



A Use-Case of Digital Transformation through VeriSM™

(The integration of the ServiceNow CMDB into Patch Management Operations)

By Richard Kroh

A Use-Case of Digital Transformation through VeriSM™

(The integration of the ServiceNow CMDB into Patch Management Operations)

Introduction

In this use case, an experienced career-long ITSM practitioner describes the value of VeriSM™ as it's applied to a specific intent. The interesting part of this is that VeriSM™ was not applied prior to inception of the effort but was inserted after its completion. It illustrates and overwhelmingly acknowledges, the value and impact of taking a VeriSM™ approach to all things service management, no matter how large and general or how small and specific.

About the Author

Richard Kroh has been utilizing varying degrees of the ITIL framework concurrently with combinations of ITSM tools, most recently being ServiceNow. While growing his career in IT Service Management, some roles included managing hybrids of help desk/desktop/remote support teams, system upgrade/ migration/infrastructure project management, engagement management and most recently ITSM consulting.

While his interests have always been the provisioning of IT services, mainly focusing on customer support, his underlying drive has been service improvement through studying and evaluating the interactive properties and outputs of not only frameworks, approaches and ITSM tools, but most importantly, the human dynamics behind each.

He was compelled to write about VeriSM™ only after he had completed a recent itSMF initiative, at which he was presented VeriSM™ by Doug Tedder.

Digital Transformation or Not

While the big buzz these days is around digital transformation, many firms plan for major service improvements by purchasing major ITSM toolsets and expect their output to magically improve. What they're missing is truly understanding how their human components currently function and enmesh with their existing toolsets. They are not taking the time to evaluate specific processes that surrounds a suspect output.

Across the various interpretations of Digital Transformation, my take on it is a company's ability to align its human components to maximize their service management capabilities to a mature enough level to capitalize on their business product. This includes the business products that are both IT and non-IT driven.

In this use case, we're integrating an existing component of ServiceNow into an existing ITIL transition operational lifecycle component. Basically, we are taking existing tools and people and applying an approach to develop their capabilities and bridge them together as a repeatable and sustainable process. As for the approach, the previously assumed premise is that we utilize characteristics and components of one methodology like Agile, Lean, etc., where VeriSM™ allows for varying components and degrees of each and does not force one or another exclusively. Direct components and activities of this use case are overlaid onto the components of VeriSM™, the Management Mesh, Governance, portfolio & principles and the Operating Model.

Problem Statement

- Inability to ensure 100% transparency into Windows, Linux and Solaris server environments.

Initiative Intent

- Integrate the ServiceNow CMDB into the Patch Management Life cycle

Intended Outcome

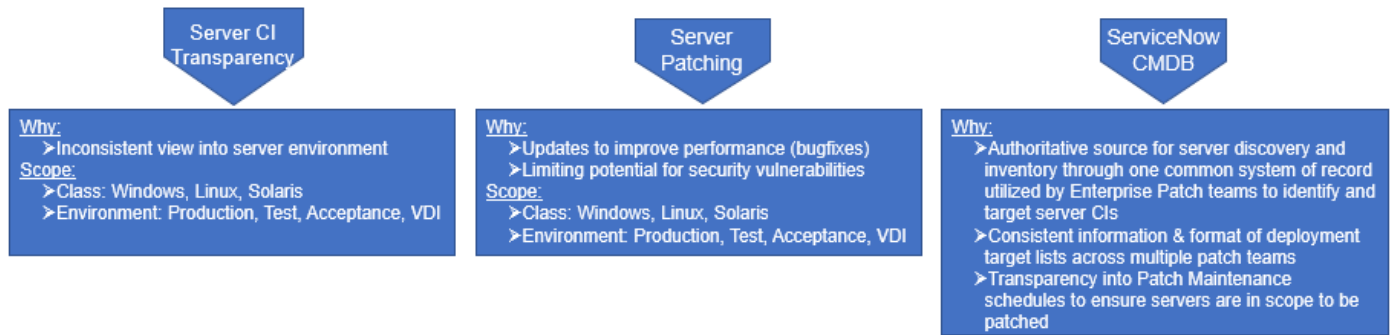
- Increase server CI transparency to enable proactive capability to identify and ensure all patch targets are identified.
- Utilize the ServiceNow CMDB as Patch Management's authoritative source of configuration item inventory.

