data is locally driven and domain-based, with no evidence of policy or guidelines to maintain consistency of information.*

SAC.BP10 - Record and maintain service configuration information.

The service configuration information has to be recorded and maintained throughout the whole asset and configuration item life cycle. [ITIL v3 - Service Transition: p79] [Expected Result 6]

*CI attribute data is locally driven and domain-based, with no evidence of policy or guidelines to maintain consistency of information.*

SAC.BP11 - Produce report either on individual CIs, complete services, or the service portfolio according to the needs of the organization
Reports of several types are necessary in the Configuration Management Process. These reports may be required by Financial Management. [ITIL v3 - Service Transition: p81] [Expected Result]

Typical reports: [ITIL v3 - Service Transition: p81]

- List of product configuration information included in a specific configuration baseline
- A list of CIs and their configuration baselines
- Details of the current revision status and change history
- Status reports on changes, waivers, and deviations
- Details of the status of delivered and maintained products concerning par and traceability numbers
- Revision status
- Report on unauthorized usage of hardware and software
- Unauthorized CIs detected
- Variations from CMS to physical audit reports

**Reporting is ad hoc and domain based.**

SAC.BP12 - Perform planned and ad-hoc audits.

A series of reviews or audits should be conducted in order to

- Ensure the conformity between the documented baselines and the actual business environment
- Verify the physical existence of CIs
- Check that release and configuration documentation is present

[ITIL v3 - Service Transition: p81] [Expected Result 7]

**There are no regular audits of configuration data, except in those domains where automated discovery has enabled these activities. Quality checking is reactive and ad hoc.**
PROCESS INPUTS & OUTPUTS

INPUTS

There are no significant inputs that were missing; (i.e., RFCs, CIs, Purchase Orders, and Service/Acquisition Requests).

OUTPUTS

Configuration Baselines, Configuration Management System (CMS) and Configuration Models exist however they are domain-based and do not capture end-to-end services, particularly customer-facing services.
SWOT ANALYSIS

STRENGTHS

The analysis of assessment results resulted in the identification of the following main strengths:

There were several domains that had a very good grasp of configuration management, including the use of discovery tools (one had written a discovery product) and effective configuration management techniques.

WEAKNESSES

The analysis of assessment results resulted in the identification of the following main weaknesses:

The principal weakness is a lack of inter-domain dependency data, and a lack of how one domain may impact another.

OPPORTUNITIES

The analysis of assessment results resulted in the identification of the following main opportunities:

Strong understanding of the importance of configuration data by staff provides a good foundation for process improvement.

THREATS

The analysis of assessment results resulted in the identification of the following main threats:

Multiple disparate tools may limit effective integration with Change and other related processes.
RECOMMENDATIONS

Service Asset & Configuration Management, while a critical ITSM process, will require time to develop. In fact, within each technical domain there is a reasonable level of configuration management activity taking place and staff are very aware of the benefits (and pitfalls) of configuration management.

Most dependency data that is missing is high-level, cross-domain dependency information associated with end-to-end services. This is (more often than not) associated with customer-facing services. CIT should take steps to capture this high-level dependency information and establish logical models of the service infrastructure starting with the most critical services.

As these logical models are established, the specific Configuration Items (CI) associated with each service should be identified along with where the CI attribute information is stored.

With Managed Desktop Services a key CIT initiative a review of Asset Management policies and procedures, including software assets, should be conducted. The location and use of secure libraries and secure stores should be identified.
At the end of the assessment, we have identified the following recommendations:

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAC.1</td>
<td>Focus in the short term on high level configuration data</td>
<td>Identify appropriate staff that can capture high-level dependency data and establish logical models of the service infrastructure.</td>
</tr>
<tr>
<td>SAC.2</td>
<td>Identify Configuration Items under control and CI repositories</td>
<td>Begin identifying critical CI data, location/type of repository and CI administrators.</td>
</tr>
</tbody>
</table>
| SAC.3 | Review Asset Management Policy                           | Evaluate asset management policies in light of the managed desktop initiative, along with integration with related process areas such as Change and Release Management.  
Evaluate software asset management policy, including the location and use of secure libraries and secure stores. |
TRANSITION PLANNING & SUPPORT

PROCESS PURPOSE

The purpose of the Transition Planning and Support process is to plan and coordinate the resources to deploy a release within the predicted cost, time and quality estimates following a commonly accepted process framework.

To plan and coordinate the resources to ensure that the requirements of Service Strategy encoded in Service Design are effectively realized in Service Operations.

EXPECTED OUTCOMES

As a result of successful implementation of the Transition Planning and Support process:

1. Transition policies and principles are defined
2. Transition strategy is defined and enforced
3. Service Transition is prepared
4. Service Transition is planned and coordinated
5. Service Transition is supported
6. Service transition is monitored

FINDINGS

The process is at level 0. Process activities are not performed significantly. Overall, the process does not achieve its purpose and outcomes.

Transition Planning & Support is dependent on Project Management, does not follow an accepted policy and does not consistently meet its objectives.
The consolidation of assessment interviews results in the following profile:

### Transition Planning and Support

<table>
<thead>
<tr>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performed</td>
<td>Managed</td>
<td>Established</td>
<td>Predictable</td>
<td>Optimizing</td>
</tr>
<tr>
<td>Assessed</td>
<td>F</td>
<td>P</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Target</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>N.A.</td>
</tr>
</tbody>
</table>

**Rating scale**
- Fully (F)
- Largely (L)
- Partially (P)
- Not (N)
- N.A. (N.A.)

---

**Legend**
- Level achieved
- Level not achieved
- Not assessed
In this section, we measure the extent to which the process is performed, achieves its purpose, and produces its outcomes.

The process is **partially** performed.

**The following practices have been reviewed during assessment interviews:**

**TPS.BP1 - Define a Service Transition policy.**

A formal policy for Service Transition should be defined and approved by the management team. The strategy has to be communicated throughout the organization and to all relevant suppliers and partners. [ITIL v3 - Service Transition: p25] [Expected Result 1]

- Policies should state the objectives and address any non-compliance
- Policies should be aligned with the overall governance framework, organization, and Service Management policies
- Use processes that integrate teams and integrate competencies keeping clear lines of accountability and responsibility
- Deliver changes in releases
- Address deployment early in the release design and release planning stages

**Best practice:** The sponsors and the decision makers developing it should formally sign the policy. [ITIL v3 - Service Transition: p25]

*Policies are typically restricted to CIT and tend to be embedded in procedures.*

**TPS.BP2 - Define and communicate the strategic approach to organize all transition processes and ensure consistency among them.**

Define the overall approach to organizing Service Transition and allocating resources, and communicate it to all parties involved in Service Transition. [ITIL v3 - Service Transition: p38, p41] [Expected Result 2]
Transitions are ad hoc and defined on a case-by-case basis. There is no consistency of releases and transition practices.

TPS.BP3 - Provide training about the Transition Strategy.

Train the teams involved in Transition Strategy [ITIL v3 - Service Transition: p38] [Expected Result 2, 3]

Training is ad hoc and takes place only for the largest transitions.

TPS.BP4 - Review and check the input deliverables.

Some of the input deliverables are:

- SDP
- Service acceptance criteria
- Evaluation report [Expected Result 3]

[ITIL v3 - Service Transition: p39]

Key transition artifacts such as the Service Design Package (SDP), Service Acceptance Criteria (SAC) and Evaluation Reports were not readily apparent. Project management may provide for some of these, but in an inconsistent fashion and on a case-by-case basis.

TPS.BP5 - Identify, raise, and schedule RFCs.

Identify, raise, and schedule RFCs [ITIL v3 - Service Transition: p39] [Expected Result 3]

When project management is involved, the project manager will issue RFCs; once production is reached the Service Manager would issue RFCs. The hand-off between transition and operations is inconsistent and unclear.

TPS.BP6 - Check the recording of configuration baselines in Configuration Management before the start of Service Transition.
Configuration baselines help fixing a point in history where interested people can apply changes to in an understandable manner [ITIL v3 - Service Transition: p39] [Expected Result 3]

Any variance to the proposed service scope, Service Strategy requirements and Service Design baseline must be requested and managed through Change Management. [ITIL v3 - Service Transition: p39]

*Application domains tend to have greater control over configuration baselines (of application code) than infrastructure. Baselines of the production infrastructure are more complicated by cross-domain inconsistencies and fragmented processes and toolsets.*

**TPS.BP7 - Define and maintain an integrated set of transition plans.**

A Service Transition plan describes the tasks and activities required to release and deploy a release into the test environments and into production. [ITIL v3 - Service Transition: p40] [Expected Result 4]

The tasks included in a transition plan are the following:

- Work environment and infrastructure for the Service Transition
- Schedule of milestones, handover and delivery dates
- Activities and tasks to be performed
- Staffing, resource requirements, budgets and time-scales at each stage
- Issues and risks to be managed
- Lead times and contingency

[ITIL v3 - Service Transition: p40]

*Presumably project management performs some of these requirements, when they are engaged. However, the lack of a clearly defined Service Transition Policy and the application of project management are inconsistent and not repeatable.*

**TPS.BP8 - Review the plans before starting the release.**
The Service Transition Planning role should verify the plans before starting the release or deployment. These plans are Service Transition, Release, and Deployment plans. [ITIL v3 - Service Transition: p40] [Expected Result 4]

Some questions that the Service Transition Planning role should ask:

- Are these Service Transition and Release plans up to date?
- Have the plans been agreed and authorized by all relevant parties? (Customers, users, operations staff, etc.)
- Do the plans include the release dates and deliverables and refer to related change requests, known errors and problems?

