­­­­

 Bitlocker Portfolio
Eddie S. Jackson
Kaplan University
IT599: Applied IT Master Project

Rhonda Chicone, Ph.D.
7/14/2015

TABLE OF CONTENTS

IT PROJECT PLAN 3

1.0 Overview 3

2.0 Scope 3

3.0 Budget 3

4.0 Stakeholders 4

5.0 Benefits 4

6.0 ROI 5

7.0 Roles and Responsibilities 5

8.0 Work Breakdown Structure 5

9.0 Milestones 8

10.0 Risk Assessment 9

11.0. Communications Plan 10

MILESTONE REPORTS 12

Milestone 1 12

Milestone 2 16

Milestone 3 18

LESSONS LEARNED 19

TECHNICAL DOCUMENTATION 28

Preface 28
Check TPM Status 29
TPM Management 31
Bitlocker Compliance 37
Helpdesk Support 39

Backup Bitlocker Passwords 41

REFERENCES 43

Company x

July 4, 2015

# IT Project Plan

## 1.0 Project Overview

Due to recent security breaches across the nation, Company X has become increasingly concerned about securing the contents of company computer hard drives. Currently, the company does have anti-virus software installed, a data loss prevention solution, and malware protection on all workstations, but does not have any form of drive encryption. Without encryption, the data on computers could be stolen, hacked while offline, or viewed by unauthorized people.

As an encryption solution, Microsoft’s Bitlocker has been recommended. Bitlocker is a full disk encryption solution, which can be implemented by using technology that already exists on the company’s workstations. Something worth mentioning, this particular solution will contain a “free” or nearly free management solution. This is to forego the costs of $150 (per workstation) 3rd party solutions, and to not have to pay the $10 per seat by using MBAM and MDOP (Microsoft Bitlocker Reporting solutions). The project will have a budget for implementing Bitlocker, however, the TCO will be very low, while the ROI will be high, and continue to grow over time. When using this inexpensive implementation method, companies can save hundreds of thousands of dollars (potentially millions of dollars) in Bitlocker implementation and management costs.

## 2.0 Project Scope

The scope of the project includes implementing Bitlocker on all company workstations, some ten thousand computers. The time is set at seven months, which includes development and testing, technical support for failed Bitlocker installations, replacing non-working machines with new, working computers, and training support staff. The end goal is to have Bitlocker deployed to all company workstations by the first quarter of 2016.

## 3.0 Project Budget

|  |  |  |
| --- | --- | --- |
| **Budget Item** | **Description** | **Cost** |
| Code development | Reporting and TPM Management solutions must be developed in-house | $3,500 |
| Training | Documentation must be created and staff trained | $2,000 |
| 20 x Computers | Twenty computers have been allocated to replace non-working TPM chips: Each computer costs $1,000. | $20,000 |
| Technical Support | $25 per hour, with a breakdown of 25 hours \* $25 \* 3 sites | $1,875 |
| Miscellaneous Costs | Costs include support for Active Directory, Network computers, and the Bitlocker solution. | $2,625 |
|  | **Total cost** | $30,000 |

## 4.0 Project Stakeholders

The stakeholders will include the CIO, CFO, the Change Management Team, the Senior Developer, and the Manager and Team Leader from the IT department.

|  |  |
| --- | --- |
| **Title** | **Description** |
| CFO | Chief Financial Officer, in charge of company finances |
| CIO | Chief Information Officer, in charge of company technology |
| Change Management Team | Authorizes changes to enterprise systems |
| Senior Developer | Responsible for software development |
| IT Manager | Communicates directly to IT staff |
| IT Team Leader | Performs training to IT staff |

## 5.0 Project Benefits

|  |  |
| --- | --- |
| **Benefit** | **Description** |
| Secure Data | The data contents of the hard drive will be secured. |
| Offline Attacks | Offline attacks, such as removing the hard drive and placing it into another computer, will be prevented. |
| Unauthorized users | If the user is not a company user, recovery keys will not be available to them, thus, any authorized user cannot access the data on the drive. |
| Disposal | When disposing hard drive, there is peace of mind that company data will not be leaked |
| Savings | A third party utility will not need to be purchased, thus saving the company the costs of maintaining a per machine license. |

## 6.0 Project ROI

The ROI has a few variables. One, standalone encryption software applications cost anywhere from $100-$200, so I will say $150 per workstation (that is $150 \* 10,000 workstations = $1,500,000) (Suneja, 2006). Next, the Microsoft reporting software costs $10 per seat, that is, 10 \* 10,000 workstations = $100,000. Adding these two figures together totals $1,600,000. The proposed solution costs $20,000 to implement.