Approach

- Introduce and gain buy-in from senior management



- Illustrate the “whats” and “whys” when introducing the initiative.



Data Collection

The VeriSM™ Management Mesh uses “Resources” as one “edge” of the mesh. This collected data represents “As Is” data to be used as part of Gap Analysis activity later in the initiative.

A major part of implementing a solution in and around current operational processes is to map and document the current mode of functionality. This includes people, processes and technology across their current framework and structure. To collect this information, interview operational staff, collect all currently utilized means of tooling, data (spreadsheets, change controls, scheduling), success/failure criteria, etc. Map each work-stream through one entire lifecycle (day, week, month...). In this use case, without understanding all components of the current patch process, you’ll never be able to identify all requirements, including corporate policy and implementation approach, for the integration of the CMDB.

Initiative Scope, Current State - Information Sources and General Feedback

Scope		
Process	Platform/Environment	Data and Collection Resources
Server Patch Management Phases: Pre-Patch Patch Post-Patch	<u>Server CI Operating System:</u> Windows, Linux, Solaris <u>Environment/Environment Type:</u> - Test/Non-Production - Acceptance/Non-Production - Production/Internal <u>Patch Target Scope</u> All Regional business units/Application Development	<u>Personnel</u> Server Patch Team(s) Management/Supervisory Deployment resources (domestic, offshore, business aligned) ServiceNow Administration Development Security/Risk Vulnerability reporting <u>Tools</u> Patch Management Vulnerability <u>Communication</u> Email: Notifications, Validation, Signoff <u>Change Control (ServiceNow)</u> Activity window, target attachment, notification

Differentiating Characteristics		
Target Organization	Environment (Test-Acceptance-Production)/Scheduling	Correspondence/Acknowledgement
Region: Domestic (Eastern) Org. A/ Bus. A Sub-LOB A Sub-LOB B Region: Domestic (Western) Org. A/ Bus. B Sub-LOB A Sub-LOB B	Test-Acceptance-Production/Enterprise Schedule - Monthly Test-Production only/Independent – Ad-hoc (as required)	Email Notification/Required validation/signoff Email Notification/No Required validation/signoff Email Notification/Required validation/signoff (IT only)

General Feedback
<ul style="list-style-type: none"> Patch deployment target tool scope and CMDB data not in synch No record of or defined patch window Constant state of "chasing" and emailing for verification and signoff Poor patch process cadence Many unknown key CI stakeholders

Wrapping VeriSM™ Service Management elements around a digital transformation effort.

As I mentioned in the beginning, I did not apply VeriSM™ until after I learned of this new approach, so in retrospect, as the initiative gained momentum and elements of the Management Mesh developed, conflict arose where multiple key stakeholders exhibited different principle drivers with opposing service management practices. Through trial and error and ultimately through flexibility, it was agreeing to utilize combinations of frameworks and methodologies which enabled forward momentum to continue. I found this to be a natural progression while the mesh continued to weave the other elements.

Activities basically began with understanding what needed to be achieved...its goals and objectives, then determined which principles were being applied that existed within the firm.

Strategic level plans were developed through the combination of enterprise governance (senior management) and combinations of existing and new service management practices, which set the roadmap to presenting options and ultimately prioritization decisions. This then took shape into tactical level plans by further engagement, partnering and collaboration to evolve next steps at the operational level. This entire combination of personnel engagement around existing processes and tools, the workflow evolved and weaved the elemental combinations of the VeriSM™ Management Mesh.

