

1.4 Contact Information

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

1.5 Type of Standard

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

1.6 Publication

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

Check One	Publish as Internal or External
<input type="checkbox"/>	Internal Standard
<input checked="" type="checkbox"/>	External Standard

1.7 Acknowledgements

1.7.1 Development Team

Name	Cluster/Ministry	Branch
Norm Watt	MBS	Infrastructure Development and Deployment Branch
Lorrie MacKinnon	MBS	ITS & Change Management Branch
Ali Ajellu	MBS	ITS & Change Management Branch
Binh Lu	MBS	ITS & Change Management Branch
Selena Leung	MBS	Infrastructure Development and Deployment Branch
Mohamed El-Deeb	MBS	Consultant to Infrastructure
Ryan Rossman	MBS	Infrastructure Development and Deployment Branch
Rick Guyatt	MBS	Infrastructure Development and Deployment Branch

1.7.2 Reviewers

Check	Area	Date: (month/year)
<input checked="" type="checkbox"/>	Technical Standards Unit, Corporate Architecture Branch, OCCTO	July 2004
<input type="checkbox"/>	Corporate Architecture Branch (CAB Architects), OCCTO	
<input checked="" type="checkbox"/>	Infrastructure Development Branch & iSERV, OCCSD	April 2004
<input type="checkbox"/>	Corporate Security Branch, OCCS	
<input type="checkbox"/>	Strategy, Policy, Planning and Management Branch (SPPM, OCCS)	
<input checked="" type="checkbox"/>	Corporate ACT and Domain Working Groups	Sept 2004
<input type="checkbox"/>	– Information Architecture Domain (IADWG)	
<input type="checkbox"/>	– Technology Architecture Domain (TADWG)	
<input type="checkbox"/>	– Application Architecture Domain (AADWG)	
<input type="checkbox"/>	– Security Architecture Working Group (SAWG)	
<input type="checkbox"/>	Cluster ACT/ARB (for cluster standards promoted to corporate standards)	
<input checked="" type="checkbox"/>	ITSC members	July/Aug '04
<input checked="" type="checkbox"/>	Others (<i>named below</i>)	

Name	Cluster/Ministry	Branch
Maria Ritchie	IJ	Infrastructure Support Branch
Michael Oas	IJ	Consultant to IJ
Darrell Bengert	CAC	Enterprise Technology Solutions
Tony Condello	HSC	Technology Management Branch
Wynann Rose	TC	IT Service Management
Rick Morasch	CSC	Information Technology and Services
Ron Brittain	EBC	Information & Technology Management Branch
Jerry Sanford	LRC	Client Services
Jim MacPherson	EBC	Consultant to ESDI

Configuration Management

2 Common Process Principles

IT organizations define principles to guide the design and delivery of services to customers or users. Principles can be common – that is they apply to all functions and groups - or local and apply specifically to a specific function or group.

The absence of well-defined common principles may result in processes that are neither aligned with customer expectations nor with the standards set for delivery of service.

Common principles for the OPS are listed below.

Principle 1:

The Configuration Management Database (CMDB) represents the current known-state of the IT environment.

Rationale:

- Ensures all authorized CIs are under Configuration Management control
- Enables the Change Management Process to determine the impact to the IT environment for each proposed change
- Supports and enhances the Incident, Problem, Change, Configuration, Operations and Release Management processes via the use of the CMDB

Implications:

- The level of detail of the Configuration Management Database will need to be determined by business needs and the cost (efforts) of maintaining the information
- Without effective automated discovery tools, certain aspects of building and maintaining the Configuration Management Database(s) become very difficult
- CI relationship matrices need to be developed and maintained
- Different types and levels of training will be required for ITSM process roles, especially around CMDB usage

Principle 2:

Each CI has an owner who is responsible for keeping the CI information accurate and current.

Rationale:

- Accurate and current CI information is made available

- Ensures that only authorized changes can be made to the CMDB
- Clear accountability

Implications:

- The CI Owner needs to be notified of all changes made to the owned CIs
- All CI owners, including external service providers, will adhere to the Configuration Management process
- Access policies are required for the CMDB to control what can be changed and who can change it

Principle 3:

Each component (CI in the CMDB) is identifiable by its location, name and relationships to enable the proper management of the environment as a whole.