[ITIL v3 - Service Transition: p40]

*Presumably project management performs some of these requirements, when they are engaged. However, the lack of a clearly defined Service Transition Policy and the application of project management are inconsistent and not repeatable.*

TPS.BP9 - Provide advice on transition processes supporting systems and tools.

Support should be provided for all users to understand and be able to follow the Service Transition framework of processes and supporting systems and tools. [Expected Result 5] [ITIL v3 - Service Transition: p41]

*The supporting systems and tools vary significantly from one business unit to another. There is no overall architecture for any ITSM toolset across the organization, which significantly fragments the ITSM processes and the organization.*

TPS.BP10 - TPS.BP10 Provide administration.

The Service Transition Planning and Support role should provide administration [Expected Result 5]

The items to administer are:

- Managing of Service Transition changes and work orders
- Managing issues, risks, deviations, and waivers
- Managing support for tools and Service Transition processes

- Communications to stakeholders

- Monitoring the Service Transition performance to provide input into CSI

[ITIL v3 - Service Transition: p41]

_The bulk of administration falls to the project manager and project team, when they are involved in transitions. When these resources are not part of the transition, it is less clear who administers these tasks; in some cases it may be the Service Manager. In the absence of clear transition policy transition administration will remain inconsistent._

TPS.BP11 - Monitor Service Transition activities against plans.

Service Transition activities require monitoring against the intention set out in the transition model and plan. [Expected Result 6] [ITIL v3 - Service Transition: p42]

_These activities fall to the project manager; there are no standard ‘gates’ or service lifecycle controls for transitions. These activities are resourced and funded on a project-by-project basis._

TPS.BP12 - Identify significant variances based on Service Transition activities report.

Management reports on the status of each transition will help to identify when there are significant variances from plan. This will allow other organizations (such as Project Management or Service Management) to make decisions and take action. [ITIL v3 - Service Transition: p42] [Expected Result 6]

_Reporting is driven by the Project Director (Service Owner), however there are no dedicated release or transition resources for these resources to work with._
PROCESS INPUTS & OUTPUTS

INPUTS

The Service Design Package (SDP) was not in evidence and is likely to be fragmented across the organization. Other key inputs (listed below) are inconsistent and depend on project management resources.

- Request for Change (RFC)
- Service Design Package (SDP)
- Release design
- Service Acceptance Criteria (SAC)
- Transition Strategy
- Integrated set of Service Transition Plans

OUTPUTS

Outputs are present but the effectiveness may be impacted by missing or incomplete inputs:

- Transition Strategy
- Integrated set of Service Transition Plans
- Request for Change (RFC)
SWOT ANALYSIS

STRENGTHS

The analysis of assessment results resulted in the identification of the following main strengths:

For larger projects, the organization has people with knowledge and experience in transition activities.

WEAKNESSES

The analysis of assessment results resulted in the identification of the following main weaknesses:

There is no transition policy, leaving room for variation from one project to another. Reliance on project management for all transition activities increases variation, and may be an inefficient use of project resources.

OPPORTUNITIES

The analysis of assessment results resulted in the identification of the following main opportunities:

Change Management is reasonably well deployed, providing a basis for improvements in this process area.

THREATS

The analysis of assessment results resulted in the identification of the following main threats:

Cultural factors and separation between applications and infrastructure present significant challenges to process adoption.
RECOMMENDATIONS

The shift away from dedicated QA and transition resources, and adjustments to the project management methods within CIT may make future transition activities more inconsistent and unreliable. Efforts should be made to clarify Transition Policies in conjunction with Project Management, Change Management and Release Management.

The Change Management, Transition Planning & Support and Release Management policies must allow for tailoring in much the same way that project management tailors methods for small, medium and large projects. In fact, greater integration between the Project Management Life Cycle (PMLC) and the Service Lifecycle is highly desirable.

The Service Lifecycle and Project Management processes can incorporate process models (i.e., Change Models, etc.) and predefined templates to make related artifacts more consistent. There may be opportunities to consolidate artifacts and agree on key baseline points based on the models and project tailoring guidelines.

This can provide the basis for the establishment of Lifecycle controls that can help customers and staff understand what is required as project move through the service lifecycle. Monitoring these control points can identify improvement opportunities not always readily apparent from a pure process control perspective.
At the end of the assessment, we have identified the following recommendations:

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TPS.1</td>
<td>Establish a Transition Policy</td>
<td>Define a transition policy with the involvement of project management and key IT staff. Ensure tailoring of projects and use of Change Models is supported. Identify roles and responsibilities for transitions, considering agreed tailoring guidelines. Clearly establish roles and responsibilities for QA.</td>
</tr>
<tr>
<td>TPS.2</td>
<td>Establish Lifecycle Controls</td>
<td>Work with Change, Project and Release Management to identify key baseline points and standard artifacts at various stages in the Service Lifecycle. Consider tailoring guidelines when establishing baseline points and artifacts, minimizing their number and complexity as appropriate for the level of risk involved.</td>
</tr>
<tr>
<td>TPS.3</td>
<td>Refine transition Work Products</td>
<td>Ensure that key stakeholders are in agreement on the presence of critical Work Products, including:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Requirements (SLR)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Service Design Package (SDP) contents</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Service Acceptance Criteria (SAC)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Transition &amp; Release Plans</td>
</tr>
</tbody>
</table>
RELEASE & DEPLOYMENT MANAGEMENT

PROCESS PURPOSE

The purpose of the Release and Deployment Management process is to build, test, and deliver the capability to provide the services specified by Service Design and that will accomplish the stakeholders' requirements and deliver the intended objectives.

The primary goal of Release and Deployment Management is to ensure that the integrity of the live environment is protected and that the correct components are released.

EXPECTED OUTCOMES

As a result of successful implementation of the Release and Deployment Management process:

1. Release and Deployment Management policies and principles are defined
2. Released packages are planned, designed and prepared
3. Release packages are built and tested
4. Release packages are validated or accepted
5. Release packages are deployed successfully
6. Release packages are reviewed and closed
7. Knowledge transfer to customers is ensured

FINDINGS

The process is at level 0. Process activities are not performed significantly. Overall, the process does not achieve its purpose and outcomes.

While the Release & Deployment process is partly performed, it is almost totally reliant on project management.

Significant variations in the process take place due to inconsistencies across technical domains, business units and project management staff.
The consolidation of assessment interviews results in the following profile:

<table>
<thead>
<tr>
<th>Process Assessment Report</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PROCESS PROFILE</strong></td>
</tr>
</tbody>
</table>

Release and Deployment Management

<table>
<thead>
<tr>
<th>Level 1 Performed</th>
<th>Level 2 Managed</th>
<th>Level 3 Established</th>
<th>Level 4 Predictable</th>
<th>Level 5 Optimizing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessed</td>
<td>F</td>
<td>P</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Target</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>Rating scale</td>
<td>Fully</td>
<td>Largely</td>
<td>Partially</td>
<td>Not</td>
</tr>
</tbody>
</table>

Legend:
- Level achieved
- Level not achieved
- Not Assessed

[Table and diagram showing the assessment results]
RESULTS ANALYSIS

LEVEL 1

In this section, we measure the extent to which the process is performed, achieves its purpose, and produces its outcomes.

The process is partially performed.

The following practices have been reviewed during assessment interviews:

RDM.BP1 - Define policies and procedures.

Define release and deployment policies and procedures, roles and responsibilities, release and deployment models and emergency release procedures [ITIL v3 - Service Transition: p85] [Expected Result 1]

It includes a unit and identification scheme [ITIL v3 - Service Transition: p85]

There are no common roles around release and deployment management outside of project management and the service owner. There is no established release policy other than a checklist for new service deployments.

RDM.BP2 - Define the approach to transitioning from the current service to the new or changed service.

Define how the transition is done from the current situation of the service to the new one [ITIL v3 - Service Transition: p85] [Expected Result 2]

For example, for deploying new releases to multiple locations there are two options: "big bang approach" or "Phased approach".

From another point of view, there are also the "push" and "pull" approaches, and the "Automation" and "manual" approaches.

The selected approach should take into account the dependencies between CIs (e.g. new application software requires an OS upgrade)

Project managers define deployment approaches in the project-planning phase. In some cases it is not always clear what is in the build and what's in the production path; risk management is often time/schedule driven.
RDM.BP3 - Define and agree deployment plans.

Derive a sound set of guidelines for the release into production and subsequent deployments. [ITIL v3 - Service Transition: p91] [Expected Result 2, 3]

The deployment plan should be aligned with one of the predefined deployment models.