(See “Use-Case Elemental overlay into the Management Mesh” diagram below)

Specific to this use case regarding patch management and the ServiceNow CMDB, it's important to understand that the main activity here was to insert the CMDB into the Patch Management lifecycle, which is a digital transformation effort. We're utilizing current management practices, methods and approaches of the organization (ITIL, Agile Service Mgmt., Lean) and mapping these relational connections to requirements for the Emerging Technology (the value to be had), being the integration of the ServiceNow CMDB into the Patch Management Lifecycle.

At the user consumption level, challenges did arise in the area of cultural change, which is one of the hardest facets of service management improvement to implement. In this use-case, manual ways of doing things with their current toolset changed to new automated solutions and tools, of which appeared easy on the surface but required very close communication and collaboration to succeed. Each degree took on different flavors during engagement with multiple business consumer groups.

Characteristics of Agile were prominent in the use-case in that the mindset going in was ready for change in direction at any time and awareness to embrace the challenges. Basically, issues were dealt with as they arose, then moved on in order to maintain forward momentum. This initiative included several separate engagement venues of which all supported elements of Agile.

It's important to note that, again, as per the VeriSM™ approach, a one size fits all or prescriptive approach was not followed here, so usage of a mix of service management practices and approaches will vary dependent on how relational areas evolved the activities over time, as next in line priorities played out.

That being said, the key driver in this use-case was a process improvement initiative to provide enablement to maintain consistency in delivering required patches to all server CIs. The output on a firm-wide scale was to enable a capability to ensure appropriate patches were delivered as bug-fixes for usability improvement, performance and patching for security vulnerabilities. As a the primary ITSM component, being the ServiceNow CMDB, this use case further supports the directive of digital transformation as a system of record being utilized across the firm for varying reasons by various teams.

Further in support of VeriSM™ and its intent to impact the entire organization, it is not necessary to immediately plan it as a firm-wide impacting initiative but is kept in mind at a strategic level. Somewhat small initiatives, in many cases, uncover gaps to ultimately improve operational functionality naturally, as the engagements across the management mesh develops its “weave” to include more and more elements.

This initiative was implemented on a small scale initially, inclusive of one business, in order to fine tune the integration and operational process, then introduced and applied to other business entities prioritized by complexity and size.

To further support the VeriSM™ approach to include an Agile component, nuisances in other business units drove seamless modifications to the initial model and integrated without issue, which proved to enhance previously completed workflows.

How the ServiceNow CMDB was integrated into a Patch Management organization in a pragmatic fashion which further encompasses the overall VeriSM™ approach in keeping it as simple as possible and basically what makes sense.

At the conclusion of this CMDB integration effort, full server CI transparency enablement had been realized. The businesses, IT, App/Dev and Risk/Vulnerability Management have now attained a very confident outlook that all potential gaps have been identified and remediated to proactively mitigate any potential gaps in server patching capability.

As the various components of engagement and general scope were identified, the information collected and utilized, directly correlate to the VeriSM™ Management Mesh.

“Weaving” the Management Mesh

Resources

- Senior Management Buy-in: Mandating the effort
- Patch Management: Operational leads, Patch deployment, B/U stakeholder engagement
- ServiceNow Administration: CMDB reporting, CI field access provisioning
- ServiceNow Development: CI Discovery, Automation request scripting
- Server CI Owners: Business representative/stakeholder, application development leads
- Security & Risk Management

Emerging Technologies

- ITSM Tools (ServiceNow, CMDB)
- Automation Scripting
- Report automation
- CI Cross-Relationship mapping
- Tool component integration into operational workflows
- Centralized Authoritative CI inventory source