## 7.0 Project Roles and Responsibilities

|  |  |
| --- | --- |
| **Role** | **Responsibility** |
| IT Specialist | Develops all code, deploys code, and runs reports |
| Stakeholders | Authorizes the stages of the project |
| IT Team Leader | Creates documentation and trains staff accordingly |
| Ohio Technician | Site tech is responsible for local support |
| Arizona Technician | Site tech is responsible for local support |
| Florida Technician | Site tech is responsible for local support |

## 8.0 Project Work Breakdown Structure Project Dates: 07/1/2015-02/29/2016, 1st Quarter of 2016*\* The critical path is in red*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Task Name | Duration | Start | Finish | Predecessors |
| BITLOCKER ROLLOUT PROJECT | 174 days? | Wed 7/1/15 | Mon 2/29/16 |  |
| **1.0 Project Start** | **8 days** | **Wed 7/1/15** | **Fri 7/10/15** |  |
|  1.1 Create Project Overview  | 3 days? | Wed 7/1/15 | Fri 7/3/15 |  |
|  1.2 Define Scope  | 3 days? | Mon 7/6/15 | Wed 7/8/15 |  |
|  1.3 Define Business Plan  | 3 days? | Mon 7/6/15 | Wed 7/8/15 |  |
|  1.4 Perform a Risk Assessment  | 2 days? | Thu 7/9/15 | Fri 7/10/15 |  |
| **2.0 Project Planning** | **5 days** | **Mon 7/13/15** | **Fri 7/17/15** |  |
|  2.1 Create Project Proposal  | 1 day? | Mon 7/13/15 | Mon 7/13/15 |  |
|  2.2 Obtain Initial Approval from Stakeholders  | 1 day? | Tue 7/14/15 | Tue 7/14/15 |  |
|  2.3 Create Budget  | 1 day? | Tue 7/14/15 | Tue 7/14/15 |  |
|  2.4 Kickoff Meeting  | 1 day? | Tue 7/14/15 | Tue 7/14/15 |  |
|  2.5 Identify Risks  | 1 day? | Wed 7/15/15 | Wed 7/15/15 |  |
|  2.6 Create Contingency Plan for Risks  | 1 day? | Wed 7/15/15 | Wed 7/15/15 |  |
|  2.7 Complete Business Analysis  | 1 day? | Wed 7/15/15 | Wed 7/15/15 |  |
|  2.8 Draft Project Plan  | 1 day? | Thu 7/16/15 | Thu 7/16/15 |  |
|  2.9 Draft Project Schedule  | 1 day? | Thu 7/16/15 | Thu 7/16/15 |  |
|  2.10 Stakeholder Meeting for Design Approval  | 1 day? | Fri 7/17/15 | Fri 7/17/15 |  |
| **3.0 Construction** | **32 days** | **Mon 7/20/15** | **Tue 9/1/15** |  |
|  **3.1 Design**  | **3 days** | **Mon 7/20/15** | **Wed 7/22/15** |  |
|  3.1.1 Coded Report for TPM status  | 1 day? | Mon 7/20/15 | Mon 7/20/15 |  |
|  **3.1.2 TPM Management for importing recovery keys**  | **2 days?** | **Mon 7/20/15** | **Tue 7/21/15** |  |
|  3.1.2.1 Active Directory Import  | 1 day? | Mon 7/20/15 | Mon 7/20/15 |  |
|  3.1.2.2 LANDesk Import  | 1 day? | Tue 7/21/15 | Tue 7/21/15 |  |
|  3.1.2.3 Email Keys  | 1 day? | Tue 7/21/15 | Tue 7/21/15 |  |
|  3.1.2.4 SFTP Keys  | 1 day? | Tue 7/21/15 | Tue 7/21/15 |  |
|  3.1.3 Coded Reports for Bitlocker Status  | 1 day? | Tue 7/21/15 | Tue 7/21/15 |  |
|  3.1.4 Weekly Status email sent to Stakeholders  | 1 day? | Tue 7/21/15 | Tue 7/21/15 |  |
|  3.1.5 Stakeholder Meeting for Development Approval  | 1 day? | Wed 7/22/15 | Wed 7/22/15 |  |
|  **3.2 Development**  | **22 days** | **Mon 7/20/15** | **Tue 8/18/15** |  |