Plans relevant for release and deployment:

- pass/fail criteria
- building and test plans
- planning of pilots
- planning of release package and build activities
- deployment planning
- logistical planning and delivery planning
- financial and commercial planning

[ITIL v3 - Service Transition: p91]

*There were not predefined deployment models observed. Release Management activities are dependent on projects.*

RDM.BP4 - Build and maintain the test environment.

The test environment of the service needs to be built and then maintained to use it in later release deployments. [ITIL v3 - Service Transition: p98] [Expected Result 2]

*There are test environments that are maintained, however occasionally they are not closely aligned to the production environment.*

RDM.BP5 - Acquire, verify, and assemble the CIs and components of the release package and document it.
Acquire CIs and components from projects, suppliers, partners, and development groups and Assemble and integrate them in a controlled manner to ensure a reproducible process.

Create the build and release documentation [ITIL v3 - Service Transition: p99] [Expected Result 3]

Include procedures to back out releases.

*The organization has not succeeded in establishing dedicated roles for release management activities, and procedures vary from one release to the next. There is no overarching process framework that ties Standard Operating Procedures together to form a consistent release management framework.*

RDM.BP6 - Verify and test release packages.

The release packages have to be tested and verified before being transferred to Configuration Management. [ITIL v3 - Service Transition: p97] [Expected Result 3]

*Each release is verified and tested in an ad hoc way; in some cases releases get into production before people can review. Variations in testing approaches may result in inefficient use of resources.*

RDM.BP7 - Perform service rehearsals and pilots.

A rehearsal includes a rehearsals plan, delivery of the rehearsal, checking the rehearsal, act after the rehearsal. A pilot is conducted with the real system with real users.

[ITIL v3 - Service Transition: p102] [Expected Result 4, 5]

The difference between a rehearsal and a pilot is that the rehearsal remains a closed test whereas the pilot is shown to the final users. They both serve to decide whether the service is suitable or not to go into production. If not, the service is sent back to design. Once the rehearsal or pilot is finished (no matter its results) it has to be formally closed.

*The KFS project performed rehearsals with positive results, but this is not typical of most efforts. Pilots are more common, but are dependent on project inputs.*
RDM.BP8 - Perform deployment readiness assessment.

Readiness assessment identifies:

- Issues and risks in delivering the current services that may affect the deployment
- Anticipated impacts (e.g. organizational structure, environment for the new or changed services, direct customers and users, partners, suppliers)
- Gaps that need to be filled

[ITIL v3 - Service Transition: p105] [Expected Result 5]

Everyone is asked to perform readiness assessments, however they are left to individual units and do not always occur. There are times when documents do not come back but releases are still marked ready for production. Rigor varies with the project (i.e., PeopleSoft gets more attention than other projects, etc.)

RDM.BP9 - Perform CIs transfer, deployment and retirement.

- Transfer financial assets
- Transfer/transition business and organization
- Deploy processes and materials
- Transfer service
- Deploy service
- Decommissioning and service retirement
- Remove redundant assets

[ITIL v3 - Service Transition: p107- p109] [Expected Result 5]

There are inconsistencies in the handling of CIs (i.e., some said no defined plan, others said it was well defined). Significant variation based on the project.

RDM.BP10 - Verify that users, service operations, other staff and stakeholders are capable of using or operating the service and assure early life support (ELS).
The tests should specifically verify that:

- The service, service assets and service capability/resources are in place
- Updates to documentation and information are completed
- Communications, orientation and learning materials are ready to be distribute
- All roles are assigned
- People and other resources are prepared to operate and use the new/changed service in all situations
- People have access to the information necessary to use, operate or support the service
- The measurement and reporting systems are established [Expected Result 5]

NOTE: ELS provides appropriate resources to resolve operational and support issues quickly, centrally and locally, to ensure that the users can use the service to support their business activities without unwarranted disruption. Check the figure 4.24, page 110 of the Service Transition book. [ITIL v3 - Service Transition: p109]"

*There is no concept of Early Life Support, and no dedicated resources to assure that operations are prepared to support a release. This leads to high levels of Incidents after a release, which tend to settle down over time.*

RDM.BP11 - Review and close release deployment.

The review should include the following activities:

- Captures experiences and feedback on customer, user and service provider satisfaction
- Highlight quality criteria that were not met
- Check that any actions, necessary fixes and changes are complete
- Review open changes
- Review performance targets and achievements
- Make sure that there are no capability, resource, capacity or performance issues at the end of the deployment
- Check that any problems, known errors and workarounds are documented and accepted
- Review the Risk Log
- Check that redundant assets have been removed
- Check that the service is ready for transition from ELS into Service Operations

The deployment is completed with a handover of the support for the deployment group or target environment to Service Operations. [ITIL v3 - Service Transition: p111] [Expected Result 6]

NOTE: A post implementation review of a deployment is conducted through Change Management process. [ITIL v3 - Service Transition: p112]

Post Implementation Reviews (PIR) are totally dependent on project management; there were indications that mistakes were repeated and knowledge not captured or adequately distributed to those with a need to know.

RDM.BP12 - Distribute all documentation and provide training.

A transition report should be produced that summarizes the outcomes. Define a training program for customer impacting releases [Expected Result 7]

A post transition workshop could be held involving all parties as a 'lessons learned' exercise. [ITIL v3 - Service Transition: p112]

The reviews at the end of a project are with the customer, and may not adequately involve all appropriate operational personnel. So while documentation and lessons learned are distributed, they may miss critical elements of the organization.
PROCESS INPUTS & OUTPUTS

INPUTS

There are a number of Work Products associated with the process, many of which may be missing, fragmented or not under appropriate management:

- Service Level Package (SLP)
- Service Package
- Service Design Package (SDP)
- IT service continuity plan
- Technology and procurement standards and catalogs
- Service assets and components
- Service assets and components documentation
- Build models and plans
- Requirements and specifications
- Policy and strategies for change and release
- Release design
- Release and deployment models
- Entry/Exit criteria for each stage of release and deployment
- Request for Change (RFC)

OUTPUTS

Similarly, key outputs are missing, fragmented or not well managed as a result of poor or missing inputs:

- Release and deployment plans
- Service notification
- Service catalog
- Service capability and environment
- Service Management documentation
- Service Package
- Service Level Package (SLP)
- Service Level Agreement (SLA)
- Service Model
- Service report
- IT service continuity plans
- Configuration Items (CI)
- Capacity Plan
- Release package
- Service Transition report
- Request for Change (RFC)
SWOT ANALYSIS

STRENGTHS

The analysis of assessment results resulted in the identification of the following main strengths:

There was evidence of Release & Deployment skills and experience in the organization, particularly for larger projects.

WEAKNESSES

The analysis of assessment results resulted in the identification of the following main weaknesses:

No dedicated Release Management resources for the project teams to work with.

OPPORTUNITIES

The analysis of assessment results resulted in the identification of the following main opportunities:

Change Management may provide a basis for process improvement.

THREATS

The analysis of assessment results resulted in the identification of the following main threats:

Cultural factors and separation between applications and infrastructure present significant challenges to process adoption.
Recommendations for Release & Deployment Management mirror those of Transition Planning & Support.

The shift away from dedicated QA and transition resources, and adjustments to the project management methods within CIT may make future transition activities more inconsistent and unreliable. Efforts should be made to clarify Release Policies in conjunction with Project Management, Change Management and Transition Planning & Support.

The Change Management, Transition Planning & Support and Release Management policies must allow for tailoring in much the same way that project management tailors methods for small, medium and large projects. In fact, greater integration between the Project Management Life Cycle (PMLC) and the Service Lifecycle is highly desirable.

The Service Lifecycle and Project Management processes can incorporate process models (i.e., Change Models, etc.) and predefined templates to make related artifacts more consistent. There may be opportunities to consolidate artifacts and agree on key baseline points based on the models and project tailoring guidelines.

This can provide the basis for the establishment of Lifecycle controls that can help customers and staff understand what is required as projects move through the service lifecycle. Monitoring these control points can identify improvement opportunities not always readily apparent from a pure process control perspective.
At the end of the assessment, we have identified the following recommendations:

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RDM.1</td>
<td>Establish a Release Policy</td>
<td>In conjunction with Transition Planning &amp; Support and Change Management, establish Release Policies that help clarify what the minimal acceptable requirements are for various types of releases.</td>
</tr>
<tr>
<td>RDM.2</td>
<td>Establish Lifecycle Controls</td>
<td>Work with Change, Project and Transition Planning &amp; Support to identify key baseline points and standard artifacts at various stages in the Service Lifecycle. Consider tailoring guidelines when establishing baseline points and artifacts, minimizing their number and complexity as appropriate for the level of risk involved.</td>
</tr>
<tr>
<td>RDM.3</td>
<td>Refine transition Work Products</td>
<td>Ensure that key stakeholders are in agreement on the presence of critical Work Products, including:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Requirements (SLR)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Service Design Package (SDP) contents</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Service Acceptance Criteria (SAC)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Service assets and components</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Service assets and components documentation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Entry/Exit criteria for each stage of release and deployment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Release Plans</td>
</tr>
</tbody>
</table>
SERVICE OPERATION

EVENT MANAGEMENT

PROCESS PURPOSE

The purpose of the Event Management process is to monitor all events that occur through the IT infrastructure to allow for normal operation.