Rationale:

- All CIs will be easily identified and located and the environment is better controlled
- Verification and audits are facilitated
- Unsupported CIs can be readily identified

Implications:

- Standard CI naming convention needs to be developed, implemented and adhered to
- CIs need to be labeled
- Relationship information, such as parent/child, needs to be recorded and tracked
- For software items and associated documentation, a Definitive Software Library (DSL) needs to be developed and managed by the Release Management process

Principle 4:

A formal CMDB audit is conducted at least once a year.

Rationale:

- Ensures that the CMDB matches closely to the IT environment
- Ensures high level of process compliance

Implications:

- Resources are required to perform the audits
- Automated audit tools are needed to enable checks to be made at regular intervals

since manual operation is likely to be error prone especially when the volume of CIs is high

- Physical audits require travel and physical access to the equipment

Principle 5:

All Service Providers will fulfill their roles in compliance with the OPS Configuration Management process.

Rationale:

- Ensures consistency
- Service providers can play key roles in the process
- Service providers own configuration items

Implications:

- Process provisions will apply to internal and external service providers
- Contracts with service providers must reflect the Configuration Management activities, tasks and linkages associated with their role

Principle 6:

Any changes to CIs tracked in the CMDB must adhere to the Change Management Process.

Rationale:

- Ensures control of all CIs in scope
- Ensures currency and accuracy of CMDB data

Implications:

- Required integration with the Change Management & Release Management Processes
- Significant analysis and planning are required to reach an informed decision on the scope & depth of tracked CI data

3 Portable Process Roles

Each process has specific roles with defined responsibilities for process design, development, execution and management. In an organization, one person can take on multiple roles as per the requirements specific to the organization. This person may choose to delegate these responsibilities to those lower in the hierarchy. Additionally, responsibilities of one role could be mapped to multiple individuals.

Regardless of specific organizational mapping, specific “portable” roles are necessary for the proper operation & management of the process. These roles are required at the Enterprise level and may also be applied at local levels of Configuration Management. This section lists these roles and their responsibilities.

In addition to process roles, service-specific roles may be defined as part of the management and governance structure for a specific service. Other roles will also be involved in the Configuration Management process activities, including other ITSM process roles, operations, and service providers.

One role is accountable for each process activity. The role may assign one or more people who are *responsible* to carry out the task. However, it is ultimately the job of the person who is accountable to ensure that the “job gets done”.

Legend: **R**esponsible, **A**ccountable, **C**onsult Before, **I**nform After

Sub-Process	Configuration Manager	Configuration Coordinator	CI Owner
4.1 - Identify Configuration Items	A	R	R
4.2 - Monitor & Verify CMDB	A	R	I
4.3 - Control & Maintain CMDB	A	R	I
4.4 - Audit CMDB	A	R	C / I

3.1 Configuration Management Process Owner

The Process Owner owns the process and the supporting documentation for the process. The Process Owner provides process leadership to the IT organization by overseeing the process and ensuring that the process is followed by the organization. When the process isn't being followed or isn't working well, the Process Owner is responsible for identifying why and ensuring that required actions are taken to correct the situation. In addition, the Process Owner is responsible for the approval of all proposed changes to the process, and development of process improvement plans.

If the organization does not require the separation of roles (Process Owner and Process Manager), responsibilities listed below should be merged with that of the Configuration Manager role that follows.

Responsibilities

- Ensures that the process is defined, documented, maintained & communicated at a Enterprise and local level
- Reviews effectiveness and efficiency of the Configuration Management process and Identify opportunities for process improvement
- Is responsible for the success or failure of the process and has the authority to represent management on common process definition decisions
- Defines and develops Configuration Management process common metrics and reporting requirements
- Ensures Configuration Management processes and tools integrate with other ITSM processes
- Is responsible for the requirement and guidelines of the Configuration Management tool usage
- Ensures organizational adherence to the process
- Ensures adequate process training is available for the organization
- Manages changes to the process within a defined governance framework. This includes reviewing and approving all proposed changes and communicating changes to all the participants and affected areas

3.2 Configuration Manager

The Configuration Manager is directly responsible for core process deliverables.

In the situation where the activities have been split among a Configuration Manager and Configuration Management Process Owner, the Configuration Manager takes on direct accountability for the day-to-day management of the process and acts as the escalation point for the business users.

