Managing Change
A CASE STUDY AT UMASS LOWELL

Agenda
- Introduction
- UMass Lowell Change History
- 2016 Change Management Initiative
- Results
- Incidents at UMass Lowell (War Stories)
- 2017 Incident Management Initiative
- Results & Conclusions
- Q&A and Discussion
Who is this guy?

- Steve Athanas
  - Director of Platforms & Systems Engineering
  - UMass Lowell Alumni, 2004 & 2017
  - Boston VMUG Leader
  - Member of Global VMUG Board of Directors
  - VMware vExpert 2013 - 2017
  - VCP, MCITP, MCSE, MCSA, ITIL
- Reach out:
  - stephen_athanas@uml.edu
  - Twitter: @steveathanas
  - LinkedIn: www.linkedin.com/in/SteveAthanas

A Brief History of Change Process at UMass Lowell

OR: “WHAT THE WILD WEST WAS LIKE”
A bit about cowboys
2004 - 2010

- UMass Lowell IT wasn’t known for discipline
  - And a good portion of that was my fault
- Shoot first, try the patch, questions are for sissies
- We got a lot done, and there were a lot of messes to clean up
- The campus had some... reliability issues

Command & Control
2010-2014

- We attempted to get on the same page
- Process maturity wasn’t our strong suit
- Some groups had different definitions of “off-hours,” etc.
- We were trying, but lacked a common framework or standard
Becoming an ITIL Shop

- In 2014, IT realigned around an initiative on Service Delivery
- 2015 – sent everyone in IT through ITIL Foundations Training
- Once you have done ITIL training – you start to realize where you aren’t following best practices

UMass Lowell’s 2016 Change Management Initiative
OR: HOW STANDARDS ACTUALLY HELP
Why do Change Management?

- **Benefits to the campus**
  - More uptime
  - Better documentation and publishing of impacts and outages
- **Benefits to IT**
  - Improved perception on campus
  - Increased rate of change and technology evolution
- **Benefits to practitioners**
  - Better visibility for projects and changes you are working on
  - They are personally be held less responsible for impacts of changes if approved by CAB

Guiding Principles and Benefits

- Be effective
- Be simple to understand
- Keep CAB meetings short
- Get input and feedback from all groups to inform the best decisions
- Follow Standard Operating Principals (SOPs) whenever applicable
- Do not create a layer of bureaucracy that inhibits forward momentum
- Change Management must improve the stability of our operations and services
Things We Want Staff To Think Through

- Scope
- Risks
- Mitigations
- Timing
- Communication
- Testing

We desperately tried to come up with a mnemonic and failed.

Risk: It’s not just a never-ending board game

- Risk is defined by two attributes:
  - The likelihood of an adverse event happening
  - The severity of an adverse event happening
- Note that something that almost certainly will not happen, but would be severe if it does is not a low risk

Risk Reporting Matrix
**Types of Changes (And Who is Responsible)**

<table>
<thead>
<tr>
<th>Change Type</th>
<th>Responsible Party</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out-of-Scope</td>
<td>The “Doer” (You)</td>
<td>Out-of-Scope is not a “change”</td>
</tr>
<tr>
<td>Pre-Approved Changes</td>
<td>CAB (Only if SOP followed)</td>
<td>Acting inconsistently with SOP voids CAB approval.</td>
</tr>
<tr>
<td>Normal/Minor</td>
<td>Unit Manager</td>
<td>Only LOW risk activities are eligible</td>
</tr>
<tr>
<td>Normal/Significant</td>
<td>CAB</td>
<td></td>
</tr>
<tr>
<td>Normal/ Major</td>
<td>CIO</td>
<td></td>
</tr>
<tr>
<td>Emergency</td>
<td>CAB</td>
<td>CAB</td>
</tr>
<tr>
<td>Did not submit to Change Management</td>
<td>“Doer”</td>
<td>This is unacceptable. Don’t go rogue.</td>
</tr>
<tr>
<td>Autonomous Crisis</td>
<td>“Doer”</td>
<td>When failure to act would be disastrous</td>
</tr>
</tbody>
</table>

**The Secret Sauce: Peer Reviews**

- CAB meetings can take hours (or a full day) at many institutions
- The challenge: How do we get the full cross-section of IT to review and comment on changes without keeping key staff in a room all day?
- The answer: Peer reviews
  - Stolen from request for comments
- Each functional area can “vote” on changes to support the change – or not
  - If the vote is “no” then they have to say why
- Each area has a primary and backup approver
What about emergencies?