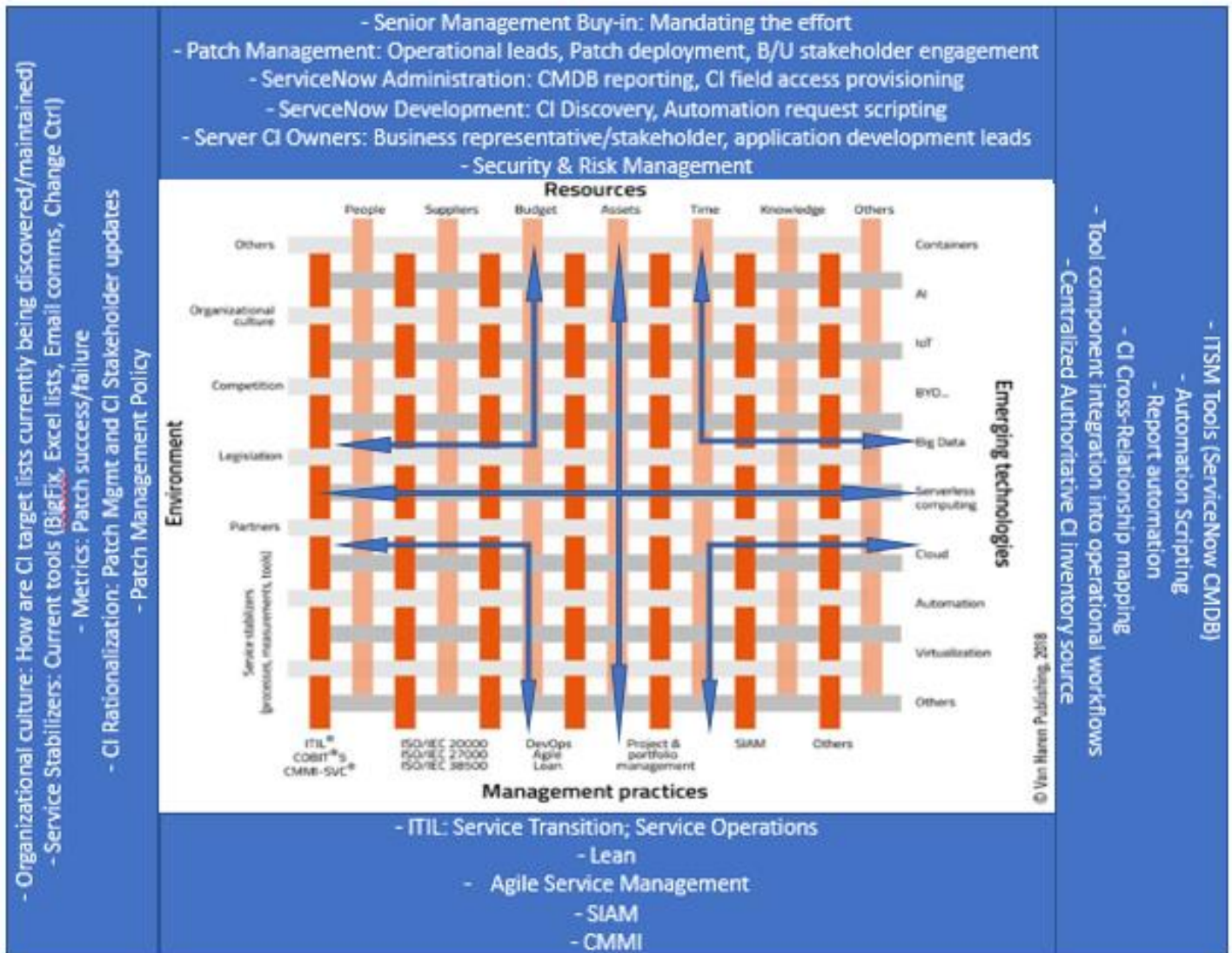
Management Practices

- ITIL: Service Transition; Service Operations
- Lean
- Agile Service Management
- SIAM
- CMMI