Responsibilities

- Ensures that unauthorized CI changes are identified and acted upon
- Escalates to Change Management on unauthorized CI changes or alterations to environment not reflected in CMDB
- Ensures integrity, accuracy and completeness of the CMDB
- Supports effective use of CMDB for other groups and processes
- Requests Change Management report metrics in support of the Configuration Management process
- Produces Configuration Management process metric reports

- Participates in Change Management process evaluation
- Approves structural changes to the CMDB
- Defines access privileges to CMDB
- Monitors Configuration Management process activities and ensures that audits are performed
- Develops, owns and manages the Configuration Management Plan

3.3 Configuration Coordinator / Administrator

The Configuration Coordinator is focused on managing and maintaining the Configuration Management System and the Configuration Management Database (CMDB).

Responsibilities

- Properly identifies and accurately registers CIs
- Identifies unauthorized CI changes, escalates non-compliance issues to Configuration Management
- Creates reports and analyses the CMDB when requested by the Configuration Manager
- Ensures authorized procedures and work practices are followed
- Supports the effective use of the Configuration Management System & database
- Maintains and recommends improvements to facilitate effective use and integrity of the CMDB
- Monitors, verifies and participates in auditing CMDB data
- Participates in the evaluation of the Configuration Management process

3.4 Configuration Item Owner

The Configuration Item Owner is anyone who owns (develops, supplies or supports) a configuration item that will be included in the Computing Environment. This includes Application Development, Database and Infrastructure projects. The CI Owners are the owners of the CI in the CMDB and are measured on the reliability, availability and performance of the CI.

Responsibilities

- Properly identifies and accurately registers CIs
- Maintain the integrity of the relationships of their CIs
- Provides additional information regarding the change when requested by the Configuration Manager/Coordinator