- Analyze the situation
- Come up with a recommended plan of action
- Contact a member of CAB that is *not* in your line of supervision
  - E.g., Systems Engineering cannot contact Steve Athanas
- After things are stable, enter the Emergency Change request *right away*
- Remember, change control isn’t a suicide pact
Results from Change Management

OR: ....NOPE. I’VE GOT NOTHING. JUST GO WITH WHAT’S UP THERE.

The Anecdotal Evidence
(Good Stuff)

- The Service Desk is more aware of changes (and therefore root causes of issues than ever before
- Administrators and Engineers are thinking in terms of risk and rollback
- CAB meetings are smooth and generally about 15 minutes long – some are done virtually
- Infrastructure (Security Ops / Systems Engineering / Network) have adopted the process well
- Unplanned changes are WAY down
  - Difficult to tell by how much – no data from previous situation
The Anecdotal Evidence (Bad Stuff)

- Not all departments have committed to rigorous Peer Reviews
- The software tool we use was complicated to beat into submission
- Tech staff have to duplicate work requests into RFCs often
- There has been some confusion around Emergency vs Expedited requests
- Peer reviews are occasionally not reviewed properly (auto-approved)

By the Numbers
July 2016–June 2017

- Changes Documented: 1106
  - Pre Approved: 231 (21%)
  - Emergency: 30 (3%)
  - Normal (Minor): 718 (65%)
  - Normal (Significant): 128 (12%)
- Note that the vast majority (86%) of changes are approved by unit managers or are pre-approved
Incidents at UMass Lowell
OR: WAR STORIES FROM THE FRONT OF A VERY LONG, VERY BORING WAR

A detailed listing of some Incidents We’ve Had

- Words that mean something that I’m not going to show to anyone at any point.
- Here are some more words that we need to use.
- Have you ever considered having some words? Here are some.
- This one will be very long to infer that something interesting is happening behind the redaction, which will be displayed shortly. Uh oh, that sentence was too short.
- Short one.
Okay.. Let’s talk in generalities

Who in the room hasn’t made a mistake that’s broken something?

Sometimes a change starts as a simple thing…

- And cascades into a complete disaster
- Firmware updates never go bad, right?

The simple reality is that the more eyes you have on a change process, the better your likelihood of success

- ….and the lower your risk of burning the core network to the ground
- ….not that we’ve ever done something like that.

2017 Incident Management Initiative
Major Incident Process

- We’ve Had Our Share of Major Incidents
- What’s a Major Incident?
  - “A Major Incident is a disruption, or potential disruption, of a Service that presents an immediate and significant risk to a critical business process.”
- Why does that matter?
  - The declaration of a Major Incident represents an organizational decision to prioritize personnel and resources to pursue a Workaround or solution to the disruption.

Process Flowchart

- Major Steps:
  - Evaluate
  - Classify
  - Define roles
  - Communicate
  - Investigate & Diagnose
  - Test Solutions
  - Remediate
  - After Action Review
- The goal is to follow a defined workflow – NOT to prescribe a solution
Major Incident Process

- Major Incident Declarers
  - CAB
- Major Incident Owner (MIO)
  - CIO Report appointed by declarer.
  - Coordinates the response
- Technical Lead
  - Appointed by MIO
  - Quarterbacks Technical Team
- Technical Team
  - Team Assembled by Tech Lead
  - Reprioritized to this issue
- Communication Lead
  - Appointed by MIO
  - Responsible for communication to external stakeholders
- Scribe
  - Appointed by MIO
  - Records steps and actions
  - Is not part of Tech Team
- Communications Assistant
  - Useful if MIO is functioning as Communication Lead

Major Incident Process

- If a Major Incident is declared – IT works on that at the expense of other deliverables
  - The Major Incident Owner and Technical Lead operate with CIO authority over resource allocation
- Define a Situation Room
  - Must be vacated if a Major Incident is declared
- Change Management Still In Effect
  - A Major Incident does not circumvent Change Management or CAB
Incident Management Results
OR: WHEN YOUR REHEARSAL IS RIGHT NOW! GO!

Major Incident Policy

- In January, when our major incident policy was brand new, we had submitted it to all of IT for review.
- And then a major network outage happened – taking down most of the core routing for the campus network
- We panicked for a little while (5 minutes)
- And then... we remembered we had a process, and we went through it.
- The incident was worked appropriately, communications had never been better and everyone felt like we were aligned to a goal.
The Bottom Line

- No presentation can tell you how to structure and run a process
  - Change Management and Incident Management are not exceptions
- However, you can take away our best practices:
  - Engage the entire IT community at your campus
  - Get buy-in and support from the parties that make the most changes
  - Be transparent – change management increases the overhead to production work ratio, but *for a good reason!*

Questions & Discussion

THANK YOU!