WaTech Governor's Agency Lean Report
Jul-Dec 2016

1. Training Data:

	Data to Report	7/2016-12/2016	Total WaTech*
1	Number of employees who have had any Lean knowledge and skill building in Lean in WaTech.	24	235
2	Number of supervisors, managers, executives who have had any Lean knowledge and skill building in Lean in your agency.	7	73
3	Number of employees who have had problem solving training.	1	47
4	Number of supervisors, managers, executives who have had problem solving training.	1	5
5	Number of supervisors, managers, executives who have had coaching training.	0	10
6	Number of employees who have had "facilitator" training.	0	8
7	Number of employees who have participated in an improvement effort.	13	108

Note: Staff counted in previous data who are no longer at WaTech are no longer included in the total data. As a result, some of our numbers fell compared to our July report.

2. Project Data: Computer Emergency Response Team (CERT) Security Assessment Process

1. GENERAL INFORMATION:

- Lead Agency Name: Washington Technology Solutions (WaTech)
- Improvement Project Title: CERT Security Assessment Process
- Date Initiated: September 14, 2016
- Project Type: Agency Strategic Plan
- Review and Approved by: David Morris

2. PROJECT SUMMARY:

The focus of this Lean project was to decrease the lifecycle of computer security assessment services in order to serve more customers each year.

3. PROJECT DETAILS:

Identify the Problem:

Computer Security Assessment Services

The Office of Cyber Security (OCS) began offering computer security assessment services to Washington State agencies in 2014. Agencies are able to request up to 11 security assessment modules from the Security Services Catalog or select only those assessments that fit their agency's specific needs.

Customer Backlog

CERT services have been so popular that there has been a backlog of customers since shortly after the services became available. In May 2016, the backlog extended until January 2017. Customers have not been happy about the current waiting period as CERT has only been able to serve about 8 customers per year.

Security Assessment Process

The security assessment process requires CERT to:

- Provide Pre-Assessment analysis with each agency to establish connectivity
- Perform the Assessment modules
- Complete Post-Assessment activities including a comprehensive summary report

The full security assessment takes 6 weeks to complete with a 4 member team.

4. PROBLEM STATEMENT:

Problems to be solved:

- The CERT Security Assessment Process currently takes 6 weeks. This project was undertaken to reduce the amount of time it takes to complete an assessment by identifying and implementing a combination of process improvements and organizational capability increases. The counter measures identified would allow the team to reach its target of completing an assessment every 4-5 weeks which they want to achieve by August 31, 2017.

5. IMPROVEMENT DESCRIPTION:

Numerous process countermeasures were identified:

Quick Wins:

- Move time slots back for initial customer meeting to reduce start date slippage.
- Establish a customer agency central point of contact to remove barriers to progress.
- Create a technical requirements FAQ to reduce inadequate system access.
- Complete reports concurrently with testing to reduce overburdening staff at the end of assessment period.

Long Term Wins:

- Improve turnaround time to send notification to agencies.
- Increase organizational capability of the assessment team.
- Revise the CERT Service Catalog so customers can use it better to improve the quality of the assessment.
- Remove the OCIO Policy module from the CERT Services Catalog.

- Standardize the most productive methods and procedures of completing tests to reduce the amount of research needed.

6. **CUSTOMER INVOLVEMENT:**
The Lean project team reviewed survey data from various agencies that had used the CERT Security Assessment process. Answers to the survey questions helped guide the direction of the process improvement efforts.

7. **PROJECT DETAILS:**

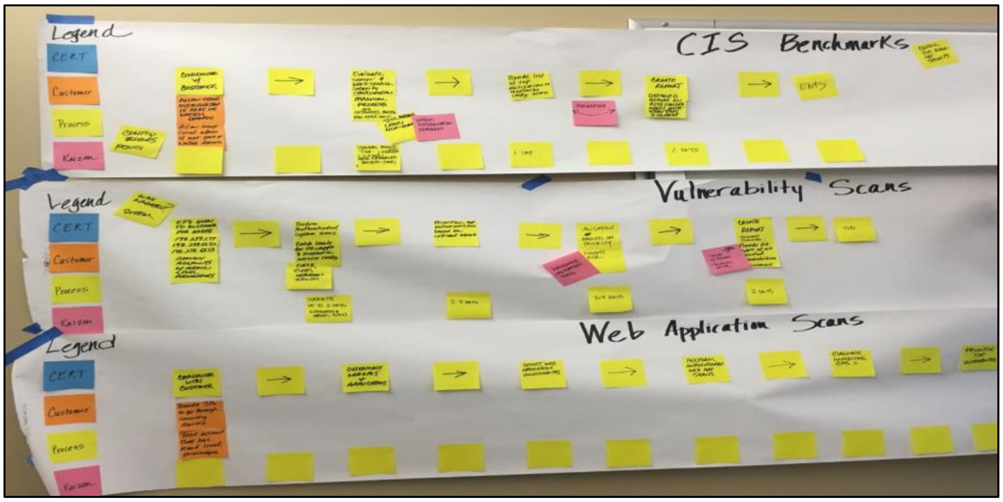
Improved process as measured by:	Specific Countermeasures Identified:	Anticipated Impact:	Results Status:
Quality	• Provide a FAQ or Quick Tips on how to provide system access in case the customer contact needs to forward the instructions to another person or technician.	• Customers get step by step instructions to provide system administrator access. • Customers have technical support for granting system administrator access. • Time savings for CERT & customer.	Due to the length of the CERT Security Assessment process, final results will not be available until after the end of August 2017.
Time	• Initial timeframe determined to be 4 weeks for the Pre-Assessment and 6 weeks for the Assessment period. After analysis of internal processes, it was determined implementation of the countermeasures would result in both the Pre-assessment and the Assessment taking 4 weeks each, which is a two week time reduction	• Time reduction for each customers and more customers can be served annually (10-12 vs. 8)	
Customer Satisfaction	• Phishing assessments are now available on a subscription basis and are no longer limited to agency security assessment periods. • The Table Top exercise will now be available upon request which will allow CERT to serve more customers.	• CERT can assist more customers • Customers do not need to wait as long for security assessments	
Employee engagement	• Central point of contact ensures CERT staff can reach customers easily.	• Less overburdening of staff • Ease of reducing barriers and moving the assessment forward	