An event can be defined as any detectable or discernible occurrence that has significance for the management of the IT infrastructure or the delivery of IT services. Events happen in an IT service, Configuration Item (CI), or monitoring tool and generate notifications.

Event Management is the entry point for the execution of many Service Operation processes and activities. Event Management can be applied to any aspect of Service Management that needs to be controlled and which can be automated.

EXPECTED OUTCOMES

As a result of successful implementation of the Event Management process:

1. Event Management policies are defined
2. Events are notified (meaningful notifications about the status of the IT infrastructure or services are generated)
3. Events are captured
4. Events are dealt with
5. Events are reviewed and closed
6. Event monitoring mechanisms and filtering rules are kept up-to-date.

FINDINGS

The process reaches level 1. Process activities are performed. The process achieves its purpose but in a non-repeatable way and with few controls. During each instance, the process is not implemented in a managed fashion (planned, monitored, and adjusted). Work Products are not appropriately established, controlled, and maintained. Moreover, the way the process is managed is not uniform throughout the organization.

There is Event Management process activities that occur, although they are restricted to technical domains.
The consolidation of assessment interviews results in the following profile:

### Event Management

<table>
<thead>
<tr>
<th>Level 1 Performed</th>
<th>Level 2 Managed</th>
<th>Level 3 Established</th>
<th>Level 4 Predictable</th>
<th>Level 5 Optimizing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessed</td>
<td>F</td>
<td>L</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Target</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>Rating scale</td>
<td>Fully</td>
<td>Largely</td>
<td>Partially</td>
<td>Not</td>
</tr>
</tbody>
</table>

**Legend**
- Level achieved
- Level not achieved
- Not assessed
RESULTS ANALYSIS

LEVEL 1

In this section, we measure the extent to which the process is performed, achieves its purpose, and produces its outcomes.

The process is largely performed.

The following practices have been reviewed during assessment interviews:

EVE.BP1 - Define event categories.

Define event categories (informational, warning or exception). [ITIL v3 - Service Operation: p37] [Expected Result 1, 3, 6]

There are different categories of events that are driven by technical domain and various monitoring tools. While they are not formally described in a document, and may vary slightly from one domain to another, staffs are well aware of the event types.

EVE.BP2 - Define events to generate.

Define events to generate (what type of event need to be detected?). [ITIL v3 - Service Operation: p45] [Expected Result 1,3,6]

The decisions on what type of events to detect are driven by the domains, which are generally well suited to identify domain-based events; however there may be less understanding of the inter-dependencies between domains.

EVE.BP3 - Generate an event notification.

An event notification is generated (by a device interrogated by a management tool, or generated by a CI when certain conditions are met). [ITIL v3 - Service Operation: p39] [Expected Result 2]

Primarily various monitors and management tools generate event notifications.

EVE.BP4 - Detect events.
Detect any generated event notifications (from CI directly, collected by a management tool) and determine event category. [ITIL v3 - Service Operation: p39] [Expected Result 3]

*Various monitoring/management tools detect events and individual CIs; event detection is occasionally driven by human interaction (phone call).*

EVE.BP5 - Establish the significance of an event.

Establish the significance of an event (by comparing this event with a set of Business rules) and determine what actions should be taken. [ITIL v3 - Service Operation: p40] [Expected Result 4]

*Technical domains and CI owners define event significance; they are sometimes based on defined thresholds. The service category (i.e., Tier 0 or Tier 1) is an important driver of event significance, regardless of the event."

EVE.BP6 - Select the appropriate response.

Select the appropriate response, including:

- Event logged
- Auto response
- Alert and human intervention
- Incident/Problem/Change?
- Open a RFC
- Open an incident record
- Open or link to a problem record
- Special types of incident

[ITIL v3 - Service Operation: p41] [Expected Result 4]

*There are procedures written by each domain that outline response actions, from calling on-call staff to establishing a bridge call. The NOC has a run book that outlines procedures for getting technical staff and/or Service Owners involved. Service Owners take responsibility for response actions; each domain maintains their own Work Instructions as required.*
EVE.BP7 - Trigger a response.

If the event is recognized, trigger the appropriate response.

[ITIL v3 - Service Operation: p41] [Expected Result 4]

NOTE: Trigger types can include: incident triggers, scripts or database triggers.

NOTE: The Event Management process interfaces to any process that requires monitoring and control.

*Response triggers are based on run books and Work Instructions within each technical domain; automated actions (scripts) are in limited use.*

EVE.BP8 - Review actions.

Check that any significant events or exceptions have been handled appropriately. [ITIL v3 - Service Operation: p43] [Expected Result 5]

*Security, the NOC and each domain perform exception handling. The NOC escalates based on pre-defined criteria set by Service Owners and domain Subject Matter Experts (SME).*

EVE.BP9 - Track trends.

Track trends or counts of event types. [ITIL v3 - Service Operation: p42] [Expected Result 5]

*Trending is left to each technical domain; cross-domain trends are not tracked.*

EVE.BP10 - Close the events.

Close every kind of event, by logging informational events, by generating a second event for auto-response events, and by linking to the appropriate record in case of events that generated an incident, a problem or a change. [ITIL v3 - Service Operation: p43] [Expected Result 5]

*Events (Alerts) are closed, however use of multiple ticketing systems may mask Event closure activities.*
EVE.BP11 - Implement effective filtering rules and mechanisms for generating meaningful events.

Implement effective filtering rules and mechanisms for generating meaningful events.

[ITIL v3 - Service Operation: p45] [Expected Result 6]

*While there was no filtering policy formally defined, each domain sets appropriate rules for filtering events by system administrators who program the various monitors in use. While the lack of cross-domain intelligence could present issues with filtering desired event types there was no indication this was occurring.*

EVE.BP12 - Maintain effective filtering rules and mechanisms for generating meaningful events.

Maintain effective filtering rules and mechanisms for generating meaningful events. [ITIL v3 - Service Operation: p45, p46] [Expected Result 6]

*While there was no filtering policy formally defined, each domain sets appropriate rules for filtering events by system administrators who program the various monitors in use. While the lack of cross-domain intelligence could present issues with filtering desired event types there was no indication this was occurring.*
PROCESS INPUTS & OUTPUTS

INPUTS

Aside from the lack of a consolidated Configuration Management System (CMS), no significant gaps in process inputs were detected:

- Event notification
- Configuration Management System (CMS)
- Event Management tool
- Event categories
- Event filtering rules

OUTPUTS

The process produces Incident and Problem records, however fragmentation and lack of maturity limit effectiveness.

- Event record
- Incident record
- Problem record
- Event trends and patterns report
- Event notification
- Event categories
- Event filtering rules
- Request for Change (RFC)

LEVEL 2 – PERFORMANCE MANAGEMENT

Process performance is not managed.

In this section, we measure the extent to which process performance is planned and managed within time and resource constraints. We assess whether the following points are covered:

a) Objectives for the performance of the process are identified.
b) The performance of the process is planned and monitored.
c) The performance of the process is adjusted to meet plans.
d) Responsibilities and authorities for performing the process are defined, assigned, and communicated.
e) The resources and information necessary for performing the process are identified, made available, allocated, and used.
f) Interfaces between the involved parties are managed to ensure both effective communication and clear assignment of responsibility.

The Assessment Team collected the following findings:

While the process purpose and expected outcomes are largely achieved, the process planning, monitoring and adjustments are ad hoc. Roles and responsibilities are assigned, but within each domain and not as part of a coordinated effort. There is no formal process ownership.

LEVEL 2 – WORK PRODUCT MANAGEMENT

Work Products (process inputs and outputs) are not managed.

In this section, we measure the extent to which the Work Products produced by the process are appropriately managed. We assess whether the following points are covered:

- Requirements for the Work Products of the process are defined.
- Requirements for documentation and control of the Work Products are defined.
- Work Products are appropriately identified, documented, and controlled.
- Work Products are reviewed in accordance with planned arrangements and adjusted as necessary to meet requirements.

The Assessment Team collected the following findings:

Work Products and management is heavily fragmented across technical domains, and while procedural documentation may exist the key inputs and outputs of the process are not managed in a coordinated fashion.
SWOT ANALYSIS

STRENGTHS
The analysis of assessment results resulted in the identification of the following main strengths:

Most IT technical domains have a strong understanding of the importance of event management.

WEAKNESSES
The analysis of assessment results resulted in the identification of the following main weaknesses:

There is a significant lack of cross-domain dependency data and monitoring intelligence.

OPPORTUNITIES
The analysis of assessment results resulted in the identification of the following main opportunities:

Some application staff are working on compiling cross-domain dependency data, presenting an opportunity for process improvement.

THREATS
The analysis of assessment results resulted in the identification of the following main threats:

Domains outside the control of CIT may be hesitant to provide access to event information, and CIT may be unable to require this data or persuade them to provide.
RECOMMENDATIONS

There are three aspects of Event Management; 1) Detecting Events, 2) Making sense of Events, and 3) Taking the appropriate control action.

CIT’s technical domains seem to do a reasonable job at all three, which are performed to varying degrees and with toolsets (monitors) tuned to domain-specific needs. However, service infrastructures increasingly span multiple technical domains that can complicate ‘making sense of events’ beyond the capability of any single individual (or even a room full of experts).

