Critical Patch Management: Getting the Process Right

David Pultorak

Principal Consultant
Pultorak & Associates, Ltd.

HP WORLD 2003
Solutions and Technology Conference & Expo

How to reach Pultorak

Pultorak & Associates, Ltd.
9335 Stenton Avenue, Suite 100
Erdenheim, Pennsylvania USA 19038
(215) 233-1205 Office
(215) 233-1206 Fax
info@pultorak.com
www.pultorak.com

The Point

- While the right tools are critical, starting with the right processes—industry standard processes based HP's ITIL-based ITSM Reference Model—is the surest path to bringing order, efficiency, and demonstrable effectiveness to patch management within your organization

Agenda

- Overview of the IT Infrastructure Library
- Hewlett-Packard’s ITSM Reference Model
- Key processes within Patch Management
- Practical guidance on implementation
- Where to got for more information
- Q&A

The IT Infrastructure Library (ITIL)

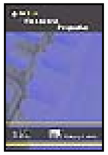
Service Support

Service Delivery

Infrastructure Management

Application Management

Planning to Implement

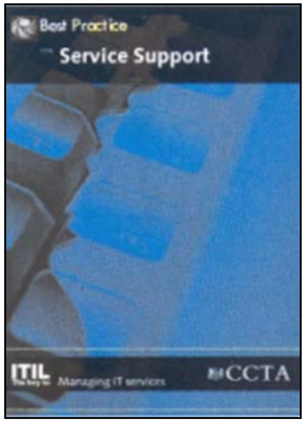

The Business Perspective

Other publications:

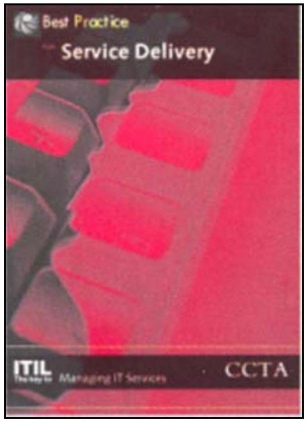
The itSMF ITIL pocket guide is ITIL service support and delivery in capsule form

The ITIL Security Management publication. Other ITIL publications refer to it, rather than include, its guidance

ITIL Service Management processes, Service Desk function



- Service Desk function
- Incident Management
- Problem Management
- Configuration Management
- Change Management
- Release Management



- Service Level Management
- Financial Management
- Capacity Management
- IT Service Continuity Management
- Availability Management

The IT Infrastructure Library (ITIL)

- The worldwide de facto standard for IT service management, generally accepted as best practice
- Non-proprietary and platform-independent
- Flexible—intended to be adapted

What is the HP ITSM Reference Model?