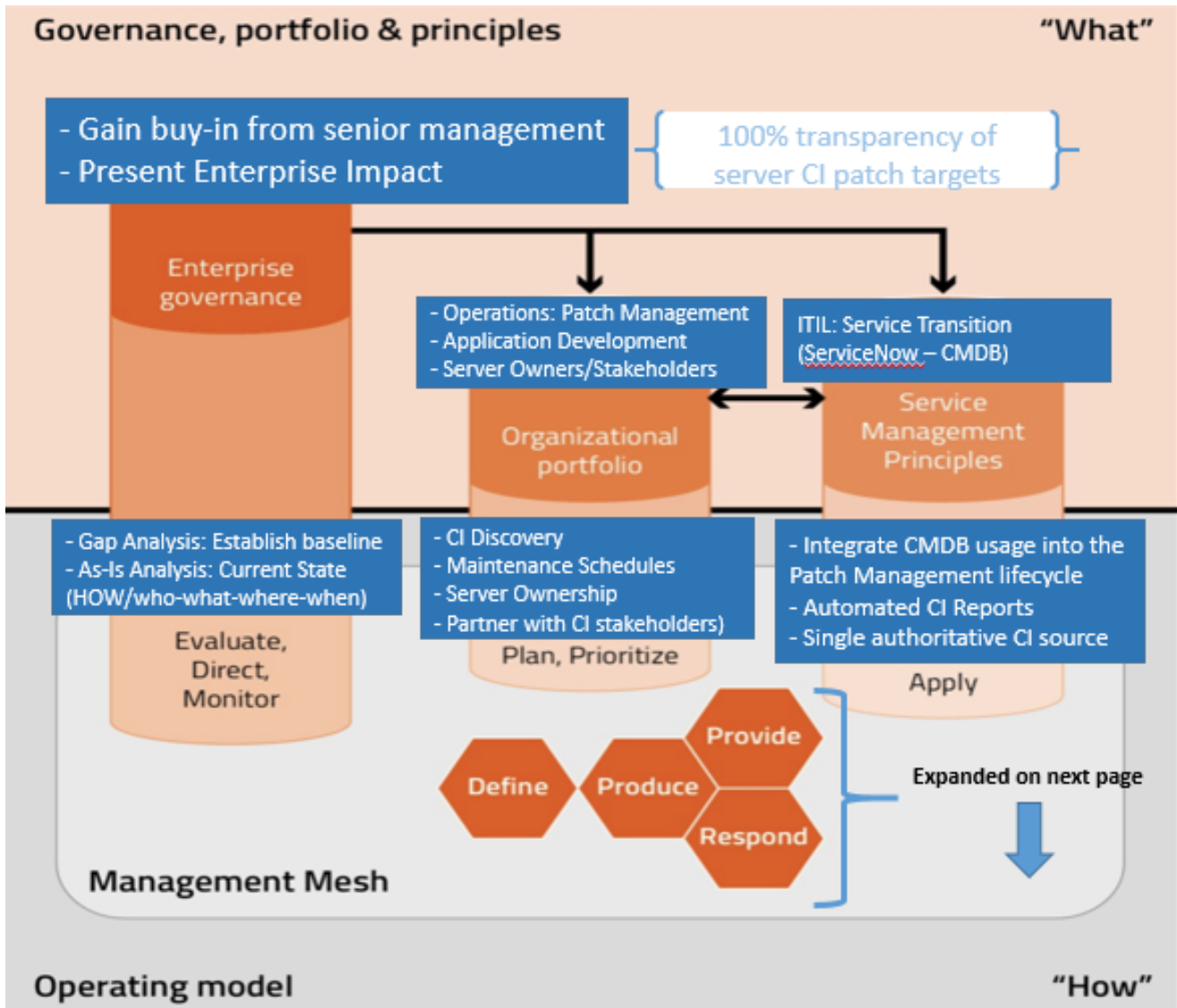
Environment

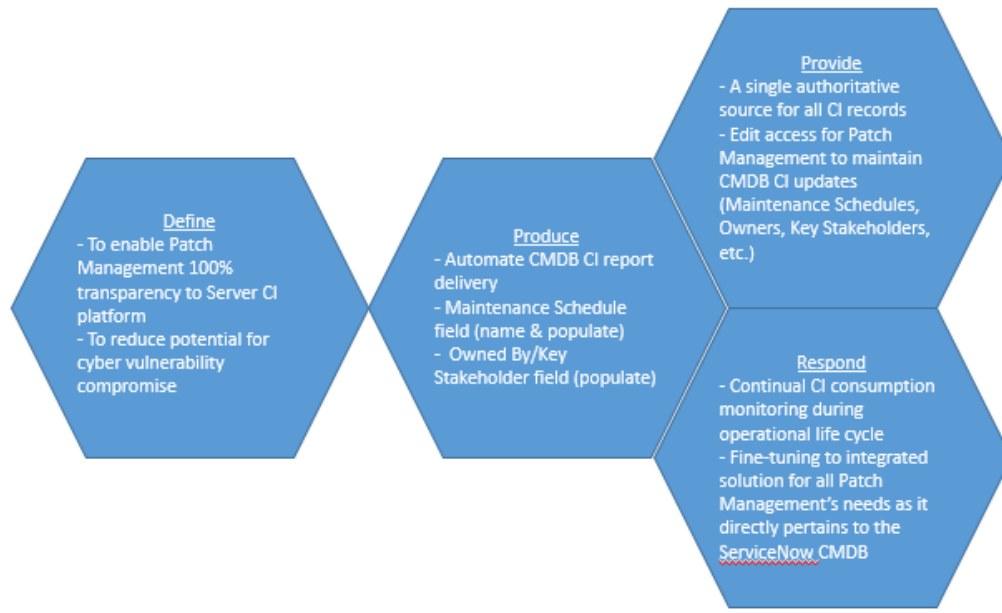
- Organizational culture: How are CI target lists currently being discovered/maintained)
- Service Stabilizers: Current tools (BigFix, Excel lists, Email comms, Change Ctrl)
- Metrics: Patch success/failure
- CI Rationalization: Patch Mgmt and CI Stakeholder updates
- Patch Management Policy

Use-Case Elemental overlay into the Management Mesh



VeriSM™ Governance, portfolio & principles and Operating Model with use case activity overlay





Accomplishments of this initiative

- A sustainable enablement and capability provided to a patch management organization
 - 100% transparency for server patch targeting.
 - Automated Server CI discovery via the ServiceNow CMDB.
 - Single authoritative source for all Server CI information and status.
 - Automated Server CI report provisioning.
 - Ease of Server CI reconciliation and maintenance between IT, App/Dev and Business Units
- Server CI relationships established to surrounding ITSM entities (Request, Incident, Problem, Change)
 - Impacting server CI activity linked to ensure full transparency to all device stakeholders.

VeriSM™ Benefits to this initiative

- Having mentioned earlier that VeriSM™ was not directly applied here prior to beginning this specific initiative, but rather afterward, exacting and correlating parallels are made across this entire initiative to this approach.

- The VeriSM™ approach illustrates the value of not having to focus within one framework or methodology and encourages blends of several as required. During the various phases of this initiative, I utilized various project and service management methodologies and approaches, some of which included ITIL, Lean Six Sigma, Agile Service Management, SIAM and CMMI.
- While VeriSM™s umbrella of reach through utilizing the Management Mesh has been utilized in this use-case within specific framework components to a single operational team, its effects span the entire organization. This same approach can be applied to much wider initiatives.
- Regarding “connecting the dots”, VeriSM™s approach ensures active connections are across the entire initiative by bridging, complex human dynamics between Business stakeholders, IT Management and IT Operations while aligning them to initiative focus of associated ITSM tools...and in this use-case, the integration of the ServiceNow CMDB into a patch management organization.

Concluding Statement

I liken the overall approach, connective qualities and entire value that VeriSM™ represents
in this age of digital competences
to that of,

“The String-Theory of ITSM”

Richard Kroh – 2019