CIT seems to recognize this, and roles have been piloted to accelerate the capture of end-to-end dependency data. Past efforts have included attempts at automating discovery development of a real time CMIS (Capacity management Information System).

Nowhere will this be more important than in the Virtual Hosted Services area, a key initiative of the CIT. The need to establish end-to-end service views is shared by other ITSM process areas as well:

- Financial Management, to prepare accurate cost models for services
- Service Level Management, to understand end-to-end requirements
- Service Asset & Configuration Management, to establish logical models of the service infrastructure

CIT should continue these efforts, perhaps combining them with other activities in progress such as Continuity efforts (BIA, etc.), Service Level Requirement (SLR) definition and Availability Management.

In addition, greater integration between the Event Management process and Incident Management is needed. The understanding of Events, both as they unfold and after action is taken, is an opportunity to raise the level of expertise of Level 1 staff. Building and validating a knowledge base that can be used in the Service Desk is a shared responsibility between the Service Desk and Level 2/3 support staff, and event management intelligence can help facilitate collaborative management.

For this reason, the organization should evaluate correlation technologies that can make sense of cross-domain events, particularly in virtual environments.
At the end of the assessment, we have identified the following recommendations:

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVE.1</td>
<td>Service Views</td>
<td>Leverage the creation of Technical Application Admins to accelerate the capture of end-to-end dependency data for critical IT services.</td>
</tr>
<tr>
<td>EVE.2</td>
<td>Service Desk bridging</td>
<td>Establish a bridge to the Service Desk and improve integration of Event and Incident Management. Ensure that communication with the Service Desk is as events happen, not after the fact.</td>
</tr>
<tr>
<td>EVE.3</td>
<td>Correlation</td>
<td>After some progress has been made capturing end-to-end dependency data, analyze Event and Incident data and conduct a feasibility study to isolate the benefits of correlating events across multiple technical domains.</td>
</tr>
</tbody>
</table>
INCIDENT MANAGEMENT

PROCESS PURPOSE

The purpose of the Incident Management process is to restore normal service operation as quickly as possible minimizing the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

Normal service operation is defined as service operation within Service Level Agreement -SLA- limits.

The incidents described here can include failures; questions or queries reported by the users, by technical staff, or automatically detected and reported by event monitoring tools.

EXPECTED OUTCOMES

As a result of successful implementation of the Incident Management process:

1. Incident management policies are defined
2. Incidents are identified
3. Incidents are investigated
4. Incidents are solved
5. Incidents are tracked all along their life cycle
6. Customers are kept informed of their incidents progress, and, if necessary, of the service level breaches
FINDINGS

The process is at level 0. Process activities are not performed significantly. Overall, the process does not achieve its purpose and outcomes.

Some non-CIT business units had significantly higher levels of Incident Management process maturity than CIT, however they were unable to leverage their process across domains when needed. The number and type of tools and different Help Desks varies significantly from one organizational unit to another.

While process activities are performed, the resulting fragmentation significantly restricts process effectiveness and efficiency, particularly within CIT.
RESULTS ANALYSIS

LEVEL 1

In this section, we measure the extent to which the process is performed, achieves its purpose, and produces its outcomes.

The process is partially performed.

The following practices have been reviewed during assessment interviews:

INC.BP1 - Define and agree on incident categories and priorities.

Define and agree on incident categories and priorities (including major incidents).

[ITIL v3 - Service Operation: p49] [Expected Result 1, 2]

Within CIT, Incident categories are defined within the Remedy toolset. Operational Categories (OpCats) are assigned by the Help Desk, however there is a limited number of full time staff on the CIT Help Desk and consistent Incident classification may be elusive. Priorities are based on Impact and Urgency which is automatically calculated by Remedy; no matrix of how impact and urgency guidelines was observed.

Major Incidents are referred to as ‘Severity 1” (aka, ‘the Big Red Button’) and a procedure for handling these Incidents was observed.

Outside of CIT, there were other tools in use however most organizational units were classifying Incidents (although in different ways). Priority was often based on the localized knowledge of customers rather than impact/urgency matrix and tools.

INC.BP2 - Define, agree and communicate timescales for all incident-handling stages.

Define and agree on timescales based upon the overall incident response and resolution targets within SLAs. Communicate timescales to all support groups. [ITIL v3 - Service Operation: p47] [Expected Result 1,3,4,6]

Service Level Agreements (SLAs) were not widely used, regardless of organizational unit. Timescales for Incident handling varied, from none to quite specific, however these timescales were not consistent across organizational units. For Incidents that span multiple domains this may cause some user confusion. In fact, small local support groups with aggressive response
times may create the perception that CIT is unresponsive, even when within 'agreed' time limits.

INC.BP3 - Detect and log the incident.

Record the relevant information (date, time, unique reference number) about the incident whatever the way of reporting. [ITIL v3 - Service Operation: p49] [Expected Result 2]

NOTE: Incidents could be reported by technical staff, users, or communicated by Event Management

Most organizational units are diligent about reporting Incidents, whether by e-mail, user calls or from technical staff. Few scripts are in use to guide Incident handling, and some organizational units (including CIT) do not clearly distinguish between Incidents and Requests.

INC.BP4 - Categorize the incident.

Assign the incidents to a type, a category and some sub-categories. [ITIL v3 - Service Operation: p50] [Expected Result 2]

NOTE: If Service requests are detected (incorrectly logged as incidents), transfer them to the Request fulfillment process.

Categorization of Incidents varies widely across organizational units. Some do not differentiate between Incidents and Requests. There are multiple tools in use, most of which provide assistance with categorizing/classifying Incidents.

INC.BP5 - Prioritize and provide initial support to the incident.

Assign a priority to the incident, by assessing its impact and urgency. Assess the incident details to find a solution to continue business, via a degraded service or a temporary solution if needed (Example: Work-around solution). [ITIL v3 - Service Operation: p51] [Expected Result 2, 4]

Within CIT, priority is driven by service Tier (Tier 0 and Tier 1). Across organizational units there is no consistency or guidelines for assigning impact and urgency. For many smaller organizational units, priority is intuitive and based on familiarity with the customer/user environment.
INC.BP6 - Investigate and diagnose the incident.

Analyze and investigate incidents by the appropriated line support. [ITIL v3 - Service Operation: p52] [Expected Result 3,4]

The investigation is likely to include such actions as:

- establishing exactly what has gone wrong or being sought by the user
- understanding the chronological order of events
- confirming the full impact of the incident, including the number and range of users affected
- identifying any event that could have triggered the incident
- knowledge searches looking for previous occurrences

*Investigation and diagnosis of Incidents is inconsistent; there was no knowledge base in use regardless of organizational unit. It is likely that many Incidents are escalated quickly to Level 2 (specialist support groups like e-mail) or Level 3 (Service Owners/Managers).*

INC.BP7 - Escalate the incident to specialize or authority lines.

Route to n-line support or authority (iterative process) if the (n-1)--line cannot resolve the incident. [ITIL v3 - Service Operation: p52] [Expected Result 3]

NOTE: Functional escalation concerns a lack of knowledge or expertise. Hierarchical escalation is done when the resolution of the incident will be not in time or satisfactory (e.g. against a SLA).

*Escalation varies with organizational unit, even though most organizational units share common resources. Escalating to Level 3 (Service Owners/Managers) by phone call; updates are intended to be hourly but frequently the Help Desk does not receive updates. Many escalation paths within organizational units are informal and ad hoc.*

INC.BP8 - Identify and test potential resolutions.

Identify and test potential resolutions.

[ITIL v3 - Service Operation: p52] [Expected Result 4]
Each organizational unit uses different approaches to maintaining resolution data, but very few (if any) have resolution databases. There are multiple independent efforts to creating knowledge bases that vary significantly by organizational unit, technical domain and tool set in use.

INC.BP9 - Implement the incident resolution.

Implement incident resolution that enables the resumption of business activities. [ITIL v3 - Service Operation: p53] [Expected Result 4]

NOTE: If needed, a Request For Change (RFC) can be raised for incident resolution through the Change Management Process.

For the most part, Service Owners/Managers and desktop support are responsible for implementing Incident resolutions; no data on the percentage of calls resolved at the Help Desk were observed. Communication between the HD and Level 2/3 is inconsistent.

INC.BP10 - Close the incident.

Close the incident, after the user confirmation that the incident is resolved and service restored, and update the records with any relevant details.

[ITIL v3 - Service Operation: p53]. [Expected Result 4]

Use of part time staff by the CIT Help Desk, and ineffective communication between Level 1 and Level 2/3 staff is limiting closure effectiveness (closed without codes or reasons, etc.).

INC.BP11 - Track and monitor the incident.

Track and monitor the incident until closure and update incident record when necessary.

[ITIL v3 - Service Operation: p49] [Expected Result 5]

If the Incident does not span multiple domains or organizational units, some Help Desks retain ownership over the Incident throughout its lifecycle, however this is the exception rather than the rule. For cross-domain Incidents there are gaps associated with ineffective escalation and communication between organizational units.
INC.BP12 - Communicate to customer.