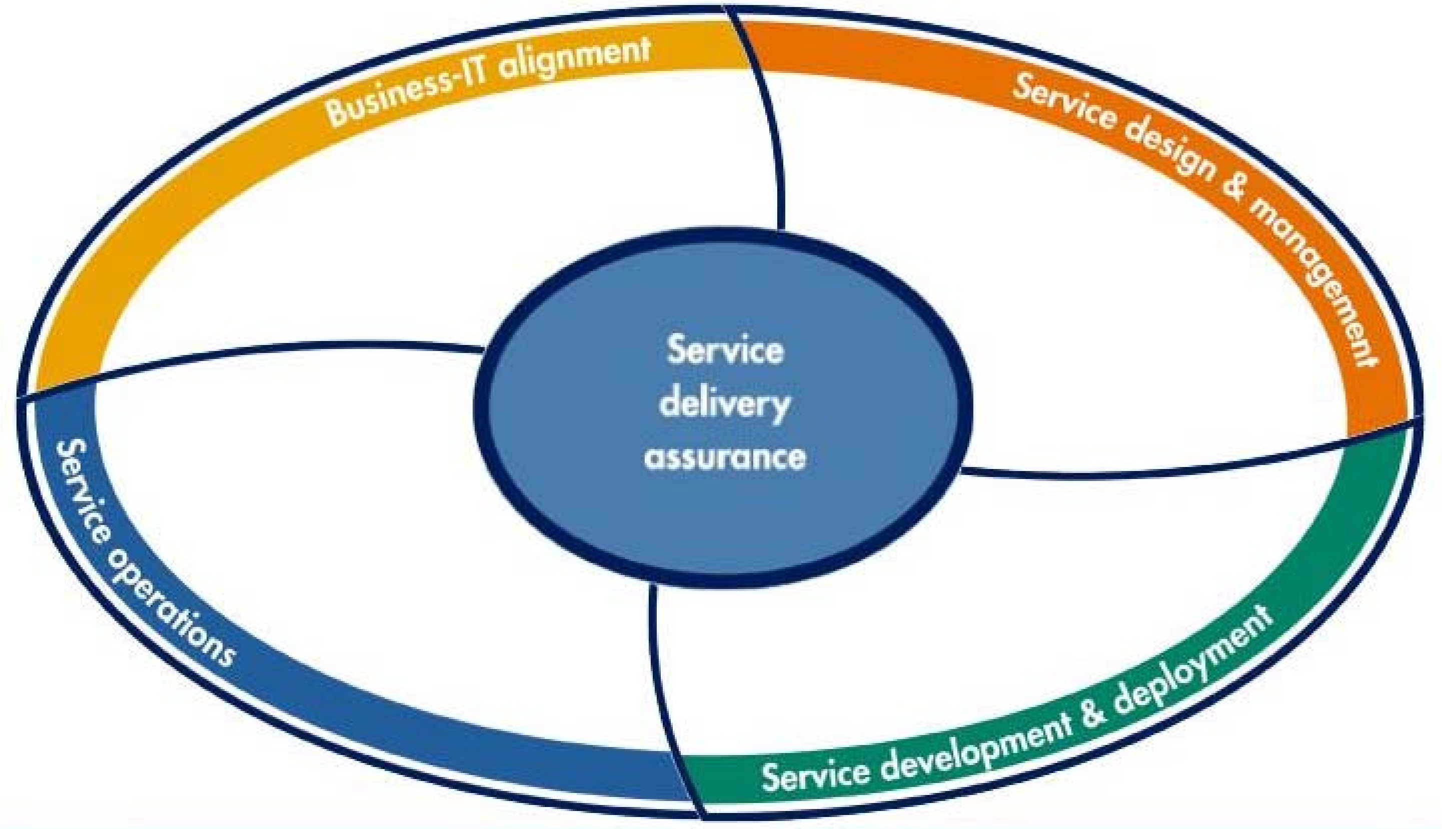
- Based on proven best practice guidance (ITIL) and experience of Hewlett-Packard consultants
- Integrated, high-level IT process relationship map
- Coherent representation of IT processes underpinned by a common language
- Tool for corporate IT organizations to:
  - Understand how people, process, and technology relate
  - Have meaningful dialogue on IT process requirements and solutions

How the HP ITSM Reference Model Builds on ITIL

- Adds prescriptive guidance for HP technologies drawn from HP ecosystem
- Can be used for all platforms in enterprise IT
- Add Operations Management guidance
- Breaks out Build and Test from Release
- Security on its own, ITSCM under Availability
- Supported by HP and Partner services and process-enabling technologies
- Some guidance freely available, some only with services or support contract
- Education and consulting services available