8. **CONTACT INFORMATION:**
Name: David Brummel
Phone: 360-407-8816

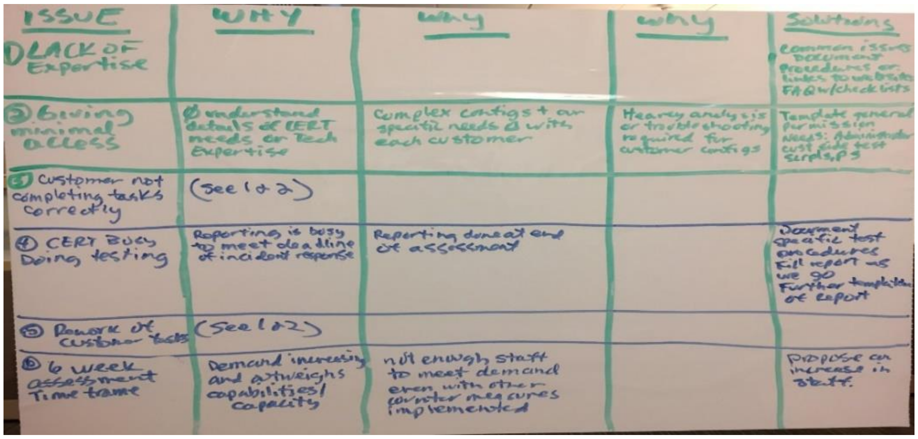
Email: david.brummel@WaTech.wa.gov

9. OPTIONAL VISUALS:

Current State VSM Examples



Root Cause Analysis



ISSUE	WHY	why	why	Solutions
① LACK OF Expertise				common issues Document Procedures or links to websites FAQ w/checklists
② Giving minimal access	Ø understand details of CERT needs or Tech Expertise	Complex configs + our specific needs Ø with each customer	Heavy analysis or troubleshooting required for customer configs	Template general permission Needs: Administrator cust side test scripts, P $
③ customer not completing tasks correctly	(See 1 & 2)			
④ CERT Busy Doing testing	Reporting is busy to meet deadline of incident response	Reporting done at end of assessment		Document specific test procedures Fill report as we go Further templating of report
⑤ Rework of customer tasks	(See 1 & 2)			
⑥ 6 week assessment Time frame	Demand increasing and outweighs capabilities/ capacity	not enough staff to meet demand even with other counter measures implemented		propose an increase in staff.

PICK Chart – Countermeasure Prioritization

Low - - - - - - - - - - - - - - - - - Cost - - - - - - - - - - - - - - - - - High

POSSIBLE • **#7 – Permissions What & Why Template** - Design a document that explains exactly what CERT's technical requirements are to complete the assessments, and why that level of access is needed. Include what is done with the information. (Timeline 4 – Some Time) • **#9 – Documented Test Procedures** - Standardize the most productive methods and procedures of completing tests. (Timeline 5 – More Time) • **#13 – Library of Web Application Vulnerability Verbiage & Recommendations** - Create a resource library of vulnerability recommendations with standard language that can be reused for future reports. (Timeline 6 – More Time)	**CHALLENGING** • **#8 – Customer Test for Connectivity** - Provide customers with a script to run so they can test connectivity before they contact CERT that they are prepared for the assessments to begin. • **#10 – Test Automation** - Develop automation for tests wherever possible.
IMPLEMENT • **#4 – Checklist Completion Deadline** - Make two weeks prior to the assessment start date the dead line for pre-assessment Checklist activity completion. (Timeline 1 – Little Time) • **#11 – Concurrent Report Completion** - Fill in the assessment report during the assessment process rather than waiting until the end of the assessment period. (Timeline 2 – Little Time) • **#2 – Central Point of Contact** - Ask customer for a central point of contact to act as liaison throughout the assessment. (Timeline 2 – Little Time) • **#12 – Report Template** - Make as much of the customer report as possible into a template, except where there is a need for customized results. (Timeline 4 – Some Time) • **#1 – Initial Meeting Timeslots** - Send email to customer 6 weeks from assessment start date with specific timeslot availability for the initial meeting so it gets scheduled as close to one month from start date as possible. (Timeline 1 – Little Time) • **#3 – Customer Guidelines for Due Dates** - Instead of giving customers the entire month to complete pre-assessment Checklist activities, provide visual guidelines/timeframes for task completion. (Timeline 2- Little Time) • **#6– System Administrator Access Procedures** - Provide an electronic copy of the specific procedure to grant system administrator access in case the customer contact needs to forward the instructions to another person or technician. (Timeline 3 – Some Time) • **#5 – System Administrator Access Quick Tips** - Design Quick Tips instruction sheet for the customer who needs to know how to provide system access. Provide a Common Issues or FAQ document. (Timeline 4 – Some Time) • **#14 – Web Application Training for CERT** - Provide CERT members with additional training on Web Applications for additional skill in detection and evaluation of vulnerabilities. (Timeline 7 – Much Time)	**KEEP FOR LATER**

Low - Complexity - High