4 Process Flow

4.1 Configuration Management Portable Process Flow

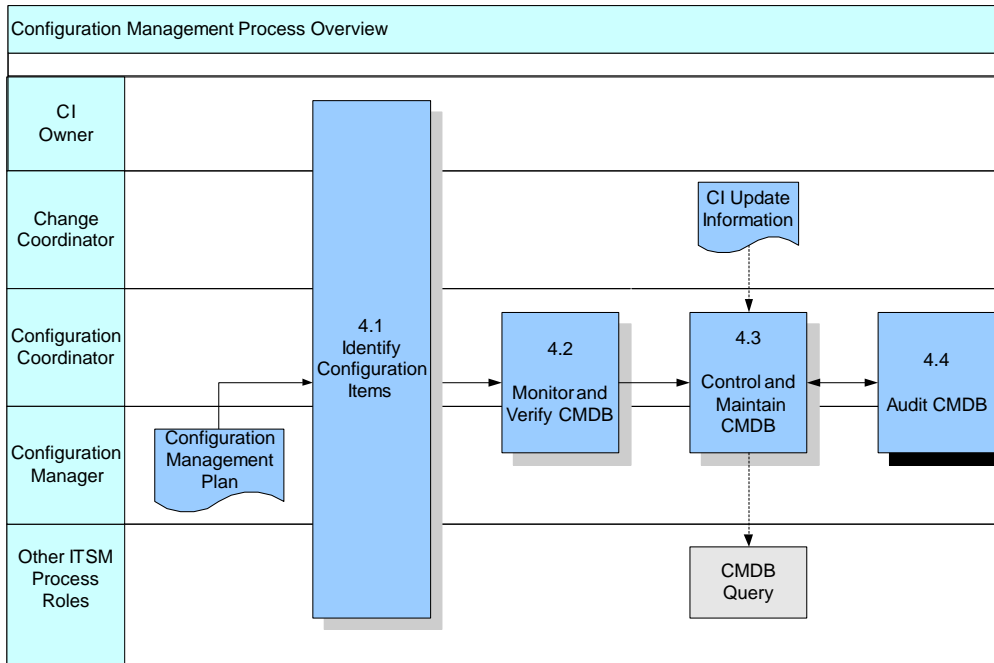


Figure 1: Configuration Management Process Overview

No.	Sub-Process	Input / Trigger	Description	Output / Completion criteria
4.1	Identify Configuration Items	Input: Configuration Management Plan, CI Requirements Discovery Tools	Identification and labeling of CIs to the granularity required – often to the extent of an independently manageable change Identification & recording of CI relationships	CI Owners Identified and Assigned to Each CI, New CIs registered, Updated Configuration Management Plan
4.2	Monitor and Verify CMDB	Input: Auto-discovery Tools, List of CIs to be monitored	Recording of authorized and identifiable CIs in the CMDB upon receipt. Updating of administrative and functional status and relationship information of CIs Ongoing verification of CMDB data.	Warning to Offender, Actions to be taken to ensure Process compliance, Corrective Action Plan to Reconcile CI, Updated CMDB
4.3	Control and Maintain CMDB	Trigger: Notification of Approved RFCs CMDB Data, List of Completed RFCs and Associated CIs, Input: Verified Discrepancies	Control on individual CIs through Change Management Interface	CMDB Updated by new / modified CIs, Defunct CIs removed

No.	Sub-Process	Input / Trigger	Description	Output / Completion criteria
4.4	Audit CMDB	Trigger: Audit Schedule Input: Configuration Management Plan, CMDB Data, Auto-Discovery Tools, Assigned Actions on corrective measures (from Change Management)	Verification of CI with that recorded in the CMDB	Final Configuration Management audit Report distributed within organization, Updated configuration Management Plan

4.2 Configuration Management Process Quality Control

In parallel to the execution of the Configuration Management process, there are activities related to the management of the process to control quality as well as to ensure that the process is both effective and efficient.

Monitoring of the service delivered by the Configuration Management team is performed regularly by the Configuration Manager. This allows the Configuration Manager to answer any questions about service quality as well as ensure that the Configuration Management process is not running into resource or ownership issues. The Configuration Manager is responsible to take corrective actions if bottlenecks are identified in the process.

Reporting involves measuring the process via metrics and recording how well it behaves with respect to its metrics. It provides the Configuration Management personnel with feedback on the process. It provides the Configuration Management Process Owner with the necessary information to review the process performance and initiate required improvements.

Evaluating the process involves regular reviews of the performance of the process and identification of possible improvements or actions to address performance gaps. Every process is only as good as its last improvement; hence, the feedback loop of continuous improvement is inherent in every process.

5 Common Process Metrics

Metrics are intended to provide a useful measurement of a process effectiveness and efficiency. Metrics are also required for strategic decision support. The following need careful consideration:

- Reporting metrics should be readily measurable (preferably automated collection and presentation of data)
- Metrics need to be chosen to reflect process activity (how much work is done?), process quality (how well was it done?) and process operation (to review and plan job on hand). Depending upon the needs of the organization, metrics can be classified as “hard (must have)” or “soft (desirable)”
- Hard metrics will be common across an organization

The following common metrics are suggested for the Configuration Management process:

- Number and percentage of CI discrepancies
- Number and percentage of CIs tracked within the CMDB
- Number and percentage of CIs added/deleted by category
- Percentage of CI's with stale audit dates
- Total configuration management effort in person-hours

6 Standard Process Parameters

Parameters used for the categorization and definitions of CIs require a certain level of standardization across OPS. Special attention needs to be given to parameters related to consistency of reporting. This is particularly important for the provision of reliable business intelligence.

Component Category (formerly Product Category) is a parameter used across Incident, Problem, Change and Configuration Management. To ensure consistency of meaning and usage it has been defined in the Terminology Reference Model. Please refer to the Classification Model section of the GO-ITS 44 ITSM Terminology Reference Model Portable Guide for standard process parameters and allowable values for **Component Category**.

See Appendix B for draft Standard Process Parameter Allowable Values.

Errata

Created: February 27, 2004

Updated: August 9, 2004

Updated: September 21, 2004

- Approved by the Architecture Review Board (ARB) as a Government of Ontario Information Technology Standard (GO-ITS). Version number reset to 1.0 for approved this approved version.

Document Numbering

Document No: GO-ITS 36
Title: Configuration Management OPS Portable Process Guide
Month Year: September 2004
Doc. Type: Microsoft Document
File Name: GO-ITS 36 Configuration Management Portable Guide V1.0.doc

Copyright

© Queen's Printer for Ontario 2004.