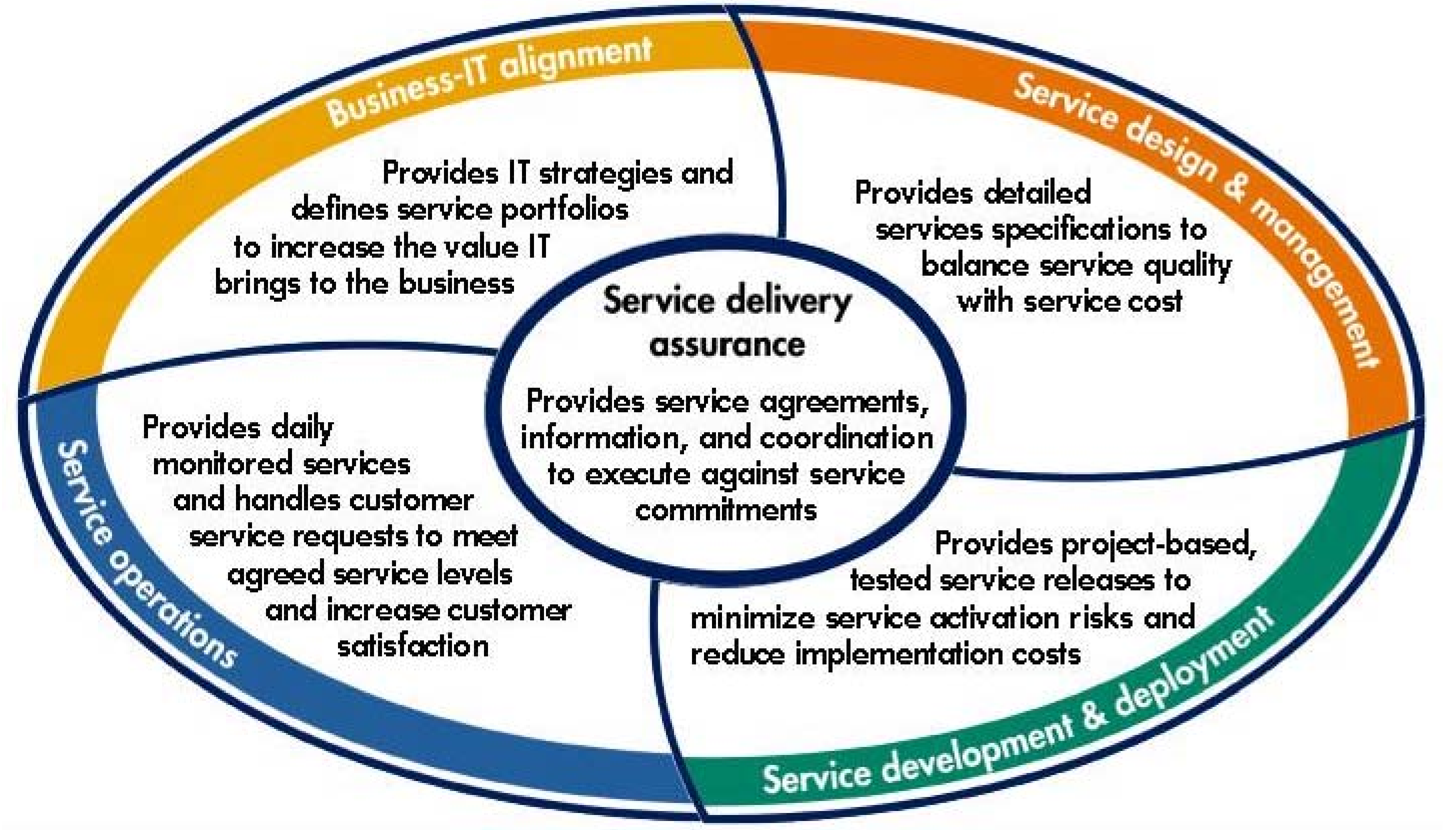
HP ITSM Reference Model

Version 3.0


Business-IT alignment
Service design & management
Service delivery assurance
Service operations
Service development & deployment