|  3.2.1 A coded report will be required for TPM status verification  | 1 day? | Fri 7/24/15 | Fri 7/24/15 |  |
|  3.2.2 Programming code to activate the TPM chip  | 1 day? | Mon 7/27/15 | Mon 7/27/15 |  |
|  3.2.3 Programming code to take ownership of the TPM chip  | 1 day? | Tue 7/28/15 | Tue 7/28/15 |  |
|  3.2.4 Programming code to add protectors to TPM chip  | 1 day? | Wed 7/29/15 | Wed 7/29/15 |  |
|  3.2.5 Programming code to upload recovery keys to FTP server  | 1 day? | Mon 8/3/15 | Mon 8/3/15 |  |
|  3.2.6 Programming code to email recovery keys to service account  | 1 day? | Wed 8/5/15 | Wed 8/5/15 |  |
|  3.2.7 Programming code to import rec. keys into Active Directory  | 1 day? | Mon 8/10/15 | Mon 8/10/15 |  |
|  3.2.8 Programming code to import rec. keys into LANDesk/SCCM  | 1 day? | Fri 8/14/15 | Fri 8/14/15 |  |
|  3.2.9 A coded report will be required for Bitlocker status  | 1 day? | Mon 8/17/15 | Mon 8/17/15 |  |
|  3.2.10 Weekly Status email sent to Stakeholders  | 1 day? | Mon 8/17/15 | Mon 8/17/15 |  |
|  3.2.11 All code successfully tested in lab environment  | 1 day? | Tue 8/18/15 | Tue 8/18/15 |  |
|  **3.3 Software Unit Testing**  | **6 days** | **Wed 8/19/15** | **Wed 8/26/15** |  |
|  **3.3.1 Start Alpha Testing**  | **3 days?** | **Wed 8/19/15** | **Fri 8/21/15** |  |
|  3.3.1.1 Identify software issues  | 1 day? | Wed 8/19/15 | Wed 8/19/15 |  |
|  3.3.1.2 Fix software issues  | 1 day? | Thu 8/20/15 | Thu 8/20/15 |  |
|  3.3.1.3 Test Again  | 1 day? | Thu 8/20/15 | Thu 8/20/15 |  |
|  3.3.1.4 Status email sent to Stakeholders  | 1 day? | Fri 8/21/15 | Fri 8/21/15 |  |
|  **3.3.2 Start Beta Testing**  | **3 days?** | **Mon 8/24/15** | **Wed 8/26/15** |  |
|  3.3.2.1 Identify software issues  | 1 day? | Mon 8/24/15 | Mon 8/24/15 |  |
|  3.3.2.2 Fix software issues  | 1 day? | Mon 8/24/15 | Mon 8/24/15 |  |
|  3.3.3.3 Test Again  | 1 day? | Tue 8/25/15 | Tue 8/25/15 |  |
|  3.3.3.4 Status email sent to Stakeholders  | 1 day? | Tue 8/25/15 | Tue 8/25/15 |  |
|  3.3.3 Prepare Report for Stakeholders  | 1 day? | Tue 8/25/15 | Tue 8/25/15 |  |
|  3.3.4 Stakeholder Meeting for UaT Approval  | 1 day? | Wed 8/26/15 | Wed 8/26/15 |  |
|  3.3.5 Complete Unit Testing  | 1 day? | Wed 8/26/15 | Wed 8/26/15 |  |
|  **3.4 User Acceptance Testing**  | **4 days** | **Thu 8/27/15** | **Tue 9/1/15** |  |
|  **3.4.1 Start Pilot testing Group 1 Ohio Site**  | **1 day?** | **Thu 8/27/15** | **Thu 8/27/15** |  |
|  3.4.1.1 Send emails to 5 users  | 1 day? | Thu 8/27/15 | Thu 8/27/15 |  |
|  3.4.1.2 Enable TPM chips in Pilot Group  | 1 day? | Thu 8/27/15 | Thu 8/27/15 |  |
|  3.4.1.3 Deploy TPM Management to Pilot Group  | 1 day? | Thu 8/27/15 | Thu 8/27/15 |  |
|  3.4.1.4 Assess Users 1-5 in Pilot Group  | 1 day? | Thu 8/27/15 | Thu 8/27/15 |  |
|  3.4.1.5 Address issues in hardware and/or software  | 1 day? | Thu 8/27/15 | Thu 8/27/15 |  |
|  3.4.1.6 Status email sent to Stakeholders  | 1 day? | Thu 8/27/15 | Thu 8/27/15 |  |
|  **3.4.2 Start Pilot testing Group 1 Arizona Site**  | **1 day?** | **Fri 8/28/15** | **Fri 8/28/15** |  |