Appendix

A. Process Variances from OPS V2.3 Process Guides

The following tables provide the detail of the specific variances from the previous OPS guides with respect to principles, roles and responsibilities, and process flow. As noted in the introduction, the purpose of these new guides is to provide the portable elements needed to be common across the OPS. As such, some principles, responsibilities, and aspects of the process flow were too specific to apply across the OPS.

Table 1 - Configuration Management Principles

Portable Process Guide (2004)	OPS Standard Process Guide (2001)		Same	Modified	New	Removed	Explanation
	Principle No.	Section No.					
1	5.2	1		X			Refers to "IT environment" instead of "Production environment"
2					X		Added for clarity
3	5.10	1		X			Made more concise with respect to CI requirements
4					X		ITSM best practice
5	5.15	1,2	X				This Principle replaces all External Contractor & Service Provider policies
6	5.14	1,2,3			X		This Principle replaces all release and version control policies
	5.2	2				X	Not required: The environment, as a whole, exists at the Enterprise Level (Federal level) of Policy.
	5.3	1				X	Part of Roles and Responsibilities: Release to Production is controlled by the Change / Config Manager(s), who are responsible for the reliability of the computing environment and who will enforce the Change and Configuration Management Process.
	5.3	3				X	Not required: The Configuration Management Process is controlled by the Configuration Manager.
	5.4	1				X	Procedural: Projects create, enhance or maintain a CI within the context of the environment, where a CI is a line item on the CMDDB.
	5.5	1				X	Part of Release Management: CIs (Applications and Infrastructure Systems) will be developed or purchased and released in accordance with an agreed upon "Standard Systems Development Lifecycle".
	5.10	2				X	Procedural: CIs (Applications) must be stored in a Corporate secured system, not on personal storage devices.
	5.12	1				X	Not required: All Releases will be activated in the Definitive Software Library, until there is no longer any possibility of a Business Unit needing to recreate the old release.
	5.13	1				X	Not required: All Platform Development will use the same configuration
	5.15	1				X	Part of Release Management: All External Contractors will supply versioned documentation that will conform to the requirements as specified in the organization System Development Lifecycle Document.
	5.15	3				X	Unenforceable: All External Contractors who own CIs will have an organizational resource also assigned to the CI to ensure the contractor follows the process.

* PLEASE NOTE: In the OPS Standard Process Guides (2001), policies were not originally numbered. To identify them for comparison, they have been assigned numbers here according to the order in which they appear in their section of the Guide.

Table 2 - Configuration Management Roles

Portable Process Guide (2004)	OPS Standard Process Guide (2001)		Same	Modified	New	Removed	Explanation
	Section No.	Role					
Configuration Management Process Owner	3.1.4	Process Owner			X		Added to clearly reflect the responsibilities around process definition, support and evolution
Configuration Manager	4.3	Configuration Manager - Enterprise Level		X			Previously roles at Enterprise and CI level were identified separately Additional responsibilities: - Ensure that (annual) audits are performed
	4.4	Configuration Manager - CI Level					Removed responsibilities: - Authorizes move of CI to the Definitive Software Library for Release to Production; - Ensures all components relative to IT Service Levels are registered;
Configuration Coordinator / Administrator	4.6	Configuration Co-ordinator (Optional)		X			No longer an optional role. Additional responsibilities: - Identify unauthorized CI changes, escalate non-compliance issues to Configuration Management - Maintain and recommend improvements to facilitate effective use and integrity of the CMDB - Participate in auditing CMDB data Removed responsibilities: - Maintain the Enterprise configuration CI dependency matrix database - Ensure Service Providers maintain adequate Config Mgmt Process disciplines and systems for their CIs - Review all test results against the Quality Plan
	4.8	Business Unit Manager				X	Removed as not a role specific to Configuration Management
CI Owner	4.9	Service Providers		X			CI Owner fulfills the role of Service Providers
	4.10	Operations / Production Control Function				X	Removed as not a role specific to Configuration Management