HP ITSM Reference Model

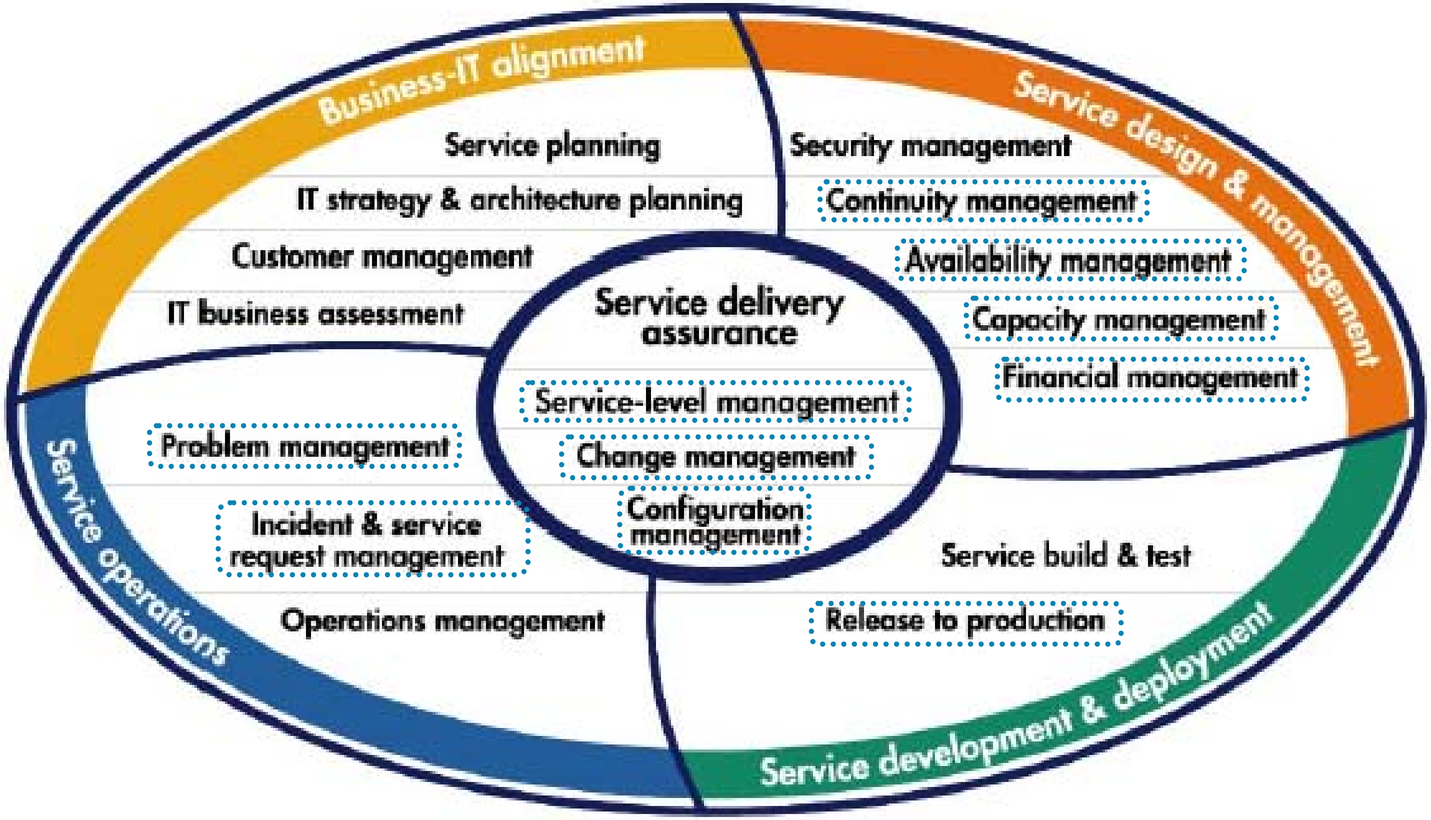
Goals



Business-IT alignment
Provides IT strategies and defines service portfolios to increase the value IT brings to the business
Service design & management
Provides detailed services specifications to balance service quality with service cost
Service delivery assurance
Provides service agreements, information, and coordination to execute against service commitments
Service operations
Provides daily monitored services and handles customer service requests to meet agreed service levels and increase customer satisfaction
Service development & deployment
Provides project-based, tested service releases to minimize service activation risks and reduce implementation costs