Communicate on the incident resolution progress, or on the service level breaches to all affected parties. [ITIL v3 - Service Operation: p52] [Expected Result 6]

*Communication with customers/users is tailored to local requirements for non-CIT organizational units, and works well when issues are locally based. However, there are multiple communication paths and frequently the Help Desk is not included in communication loops. There is no significant presence of Service Level Agreements (SLA), which makes setting clear expectations difficult or impossible.*
PROCESS INPUTS & OUTPUTS

INPUTS

Key inputs to the process are absent, including:

- Configuration Management System (CMS)
- Service Level Agreement (SLA)
- Known Error Database (KEDB)
- Incidents knowledge base
- Problem knowledge base

OUTPUTS

Missing inputs negatively impacts outputs:

- Incident categories
- Incident record
- Incidents knowledge base

In addition, other than Major Incidents (Severity 1, ‘Big Red Button’) and Security Incidents there are no Incident Models documented.

LEVEL 2 – PERFORMANCE MANAGEMENT

Process performance is **not** managed.

In this section, we measure the extent to which process performance is planned and managed within time and resource constraints. We assess whether the following points are covered:

- Objectives for the performance of the process are identified.
- The performance of the process is planned and monitored.
- The performance of the process is adjusted to meet plans.
- Responsibilities and authorities for performing the process are defined, assigned, and communicated.
- The resources and information necessary for performing the process are identified, made available, allocated, and used.
- Interfaces between the involved parties are managed to ensure both effective communication and clear assignment of responsibility.
The Assessment Team collected the following findings:

From an IT@Cornell perspective, Incident Management is not a managed process, but there are some organizational units that might be considered “Largely” managed. Unfortunately given the shared dependencies that each unit has with IT, the benefits may not justify the increased costs associated with multiple, local Help Desks and independent Incident Management processes.

LEVEL 2 – WORK PRODUCT MANAGEMENT

Work Products (process inputs and outputs) are not managed.

In this section, we measure the extent to which the Work Products produced by the process are appropriately managed. We assess whether the following points are covered:

- Requirements for the Work Products of the process are defined.
- Requirements for documentation and control of the Work Products are defined.
- Work Products are appropriately identified, documented, and controlled.
- Work Products are reviewed in accordance with planned arrangements and adjusted as necessary to meet requirements.

The Assessment Team collected the following findings:

Regardless of organizational unit, Work Products are not well identified, defined, documented and controlled. This pattern was common across all organizational units and all process areas.

LEVEL 3 – PROCESS DEFINITION

The reference process is not defined.

In this section, we measure the extent to which a standard process is maintained to support the deployment of the defined process. We assess whether the following points are covered:

- A standard process, including appropriate tailoring guidelines, is defined, which describes the fundamental elements that must be incorporated into a defined process.
- The sequence and interaction of the standard process with other processes are determined.
- Required competencies and roles for performing a process are identified as part of the standard process.
The Assessment Team collected the following findings:

Regardless of business unit, the process has not been formally defined, particularly with regards to tailoring guidelines, interaction with other process areas, competencies/roles and (in some cases) process monitoring effectiveness.

**LEVEL 3 – PROCESS DEPLOYMENT**

The standard process is **not** deployed.

In this section, we measure the extent to which the standard process is effectively deployed as a defined process to achieve its process outcomes. We assess whether the following points are covered:

- A defined process is deployed based on an appropriately selected and/or tailored standard process.
- Required roles, responsibilities, and authorities for performing the defined process are assigned and communicated.
- Personnel performing the defined process are competent based on appropriate education, training, and experience.
- Required resources and information necessary for performing the defined process are made available, allocated, and used.
- Required infrastructure and work environment for performing the defined process are made available, managed, and maintained.
- Appropriate data is collected and analyzed as a basis for understanding the behavior of, and to demonstrate the suitability and effectiveness of, the process and to evaluate where continuous improvement of the process can be made.

The Assessment Team collected the following findings:

As a standard process has not been defined, this attribute is not relevant.
SWOT ANALYSIS

STRENGTHS

The analysis of assessment results resulted in the identification of the following main strengths:

There are several organizational units that have strong Incident Management process capability.

WEAKNESSES

The analysis of assessment results resulted in the identification of the following main weaknesses:

The de-centralized nature of IT (multiple Help Desks, tools, etc.) significantly increases the complexity of the process from an IT@Cornell perspective.

OPPORTUNITIES

The analysis of assessment results resulted in the identification of the following main opportunities:

Multiple organizational units expressed interest in process support (tool) improvement potential; presenting an opportunity for process improvement.

THREATS

The analysis of assessment results resulted in the identification of the following main threats:

Some organizational units continue to invest in the purchase and/or development of independent Incident Management toolsets and process initiatives.
The Service Desk is the ‘face of IT’ and is highly dependent on the Incident and Request Fulfillment processes. CIT’s Incident Management process is significantly constrained due to fragmentation across multiple business units, multiple diverse tools in use, and the use of temporary staff.

This exacerbates the perception of CIT as ‘not having the ability to deliver quality, reliable services’\(^3\). CIT should take steps to increase the number of full time, professional staff on the Help (Service) Desk.

Less clear is the degree to which consolidation of various Help Desks would be beneficial, however significant duplication of effort exists. There needs to be a discussion about the scope of a University-wide Incident Management process and the appropriate structure of the Service Desk based on real customer requirements and cost constraints.

Cornell should implement a formal Incident Management process across the University, perhaps starting with CIT but expanding its scope to other units as defined and agreed during the scoping and chartering of the process.

Steps should be taken as soon as possible to compile a resolution and/or knowledge base for use by front line staff in Incident handling. Requests should be separately categorized from Incidents in areas where this is not already occurring, and volume data for both Incidents and Requests should be compiled. Self-service capabilities that exist should be leveraged if possible.

\(^3\) Report of the Ad Hoc Review Committee for IT@Cornell
At the end of the assessment, we have identified the following recommendations:

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INC.1</td>
<td>Service Desk Staffing</td>
<td>Increase the number of full-time professional staff on the CIT Help Desk.</td>
</tr>
<tr>
<td>INC.2</td>
<td>Clarify Incident Mgt scope</td>
<td>Agreement needs to be reached on the scope of the Incident Management process; CIT only, CIT for desktops, CIT and select business units, etc.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Identify the appropriate mix of Service Desk structures for the organization (Central, Local, etc.)</td>
</tr>
<tr>
<td>INC.3</td>
<td>CIT Incident Management</td>
<td>Formally define and implement a formal Incident Management process, initially focusing on CIT, but incorporating inputs from other stakeholders as appropriate.</td>
</tr>
<tr>
<td>INC.4</td>
<td>Begin populating a resolution and knowledge base</td>
<td>Populate an Incident Resolution and/or knowledge base for common Incidents, communicate and update to all Service Desk staff.</td>
</tr>
<tr>
<td>INC.5</td>
<td>Requests vs. Incidents</td>
<td>Begin to separate tracking and reporting of Requests from Incidents. Establish Request Models in cooperation with Change Management and leverage self-service wherever possible.</td>
</tr>
</tbody>
</table>
REQUEST FULFILLMENT

PROCESS PURPOSE

The purpose of the Request Fulfillment process is to respond to service requests from the users.

A Service Request is a request from a user for information, advice, a standard change, or access to a service (without any impact on current service delivery).

Some organizations treat the service requests as a special type of incident.

EXPECTED OUTCOMES

As a result of successful implementation of the Request Fulfillment process:

1. Service Request management policies are defined
2. Standard services are requested and received through a dedicated communication channel
3. Service Requests are approved
4. Service requests are fulfilled
5. Service Requests progress is monitored
6. Users are kept informed of their service requests progress

FINDINGS

The process reaches level 1. Process activities are performed. The process achieves its purpose but in a non-repeatable way and with few controls. During each instance, the process is not implemented in a managed fashion (planned, monitored, and adjusted). Work Products are not appropriately established, controlled, and maintained. Moreover, the way the process is managed is not uniform throughout the organization.

Request Fulfillment is not uniform but process activities are performed and it achieves its purpose, however procedures may not be well controlled.
The consolidation of assessment interviews results in the following profile:

**Request Fulfilment**

<table>
<thead>
<tr>
<th>Level 1 Performed</th>
<th>Level 2 Managed</th>
<th>Level 3 Established</th>
<th>Level 4 Predictable</th>
<th>Level 5 Optimizing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessed</td>
<td>L</td>
<td>F</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Target</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td></td>
</tr>
</tbody>
</table>

**Rating scale**

- **Fully**
- **Largely**
- **Partially**
- **Not**
- **N.A.**

**Legend**

- Level achieved
- Level not achieved
- Not assessed
RESULTS ANALYSIS

LEVEL 1

In this section, we measure the extent to which the process is performed, achieves its purpose, and produces its outcomes.

The process is **largely** performed.

**The following practices have been reviewed during assessment interviews:**

REQ.BP1 - Agree on timescales for all request-handling stages.

Agree on timescales for all request-handling stages.