Table 3 - Configuration Management Process

Portable Process Guide (2004)	OPS Standard Process Guide (2001)		Same	Modified	New	Removed	Explanation
	Section No.	Process					
(4.1) Identify Configuration Items	4.2.1.1	Identification of Enterprise Configuration Items		X			<ul style="list-style-type: none"> - Process has been generalized to eliminate distinction between enterprise level CMDB and CI level CMS. - Process flow now involves Configuration Coordinator as well as Configuration Manager. - Change Coordinator provides the interface to other Processes
	4.2.2.1	Identification of CI Level Configuration Items					
(4.2) Monitor and Verify CMDB	4.2.1.2	Monitor and Verify the CMDB		X			<ul style="list-style-type: none"> - Process has been generalized to eliminate distinction between enterprise level CMDB and CI level CMS. - Process flow now involves Configuration Coordinator as well as Configuration Manager.
	4.2.2.2	Monitor and Verify the CI Level CMS					
(4.3) Control and Maintain CMDB	4.2.1.3	Control and Maintain the CMDB		X			<ul style="list-style-type: none"> - Process has been generalized to eliminate distinction between enterprise level CMDB and CI level CMS. - Process flow now involves Configuration Coordinator as well as Configuration Manager. - Change Coordinator provides the interface to other Processes
	4.2.2.3	Control and Maintain the CI Level CMS					
	4.2.1.4	Report Metrics				X	Removed as not required for portable guide
	4.2.2.4	Report Metrics				X	Removed as not required for portable guide
(4.4) Audit CMDB	4.2.1.5	Verification Process		X			<ul style="list-style-type: none"> - Process has been generalized to eliminate distinction between enterprise level CMDB and CI level CMS. - Process flow now involves Configuration Coordinator as well as Configuration Manager.
	4.2.2.5	Verification Process					
	4.2.1.6	Evaluate Process				X	Removed as not required for portable guide
	4.2.2.6	Evaluate Process				X	Removed as not required for portable guide

B. Standard Parameter Allowable Values

Component Category

It is recommended that a multi-level tree be used with the top two levels standardized across OPS and the lower levels subject to localization. Because the top level is used across Incident, Problem, Change and Configuration Management standard definitions have been defined in the Terminology Reference Model. Please refer to the Classification Model section of the GO-ITS 44 ITSM Terminology Reference Model Portable Guide for standard process parameters and allowable values for **Component Category**.

The following are the values for the top level as per the Terminology Reference Model:

- Application
- Data
- Documentation
- Support Software
- Hardware
- Network
- Non-Production Environment
- Process
- Standards
- Facilities

CI Status

The following are the recommended values:

Status	Description
Planned	The CI (or this version of it) is currently being procured, built, and/or developed and is planned to be put into the production state in the future.
Production	The CI exists and is functional within the production I&IT infrastructure. This is the “normal” state for most CI’s in the CMDB.
Out-of-Service	The CI is not working or unavailable for a prolonged period of time. (Note – it is not the intention to modify the CI status for short-term service outages).
Decommissioned	The CI (or this version of it) is no longer supported within the production IT infrastructure.

C. Process Localization Guidelines

Portable guide content applies to all organizations and groups within OPS. Localization involves adding group-specific information that applies to a particular organization or group. For every group, local content will focus on what's important for the particular environment.

Local content is expected to evolve significantly as the processes are adopted and as more detailed requirements emerge.

The Portable guide content will always apply to all localizations; the local guides are expected to be more granular and organization specific.

Localization Principles

- ITIL & ITSM represent our reference frameworks for guidance on best practices
- Current practices will be considered to the extent that this does not jeopardize the long-term vision of an integrated set of ITSM processes and tools
- Deployment will focus on the short term but design on the long term
- Interrelationships with other ITSM processes will always be considered

Local Process Guide Content

- All Portable guide content plus:
- Local Operational Principles, Guidelines & Standards (if required)
- Local Process Roles and Responsibilities
- Local RACI Charts
- Local Process Activities (such as Escalation)
- Local Reporting Metrics

Glossary

A glossary of terms used in this guide is provided below:

Term	Description
Asset Management	A standard accounting process concerned with maintaining the details of assets above a specified value, including depreciation, lease agreement information, expected life, etc. Asset management does not track the relationship between assets and may not track each individual item purchased or leased as part of a "bundle" purchase. (For example, asset management would track the fact that 100 personal computers were purchased, but would not track the individual units.) Configuration Management would typically track the individual PCs.
Availability	Ability of a component or service to perform its required function at a stated instant or over a stated period of time. Generally, availability is expressed as the availability ratio, which is the proportion of time that the service is actually available for use by the Customers within the agreed service hours.
Availability Management	A process that focuses on understanding and managing availability requirement of the business.
Change Advisory Board (CAB)	An advisory committee that provides expert advice to the change manager on change issues
Change Advisory Board Emergency Committee (CAB/EC)	A subset of the CAB that is always available to be called upon to address urgent change issues
Capacity Management	A process that aims at ensuring that the capacity of the IT infrastructure matches current and future requirements of the business.
Category	Classification - possibly based on nature of event.
Change	Any modification – addition or removal of approved, supported or base lined hardware, network, software, application, environment, system, desktop build or associated documentation.
Change Management	Process of implementing Changes to the infrastructure or any aspect of services, in a controlled manner, enabling approved Changes with minimum disruption to service.
CI (Configuration Item)	Component of IT infrastructure or a related item under the control of Configuration Management.
Configuration Baseline	A snapshot of the IT Infrastructure as recorded in the CMDB. Although the snapshot may be updated later, as changes are applied to CIs, the baseline remains unchanged and available as a reference of the original state and as a comparison against the current state.
Configuration Management	A process for identifying, recording, auditing and reporting on the CIs for accuracy and completeness.
Configuration Management Database (CMDB)	A database containing the relevant details of each CI and details of the important relationships between CIs.

Term	Description
Configuration Management Plan	Document describing the organization and procedures for the Configuration Management of a specific project, product, system, support group or service.
Contingency Planning	The preparation to address unwanted occurrences that may happen at a later time. Usually, the term has been used to refer to planning for the recovery of IT systems rather than entire business processes.
Continuity Management	A process that supports the Business Continuity process to ensure that IT Services are recovered within agreed time scale.
Crises Management	An occurrence and / or perception that threatens the operations, staff, shareholder value, stakeholders, brand, reputation, trust and / or strategic / business goals of an organization.
Customer	Recipient of a service, responsible for funding the service against business requirements.
Customer Management	Customer Management process establishes and maintains links between executive business managers and the IT services organization.
Definitive Hardware Store (DHS)	Definitive Hardware Store. An area that is aside for the secure storage of definitive hardware spares.
Definitive Software Library (DSL)	Definitive Software Library. A secure software library where all versions of accepted software configuration items (CIs) are held in their definitive, quality-controlled form.
Disaster recovery planning	Set of processes that focus only on the recovery processes, mainly in response to the physical disasters, which are contained within BCM.
End User (or User)	The individual who uses the service on a day-to-day basis.
Forward Change Schedule	A schedule of all approved changes and their planned implementation dates for a pre-specified period.
Impact (For Incident)	Measure of scope and criticality to business.
Incident	An event that negatively impacts the standard delivery of a service, or a service request
Incident Management	A process that is committed to restoring normal service operations as documented in Service Level Agreements as well as processing service requests.
IT Service Delivery	IT Service Delivery processes (Availability Management, Capacity Management, Continuity Management, Financial Management and Service Level Management) address from a design and management perspective the service that business requires of the provider.
KDB	Knowledge database. A database of solutions and workarounds that is used by front line support staff to restore normal Service operation.
Known Error	An incident or Problem for which the root cause is known and for which a temporary Work-around or a permanent alternative has been identified. If a business case exists, an RFC will be raised, but, in any event, it remains a known error unless it is permanently fixed by a change.
Maintainability	Describes the ability of the Internal IT groups to maintain the services via the management of IT infrastructure components or services. Managed through OLAs.