HP ITSM Reference Model

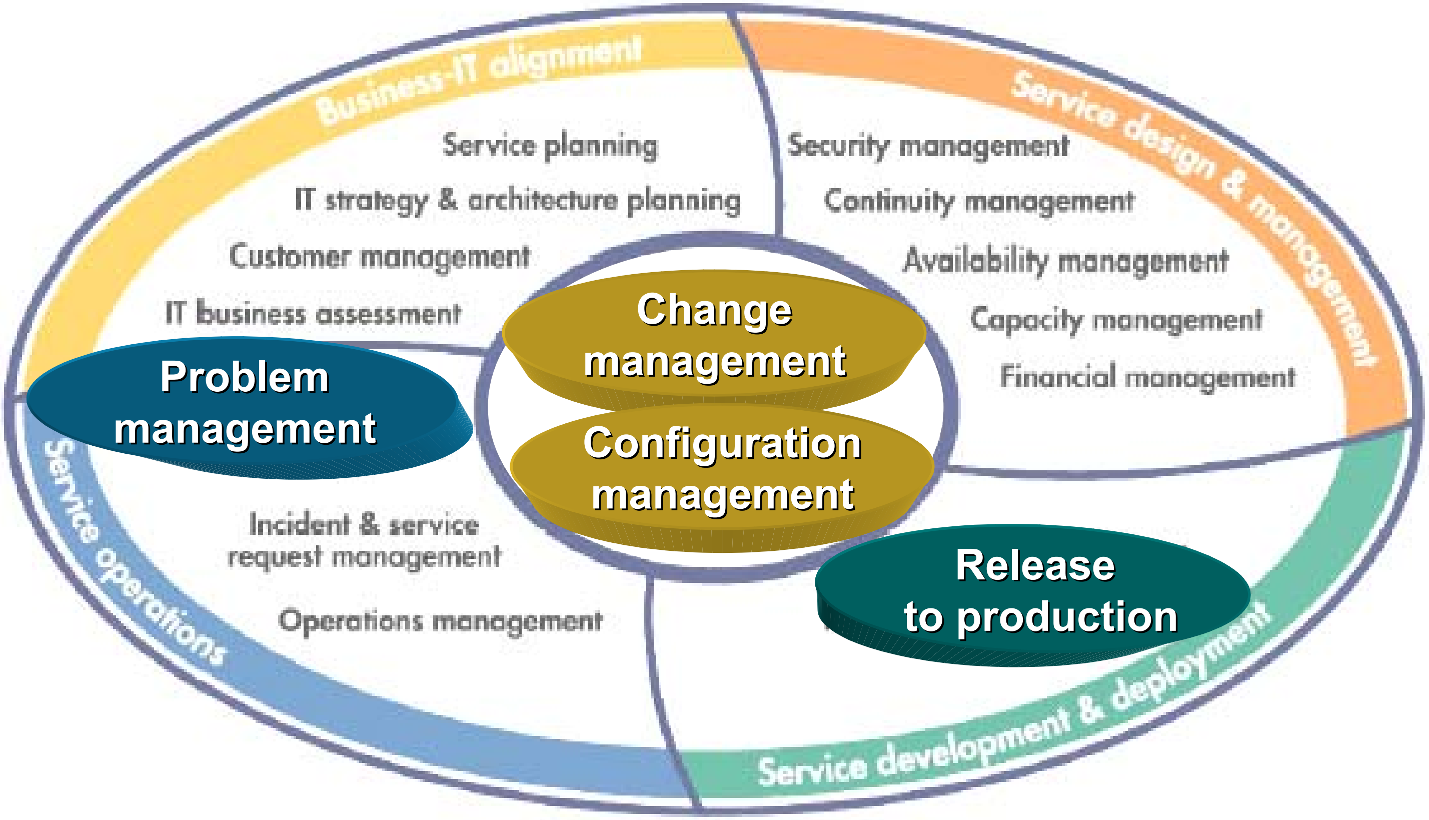
Processes



Circled processes map to ITIL Service Management

HP ITSM Reference Model

ITSM processes used in Patch Management



Plus **Patch evaluation**

Patch Management Process

- Goal:
  - Prevent adverse business impact of malicious code and software vulnerabilities by:
    - ☑ maintaining infrastructure in a known, controlled state
    - ☑ maintaining an effective mechanism for deploying and confirming deployment of urgent and routine patches
    - ☑ applying relevant patches to maintain code levels to a predefined and agreed process and schedule
    - ☑ In regulated environments, provide documented evidence that patches are being applied according to the predefined process and schedule

Patch Management Process

Patch Evaluation

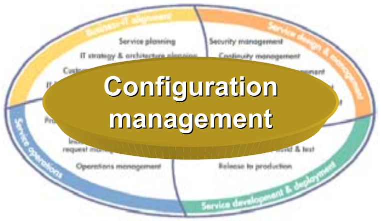
- Goal:
  - Ensure new patches are quickly reviewed and a decision made about whether to proceed with deployment
- Activities:
  - Monitor new patches
  - Review patch relevance
  - Assign patch urgency
  - Verify patch authenticity

Patch evaluation
Business-IT alignment
Service planning
IT strategy & architecture planning
Service design & management
Security management
Continuity management
Service operations
Operations management
Service development & deployment
Release to production
Build & test

Patch Management Processes

Configuration Management

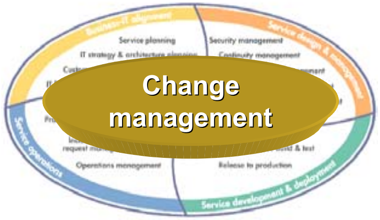
- Goal:
  - Maintain an up-to-date logical record of infrastructure components including how those components relate to one another
- Activities:
  - Define and maintain Configuration Items (CIs)
  - Report Configuration Management Database (CMDB) data
  - Verify CMDB data