[ITIL v3 - Service Operation: p56] [Expected Result 1, 4, 5]

*There are timescales for different requests, however there are no SLAs. The different Help Desks are generally well aware of these timescales.*

REQ.BP2 - Define, document and agree on what is a standard service request.

Define, document and agree on what is a standard service request.

[ITIL v3 - Service Operation: p56] [Expected Result 1]

*Individual business units define standard service requests; procedures are stored in various locations and managed independently. Variation in controls over these procedures exists. The knowledge of standard service requests is limited to individual Help Desks.*

REQ.BP3 - Record the Service Requests.

Record service requests, whatever the way of reporting. [ITIL v3 - Service Operation: p57] [Expected Result 2, 5]

*Recording of service requests varies with organizational unit and tools in use, but most units are recording requests.*

REQ.BP4 - Establish an estimate of the cost.
Establish an estimate of the cost of fulfilling the Service Request.

[ITIL v3 - Service Operation: p57]. [Expected Result 3]

*Estimating the cost of fulfilling a request is typically limited to obtaining the price of a requested item, not actual fulfillment costs. Procedures for estimating costs are developed and maintained within each business unit or technical domain.*

REQ.BP5 - Submit the estimate of the cost.

Submit the estimate of the cost of fulfilling the Service Request to the user for approval.

[ITIL v3 - Service Operation: p57] [Expected Result 3, 6]

  **NOTE:** Define and check compliance-related or wider business approval.

  *Estimates are sent to users who have 30 days to respond (typical). Users may negotiate requirements but not price.*

REQ.BP6 - Escalate the requests.

Escalate the requests to specialist groups and/or supplier when necessary.

[ITIL v3 - Service Operation: p57] [Expected Result 4, 5, 6]

  *Stakeholders were generally satisfied with escalation, although documentation on escalation procedures was not observed.*

REQ.BP7 - Handle service requests.

Handle service requests, and charge for the work done, if necessary.

[ITIL v3 - Service Operation: p57] [Expected Result 4]

  *Service requests are handled well, but not as a result of clearly defined Request Models. Most organizations rely on organizational familiarity for request handling.*

REQ.BP8 - Close Service Requests.
Close Service Requests and check that the user is satisfied with the outcome.

[ITIL v3 - Service Operation: p57] [Expected Result 4]

Requests are routinely closed; some units have automated the closure process, others rely on follow up from the Help Desk, but requests are closed and reasonable attempts to verify with the customer are made.

REQ.BP9 - Monitor Service request progress.

Monitor Service request progress all along its lifecycle.

[ITIL v3 - Service Operation: p57] [Expected Result 5]

NOTE: Update service request record when necessary

Most organizational units are effectively tracking requests however there are no Operational Level Agreements or formal reporting that consolidates all request activity.

REQ.BP10 - Keep users informed.

Keep users informed of their service requests progress.

[ITIL v3 - Service Operation: p57]. [Expected Result 6]

Communication with users is (in some cases) automated. The type of communication varies by request type and organizational unit.

PROCESS INPUTS & OUTPUTS

INPUTS

While there is no organization-wide Configuration Management System (CMS), principal inputs that may not be adequately controlled include Request Models; these procedures are developed and maintained within each business unit.

OUTPUTS
Procedural outputs (Request Models, Standard Fulfillment Procedures) are fragmented and ad hoc.

**LEVEL 2 – PERFORMANCE MANAGEMENT**

Process performance is **Partially** managed.

In this section, we measure the extent to which process performance is planned and managed within time and resource constraints. We assess whether the following points are covered:

- Objectives for the performance of the process are identified.
- The performance of the process is planned and monitored.
- The performance of the process is adjusted to meet plans.
- Responsibilities and authorities for performing the process are defined, assigned, and communicated.
- The resources and information necessary for performing the process are identified, made available, allocated, and used.
- Interfaces between the involved parties are managed to ensure both effective communication and clear assignment of responsibility.

The Assessment Team collected the following findings:

There was evidence of process performance management, including process objectives, performance monitoring, resource allocation and managed interfaces. However, formal documentation (particularly procedural) is ad hoc.

**LEVEL 2 – WORK PRODUCT MANAGEMENT**

Work Products (process inputs and outputs) are **Not** managed.

In this section, we measure the extent to which the Work Products produced by the process are appropriately managed. We assess whether the following points are covered:

- Requirements for the Work Products of the process are defined.
- Requirements for documentation and control of the Work Products are defined.
- Work Products are appropriately identified, documented, and controlled.
- Work Products are reviewed in accordance with planned arrangements and adjusted as necessary to meet requirements.

The Assessment Team collected the following findings:

Regardless of organizational unit, Work Products are not well identified, defined, documented and controlled. This pattern was common across all organizational units and all process areas.
SWOT ANALYSIS

STRENGTHS

The analysis of assessment results resulted in the identification of the following main strengths:

Some business units showed significant process capability, including process supports (tools).

WEAKNESSES

The analysis of assessment results resulted in the identification of the following main weaknesses:

There is no consistency across organizational units, and procedures may vary considerably.

OPPORTUNITIES

The analysis of assessment results resulted in the identification of the following main opportunities:

There may be opportunities to apply effective procedures as models for the organization.

THREATS

The analysis of assessment results resulted in the identification of the following main threats:

Process maturity, where it exists, may be strongly tied to specific business unit needs and not easily transferable to other units.
RECOMMENDATIONS

Most business units have established procedures (Request Models) to handle requests, although they are documented in different ways and maintained to varying degrees on different systems. Capturing and cataloging these Request Models is recommended.

As the structure for the Service Desk is understood and evolves, it will be important that these procedures (Request Models) are validated, maintained and communicated to the Service Desks that will require them. Boundaries for those business units that have isolated fulfillment processes and procedures will need to be understood and defined.

The timeframes for handling requests should be reviewed by Service Level Management and agree by all stakeholders in order to set proper expectations with customers and users.
At the end of the assessment, we have identified the following recommendations:

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>REQ.1</td>
<td>Capture Request Models</td>
<td>Using procedures that already work and are in use, create a library of Request Models and validate with Change Management as appropriate as Standard Changes. Place these procedures under document control.</td>
</tr>
<tr>
<td>REQ.2</td>
<td>Clarify process boundaries</td>
<td>Using the agreed structure for Service Desk(s), ensure that request fulfillment procedures (Request Models) are known to appropriate stakeholders. Ensure that Request Fulfillment process boundaries between CIT and non-CIT entities are clearly understood and communicated.</td>
</tr>
<tr>
<td>REQ.3</td>
<td>Expectation Management</td>
<td>Ensure that timeframes for requests are understood and agreed by customers, and represented in Service Catalog and Service Level Management activities.</td>
</tr>
</tbody>
</table>
PROBLEM MANAGEMENT

PROCESS PURPOSE

The purpose of the Problem Management process is to prevent problems and resulting incidents from happening, to eliminate recurring incidents, and to minimize the impact of incidents that cannot be prevented.

ITIL defines a ‘problem’ as the unknown cause of one or more incidents.

Incident and Problem Management are closely related and may use similar categorization, impact and priority coding systems.

Proactive Problem Management is generally driven as part of Continual Service Improvement.

EXPECTED OUTCOMES

As a result of successful implementation of the Problem Management process:

1. Problem management policies are defined;
2. Problems are identified;
3. Problems are either resolved or gotten round;
4. Problems are closed;
5. Problem resolutions are reviewed.

FINDINGS

The process is at level 0. Process activities are not performed significantly. Overall, the process does not achieve its purpose and outcomes.

Problem Management is ad hoc and reactive, and really an extension of Incident Management. Key inputs are absent and the purpose is not achieved.
The consolidation of assessment interviews results in the following profile:

### Problem Management

<table>
<thead>
<tr>
<th>Level 1 Perfomed</th>
<th>Level 2 Managed</th>
<th>Level 3 Established</th>
<th>Level 4 Predictable</th>
<th>Level 5 Optimizing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance</td>
<td>Management</td>
<td>Management</td>
<td>Control</td>
<td>Measurement</td>
</tr>
<tr>
<td>Managed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assessed</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Target</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td></td>
</tr>
</tbody>
</table>

**Rating scale**

- Fully: F
- Largely: L
- Partially: P
- Not: N
- N.A.: N.A.

**Legend**

- Level achieved
- Level not achieved
- Not Assessed
In this section, we measure the extent to which the process is performed, achieves its purpose, and produces its outcomes.

The process is **not** performed.

**The following practices have been reviewed during assessment interviews:**

**PRO.BP1 - Define and agree on what is a major problem.**

Define and agree on what is a major problem.

[Expected Result 1, 2]

_The organization uses Severity 1 (Incidents) as Problems. Directors push the 'Big Red Button' that is almost always the result of an outage (Incident)._

**PRO.BP2 - Detect problems.**

Detect problems, reported by service desk, event management, incident management, proactive problem management, supplier or contractor. [ITIL v3 - Service Operation: p61]

[Expected Result 2]

_No proactive problem management takes place; unless a Director pushes the ‘Big Red Button’ problem management does not occur._

**PRO.BP3 - Log problems.**

Record each problem with all relevant information such as:

- user details
- service details
- equipment details
- date/time initially logged
- priority and categorization details
- incident description
- details of all diagnostic or attempted recovery actions taken

[ITIL v3 - Service Operation: p61] [Expected Result 2]

*Problem logging is the result of individual efforts rather than defined process and procedure.*

PRO.BP4 - Allocate problem category.