|  3.4.2.1 Send emails to 5 users  | 1 day? | Fri 8/28/15 | Fri 8/28/15 |  |
|  3.4.2.2 Enable TPM chips in Pilot Group  | 1 day? | Fri 8/28/15 | Fri 8/28/15 |  |
|  3.4.2.3 Deploy TPM Management to Pilot Group  | 1 day? | Fri 8/28/15 | Fri 8/28/15 |  |
|  3.4.2.4 Assess Users 1-5 in Pilot Group  | 1 day? | Fri 8/28/15 | Fri 8/28/15 |  |
|  3.4.2.5 Address issues in hardware and/or software  | 1 day? | Fri 8/28/15 | Fri 8/28/15 |  |
|  3.4.2.6 Status email sent to Stakeholders  | 1 day? | Fri 8/28/15 | Fri 8/28/15 |  |
|  **3.4.3 Start Pilot testing Group 1 Florida Site**  | **1 day?** | **Mon 8/31/15** | **Mon 8/31/15** |  |
|  3.4.3.1 Send emails to 5 users  | 1 day? | Mon 8/31/15 | Mon 8/31/15 |  |
|  3.4.3.2 Enable TPM chips in Pilot Group  | 1 day? | Mon 8/31/15 | Mon 8/31/15 |  |
|  3.4.3.3 Deploy TPM Management to Pilot Group  | 1 day? | Mon 8/31/15 | Mon 8/31/15 |  |
|  3.4.3.4 Assess Users 1-5 in Pilot Group  | 1 day? | Mon 8/31/15 | Mon 8/31/15 |  |
|  3.4.3.5 Address issues in hardware and/or software  | 1 day? | Mon 8/31/15 | Mon 8/31/15 |  |
|  3.4.3.6 Status email sent to Stakeholders  | 1 day? | Mon 8/31/15 | Mon 8/31/15 |  |
|  3.4.4 Prepare report for Stakeholder meeting  | 1 day? | Mon 8/31/15 | Mon 8/31/15 |  |
|  3.4.5 Stakeholder Meeting for Approval - Go-live approval  | 1 day? | Tue 9/1/15 | Tue 9/1/15 |  |
|  3.4.6 Transfer technical documentation to IT Team Leader  | 1 day? | Tue 9/1/15 | Tue 9/1/15 |  |
|  3.5 User Acceptance Test Complete | 1 day? | Tue 9/1/15 | Tue 9/1/15 |  |
| **4.0 Implementation** | **152 days** | **Wed 9/2/15** | **Thu 3/31/16** |  |
|  **4.1 Enable TPM Chips**  | **61 days** | **Wed 9/2/15** | **Wed 11/25/15** |  |
|  **4.1.1 Enable TPM Chips at Ohio site 3,300 computers**  | **20 days** | **Wed 9/2/15** | **Tue 9/29/15** |  |
|  4.1.1.1 Weekly Status Report (825 computers)  | 5 days? | Wed 9/2/15 | Tue 9/8/15 | 80 |
|  4.1.1.2 Weekly Status Report (825 computers)  | 5 days? | Wed 9/9/15 | Tue 9/15/15 | 84 |
|  4.1.1.3 Weekly Status Report (825 computers)  | 5 days? | Wed 9/16/15 | Tue 9/22/15 | 85 |
|  4.1.1.4 Weekly Status Report (825 computers)  | 5 days? | Wed 9/23/15 | Tue 9/29/15 | 86 |
|  **4.1.2 Enable TPM Chips at Arizona site 3,300 computers**  | **20 days** | **Wed 9/30/15** | **Tue 10/27/15** |  |
|  4.1.2.1 Weekly Status Report (825 computers)  | 5 days? | Wed 9/30/15 | Tue 10/6/15 |  |
|  4.1.2.2 Weekly Status Report (825 computers)  | 5 days? | Wed 10/7/15 | Tue 10/13/15 | 89 |
|  4.1.2.3 Weekly Status Report (825 computers)  | 5 days? | Wed 10/14/15 | Tue 10/20/15 | 90 |
|  4.1.2.4 Weekly Status Report (825 computers)  | 5 days? | Wed 10/21/15 | Tue 10/27/15 | 91 |
|  **4.1.3 Enable TPM Chips at Florida site 3,400 computers**  | **21 days** | **Wed 10/28/15** | **Wed 11/25/15** |  |
|  4.1.3.1 Weekly Status Report (850 computers)  | 5 days? | **Wed 10/28/15** | Tue 11/3/15 |  |
|  4.1.3.2 Weekly Status Report (850 computers)  | 5 days? | Wed 11/4/15 | Fri 11/13/15 |  |