Patch Management Processes

Change Management

- Goal:
  - Minimize business disruption caused by changes and ensure a record of what changed
- Activities:
  - Process Requests for Change (RFC)
  - Assess impact
  - Approve Changes
  - Schedule and coordinate Changes
  - Coordinate recovery from Change failures
  - Manage Urgent Changes



Patch Management Processes

Release to Production

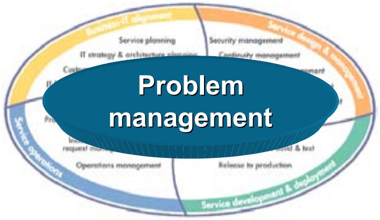
- Goal:
  - Assure the success of releases through consistent release policies, practices, and tools
- Activities:
  - Procure resources
  - Assemble and distribute service components
  - Implement service support / control mechanisms
  - Implement service components end-to-end
  - Perform software administration
  - Perform testing

Business-IT alignment
Service planning
IT strategy & architecture planning
Security management
Continuity management
Service design & management
Service operations
Operations management
Build & test
Release to production
Service development & deployment
Release
to production

Patch Management Processes

Problem Management

- Goal:
  - Ensure that errors in the infrastructure are known and that something is being done to address them
- Activities:
  - Log Problems
  - Identify root causes
  - Track Problem solution progress
  - Verify and control Known Errors
  - Resolve and close Problems and Known Errors



Patch Management Process Variants

Variant #1: The Emergency Process

- Used to deploy patches of high urgency—those that address a vulnerability with high risk of immediate exploitation
- Used on an as-needed basis
- Leverages emergency Change request and approval process

Patch Management Process Variants

Variant #2: The Standard Process

- Used to deploy patches of normal urgency
- Follows a predetermined patch release schedule (e.g., quarterly, semi-annually)
- Leverages normal Change request and approval process

Patch Management Process SLAs

Example: Server Operating System

	Patch Evaluation Complete	Quarantine Complete	RFC Submitted	RFC Processed	Release Ready	Deployment Confirmed (90% Saturation)
EMERGENCY PROCESS (Critical Patches)	2 hours	1 hour	1 hour	1 hour	3 hours	24 hours
Standard Process (Non-Critical Patches)	2 days	2 days	2 days	7 days	30 days	30 days

Patch Management Processes

Process Metrics and Performance Measurement

Measure	Using these Metrics	Why it's Important
Patch Statistics	▪ Patches Screened by Period ▪ Patches Deployed by Period ▪ Patches by Category by Period ▪ Patches by Platform by Period	▪ Captures overall volume ▪ Highlights trends in types of patches and platforms
Process Cycle Time	▪ End-to-End Process Cycle Time ▪ Sub-process cycle time	▪ Helps identify weak points or potential bottlenecks in the process ▪ Useful if process is managed to specific cycle time targets
Deployme nt Quality	▪ Counts and Percentage of successful patch deployments in a given period	▪ Helps identify technical problems in deployment