Allocate problem category in the same way as incidents (and it is advisable to use the same coding system). [ITIL v3 - Service Operation: p61] [Expected Result 2]

*Problem coding is the same as Incidents (there is little to no differentiation between Incident and Problem records).*

PRO.BP5 - Allocate problem priority.

Allocate problem priority in the same way and for the same reasons as incidents (but the frequency and impact of related incidents must also be taken into account).

[ITIL v3 - Service Operation: p61] [Expected Result 2]

*There is no policy or rules for establishing the priority of Problems.*

PRO.BP6 - Investigate problems.

Investigate problems by using such techniques as:

- chronological analysis
- pain value analysis
- Kepner and Tregoe
- Brainstorming
- Ishikawa diagrams
- Pareto analysis
**Director will push problem teams; when root-cause is established action items are identified and resolution steps are taken. Service Managers do most of the investigation.**

PRO.BP7 - Implement resolution or workaround.

If any change in functionality is required to solve the problem, then implement resolution through Change Management, else, document details of the workaround within the problem record. [Expected Result 3]

**NOTE:** RFC follows Change Management process.

[ITIL v3 - Service Operation: p64]

*Resolutions are documented in Remedy (Incident) and RFCs are created as needed, even if after the fact. The Director (Service Owner) is responsible for resolution.*

PRO.BP8 - Update the known error database.

Update the known error database, as soon as the diagnosis is complete, and particularly where a workaround has been found.

[ITIL v3 - Service Operation: p64] [Expected Result 3]

*While applications teams may log application bugs, there is no formal process for logging known errors and they’re not routinely communicated to the Help Desk.*

PRO.BP9 - Check and update problem record.

Check and update problem records.

[ITIL v3 - Service Operation: p64] [Expected Result 4]

*There is no systematic review of known errors; this is done ad hoc.*
PRO.BP10 - Close problem record.

Close problem record (when any change has been completed, successfully reviewed and the resolution has been applied).

[ITIL v3 - Service Operation: p64] [Expected Result 4]

*Records (Remedy/Incident) are closed, but they may not be uniquely defined as problem records; (individual efforts may collate these after the fact).*

PRO.BP11 - Conduct a review after every major problem.

Conduct a review after every problem, and especially for major problems.

[ITIL v3 - Service Operation: p64] [Expected Result 5]

*There is not really a definition of a Major Problem that can be distinguished from a Severity 1 (Major Incident), however these are reviewed.*
PROCESS INPUTS & OUTPUTS

**INPUTS**

Key inputs are missing including:

- Problem knowledge base
- Known Error Database (KEDB)
- Incidents knowledge base
- Configuration Management System (CMS)

**OUTPUTS**

Key outputs are missing including:

- Problem record
- Problem knowledge base
- Known Error Database (KEDB)
SWOT ANALYSIS

STRENGTHS

The analysis of assessment results resulted in the identification of the following main strengths:

There are individual efforts being made to track Problems, and application groups are logging known errors (bugs).

WEAKNESSES

The analysis of assessment results resulted in the identification of the following main weaknesses:

Problems are treated like Major Incidents.

OPPORTUNITIES

The analysis of assessment results resulted in the identification of the following main opportunities:

There may be basic actions that can begin to raise the awareness of the process.

THREATS

The analysis of assessment results resulted in the identification of the following main threats:

There is low maturity in related process areas (Incident, Availability, Service Asset & Configuration, etc.)
RECOMMENDATIONS

An important element of Problem Management is both its separation from, and relationship with, Incident Management. Performing root-cause analysis after a Major Incident is not the objective of the process; it is preventing Incidents in the first place (or reducing their impact).

Level 2/3 staff should be encouraged to provide workarounds for Level 1 staff, to minimize the impact of Incidents to users and reduce the number of escalations to Level 2/3 staff.

Correctly identifying Problems (the unknown cause of one or more Incidents) and establishing a log of the ‘top 10’ is one way to highlight the need for Problem Management resources to be assigned. These teams should include informal benefit statements in problem resolution data to help justify the commitment to the process.

The Service Level Management process should ensure integration between the Service Improvement Plan (SIP) procedures and the Problem Management process when needed.
At the end of the assessment, we have identified the following recommendations:

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRO.1</td>
<td>Knowledgebase development</td>
<td>Capture Known Errors and communicate their workarounds to the Service Desk.</td>
</tr>
<tr>
<td>PRO.2</td>
<td>Top 10 List</td>
<td>Identify and prioritize a Top 10 Problems list. Apply staff to perform problem analysis and problem resolution, as resources are available.</td>
</tr>
<tr>
<td>PRO.3</td>
<td>SIP integration</td>
<td>For Major Incidents and/or critical service level breaches, establish Problem Teams and document resolution activity and results (benefits).</td>
</tr>
</tbody>
</table>
**APPENDIX**

**READING THE RESULTS OF A TIPA ASSESSMENT**

**MATURITY LEVELS**

Processes are assessed using a Maturity Scale going from 1 to 5. Level 0 reflects a non-implemented process or a process that fails to partially achieve its expected results. Level 5 is the more mature level. It reflects a process that achieves its purpose and is managed, defined, and performed within defined limits and in continuous improvement.

**PROCESS MODEL**

The assessment is based on a structured description of processes called *process model*. Each process is defined in terms of purpose, Expected Results, Base Practices, inputs, and outputs.

**MATURITY LEVELS AND ATTRIBUTES**

Each level is composed of two sublevels (attributes), except for level 1, which contains only one. To assess a process, these sublevels are rated.

- To reach a specific level, attributes for this level should be “Largely” or “Fully” achieved and attributes of lower levels should be “Fully” achieved.
- For level 1: The process is performed when its purpose is achieved and when it produces its outcomes.
- For levels 2 to 5: Attributes for levels 2 to 5 are always the same for all processes. They are detailed in ISO/IEC 15504.

The *Capability Levels and Attributes* table outlines the definition of attributes at each level.
<table>
<thead>
<tr>
<th>Maturity Level</th>
<th>Process Attributes (PAs)</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 0 – Incomplete</td>
<td></td>
<td>The process is not implemented or only partially achieves its purpose.</td>
</tr>
<tr>
<td>Level 1 – Performed</td>
<td>PA 1.1 Process Performance</td>
<td>Process activities are performed. The process achieves its purpose but in a non-repeatable way and with few controls.</td>
</tr>
<tr>
<td>Level 2 – Managed</td>
<td>PA 2.1 Performance Management</td>
<td>During each instance, the process is implemented in a managed fashion (planned, monitored, and adjusted). Work Products are appropriately established, controlled, and maintained. However, the way the process is managed is not uniform throughout the organization.</td>
</tr>
<tr>
<td></td>
<td>PA 2.2 Work Product Management</td>
<td></td>
</tr>
<tr>
<td>Level 3 – Established</td>
<td>PA 3.1 Process Definition</td>
<td>The process is defined in a standard way and implemented in accordance with its definition throughout the organizational unit.</td>
</tr>
<tr>
<td></td>
<td>PA 3.2 Process Deployment</td>
<td></td>
</tr>
<tr>
<td>Level 4 – Predictable</td>
<td>PA 4.1 Process Measurement</td>
<td>The process operates within defined limits to achieve its outcomes. It is quantitatively managed to become predictable within defined limits.</td>
</tr>
<tr>
<td></td>
<td>PA 4.2 Process Control</td>
<td></td>
</tr>
<tr>
<td>Level 5 – Optimizing</td>
<td>PA 5.1 Process Innovation</td>
<td>The process is continuously improved to meet relevant current and projected business goals.</td>
</tr>
<tr>
<td></td>
<td>PA 5.2 Process Optimization</td>
<td></td>
</tr>
</tbody>
</table>

**Capability Levels and Attributes**
RATING SCALE

Each item is rated using a scale that reflects to which extent an item is achieved.

- “Fully” achieved: Achieved between 86 and 100% (“Fully”)
- “Largely” achieved: Achieved between 51 and 85% (“Largely”)
- “Partially” achieved: Achieved between 16 and 50% (“Partially”)
- “Not” achieved: Achieved between 0 and 15% (“Not”)

PROCESS PROFILE: PRESENTATION OF THE RESULTS

The graphical presentation of the assessment results for attributes is called the process profile. This profile presents assessed processes horizontally and levels and attributes vertically.

<table>
<thead>
<tr>
<th>Process</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Performed</td>
<td>Managed</td>
<td>Established</td>
<td>Predictable</td>
<td>Optimising</td>
</tr>
<tr>
<td>Process 1</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>F</td>
<td>P</td>
</tr>
<tr>
<td>Process 2</td>
<td>F</td>
<td>L</td>
<td>P</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process 3</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>L</td>
<td>P</td>
</tr>
<tr>
<td>Process 4</td>
<td>P</td>
<td>P</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Legend:

- “Fully” (F)
- “Largely” (L)
- “Partially” (P)
- “Not” (N)

Not Assessed