Term	Description
Mean Time Between Failures (MTBF)	Expected future performance based on the actual past performance of a population of units. Calculated as: $(MTBF = \text{total actual operating time} / \text{total number of failures})$.
Mean Time To Repair (MTTR)	Average amount of time it takes to repair a component. MTTR typically includes time from when the unit failed until replaced, thus including hardware unavailability, response time, travel time, and on-site repair time.
Metric	A measurable element of the service process or function.
Operational Level Agreement	An internal agreement covering the delivery of services, which support the IT organization in their delivery of services.
Operational Test Environment	A test environment that is directly used by customers or end-users as part of the IT services they receive.
Operations Management	A process that consists of all activities and measures necessary to enable and maintain the intended use of IT services and production environment.
Post Implementation Review	A review for verification of correct implementation of change by authorized personnel.
Priority	Relative order in which a given event needs to be addressed. This usually depends on Impact and Urgency.
Problem	An unknown underlying cause which could or has caused disruption of service.
Problem Management	A process that minimizes the effect of errors in infrastructure / services and external events on the customers. It is a process focused on diagnosing and rectifying faults in the IT infrastructure to obtain the highest possible IT service stability.
Procedure	A set of specific steps that describe how an activity should be carried out, and by whom. Procedures may be supported by more detailed Work Instructions. A Process defines what is to be achieved; Procedures define how the objectives are to be achieved.
Process	A series of related activities aimed at achieving a set of objectives (or Principles) in a measurable, usually repeatable, manner. It will have defined information inputs and outputs, will consume resources and will be subject to Management controls over time, cost and quality. It will also balance benefits against risks.
Process Owner	The Process Owner is the person involved in the project with regard to process design and / or re-engineering efforts.
Production environment	A subset of IT infrastructure that participates in delivery of Service.
RACI Matrix	RACI diagrams are tools used to map activities to roles and define how roles contribute to an activity.
Release	A collection of new or changed CIs.
Release to Production	The HP ITSM process, which controls the release of changes in the production IT Infrastructure. It is a component of the ITIL Release Management Process.
Reliability	The service or IT infrastructure Configuration Item (CI) is available when expected / as defined in the SLA. It can also be described as freedom from failure. It is expressed in terms of MTBF - average uptime.

Term	Description
Request for Change (RFC)	Form, or screen, used to record details of a request for a change to any CI within an infrastructure or to procedures and items associated with the infrastructure.
Resilience	Degree redundancy of a CI with the intent of eliminating single points of failure in the infrastructure.
Security Incidents	Security incidents are those events that cause damage to confidentiality, integrity or availability of information or information processing and materialize as accidents or deliberate acts.
Security Management	Security Management is the process of managing a defined level of security on information and IT services, in addition to managing the response and effect of security incidents.
Service achievement	The actual service levels delivered by the IT organization to a customer within a defined life span.
Service Build and Test	Service Build & Test process develops, tests and documents new Services and enhancements & fixes to an existing Service.
Service Catalogue	Written statement of IT services, default levels and options.
Service Delivery	Processes that address Service Management from a design and management perspective.
Service Desk	Single point of contact between Service Provider and the users of the Service.
Service Improvement Program	A formal project undertaken within an organization to identify and introduce measurable improvements within a specified work area or work process.
Service Level Agreement (SLA)	Written agreement between a service provider and the Customer(s), that documents agreed Service Levels for a Service. The scope of an SLA covers the target environment to be serviced, specific IT service deliverables, service functionality, service coverage (e.g., level, hours, availability, responsiveness, restrictions, authorizations, etc.), security policies, and cost of the services being provided.
Service Level Management	A process that defines Service levels agreed with customer and subsequently manages at an acceptable cost.
Service Level Objective (SLO)	A defined target for a service metric, usually specified in an SLA.
Service Management	Management of Services to meet the Customer's requirements.
Service Planning	The Service Planning process designs, develops and controls Service Plan required for service development. This plan will describe scope, functional requirements and required components for service implementation that aids in determination of service ROI along with decisions like "Buy Vs Build".
Service provider	Third-party organization supplying services or products to customers.
Service quality plan	The written plan and specification of internal targets designed to guarantee the agreed service levels.
Service Request	Every Incident not being a failure in the IT Infrastructure, such as requesting information or moving equipment.
Serviceability	Describes the external contracts or Underpinning Contracts (UCs) that exist with suppliers that are required to deliver

Term	Description
	service.
Services	The deliverables of the IT Services organization as perceived by the Customers; the services do not consist merely of making computer resources available for customers to use.
Underpinning contract	A contract with an external supplier covering delivery of services that support the IT organization in their delivery of services.
Urgency	Measures how quickly an event needs to be addressed.
User	Person who uses services on a day-to-day basis.
Workaround	Restoring service by application of temporary fix or routing service to the customer via another channel.
Workgroup	An organizational or logical unit of individuals with similar specialization and responsibilities

References

- OPS Standard Change & Configuration Management Process Guide version 2.3 (last updated in March, 2001).