Patch Management

Considerations and Keys to Success

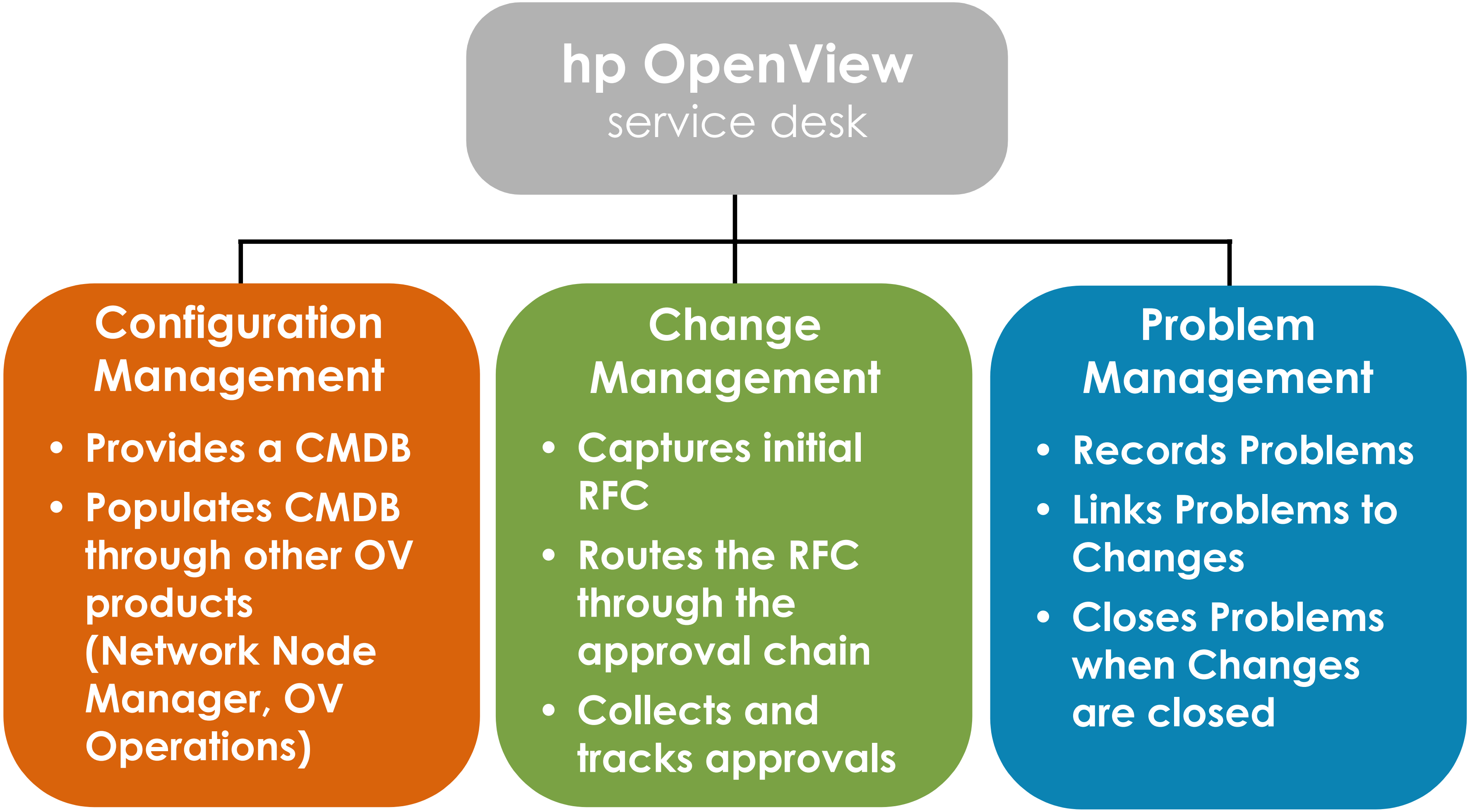
- Evaluate quickly to avoid a backlog and enable rapid deployment (if needed)
- Distribute evaluation responsibility by platform (e.g., HP-UX, Windows Server, etc.)
- Don’t rely on vendor urgency classifications—too many patches are classified as “critical”
- Log all patches, regardless of relevance—maintain records of total patches evaluated, total deployed, and reasons for not deploying
- Use a Release schedule to routinely batch up and apply all non-critical relevant patches

Remember the Point?

- While the right tools are critical, starting with the right processes—industry standard processes based HP's ITIL-based ITSM Reference Model—is the surest path to bringing order, efficiency, and demonstrable effectiveness to patch management within your organization

Patch Management Tools

OpenView Service Desk and Patch Management



hp OpenView
service desk

Configuration Management

- Provides a CMDB
- Populates CMDB through other OV products (Network Node Manager, OV Operations)

Change Management

- Captures initial RFC
- Routes the RFC through the approval chain
- Collects and tracks approvals

Problem Management

- Records Problems
- Links Problems to Changes
- Closes Problems when Changes are closed

Where to go for more information

HP ITSM Reference Model	www.hp.com/hps/itsm
ITIL	www.itil.co.uk
OpenView Service Desk	www.openview.hp.com/products/sdesk

HP WORLD 2003

Solutions and Technology Conference & Expo

Interex, Encompass and HP bring you a powerful new HP World.

interex
shared knowledge • shared power

encompass
AN HP USER GROUP

hp
invent