|  4.1.3.3 Weekly Status Report (850 computers)  | 5 days? | Wed 11/11/15 | Tue 11/17/15 | 95 |
|  4.1.3.4 Weekly Status Report (850 computers)  | 5 days? | Wed 11/18/15 | Tue 11/24/15 | 96 |
|  4.2 Create TPM Chip Master Status Report  | 1 day? | Wed 11/25/15 | Wed 11/25/15 | 97 |
|  **4.2 Deploy TPM Management**  | **68 days** | **Wed 11/25/15** | **Fri 2/26/16** |  |
|  4.2.1 Deploy TPM Management at Ohio site 3,300 computers  | **21 days** | **Wed 11/25/15** | **Wed 12/23/15** |  |
|  4.2.1.1 Weekly Status Report (825 computers)  | 5 days? | Thu 11/26/15 | Wed 12/2/15 | 98 |
|  4.2.1.2 Weekly Status Report (825 computers)  | 5 days? | Thu 12/3/15 | Wed 12/9/15 | 101 |
|  4.2.1.3 Weekly Status Report (825 computers)  | 5 days? | Thu 12/10/15 | Wed 12/16/15 | 102 |
|  4.2.1.4 Weekly Status Report (825 computers)  | 5 days? | Thu 12/17/15 | Wed 12/23/15 | 103 |
|  4.2.2 Deploy TPM Management at Arizona site 3,300 computers  | **20 days** | **Mon 1/4/16** | **Fri 1/29/16** |  |
|  4.2.2.1 Weekly Status Report (825 computers)  | 5 days? | Mon 1/4/16 | Fri 1/8/16 | 104 |
|  4.2.2.2 Weekly Status Report (825 computers)  | 5 days? | Mon 1/11/16 | Fri 1/15/16 | 106 |
|  4.2.2.3 Weekly Status Report (825 computers)  | 5 days? | Mon 1/18/16 | Fri 1/22/16 | 107 |
|  4.2.2.4 Weekly Status Report (825 computers)  | 5 days? | Mon 1/25/16 | Fri 1/29/16 | 108 |
|  4.2.3 Deploy TPM Management at Florida site 3,400 computers  | **20 days** | **Mon 2/1/16** | **Fri 2/26/16** |  |
|  4.2.3.1 Weekly Status Report (850 computers)  | 5 days? | Mon 2/1/16 | Fri 2/5/16 | 109 |
|  4.2.3.2 Weekly Status Report (850 computers)  | 5 days? | Mon 2/8/16 | Fri 2/12/16 | 111 |
|  4.2.3.3 Weekly Status Report (850 computers)  | 5 days? | Mon 2/15/16 | Fri 2/19/16 | 112 |
|  4.2.3.4 Weekly Status Report (850 computers)  | 5 days? | Mon 2/22/16 | Fri 2/26/16 | 113 |
|  4.3 Run TPM Management Status Report  | 1 day | Mon 2/29/16 | **Mon 2/29/16** | 114 |
| **5.0 Project Closure** | **1 day** | **Mon 2/29/16** | **Mon 2/29/16** |  |
|  5.1 Discuss Lessons Learned/Create PowerPoint  | 1 day | **Mon 2/29/16** | Mon 2/29/16 | 115 |
|  5.2 Project Closure Report  | 1 day | **Mon 2/29/16** | Mon 2/29/16 | 117 |
|  5.3 Close out project with Stakeholders  | 1 day | **Mon 2/29/16** | Mon 2/29/16 | 118 |
|  5.4 Project Closure is Complete  | 1 day | **Mon 2/29/16** | Mon 2/29/16 | 119 |

## 9.0 Project Milestones

|  |  |
| --- | --- |
| **Milestone** | **Description** |
| Development | The first step in the Bitlocker rollout is to develop and test all the code that will be necessary to manage Bitlocker recovery keys. The deliverables will be code (1) to report the status on TPM chips, (2) code to manage the recovery keys, (3) code to report on Bitlocker compliance, and (4) code for support staff and (5) general administration (backup). |
| TPM Enable | Once all the code has been developed and tested, the next milestone will be to enable TPM chips on all workstations. This stage is critical to the overall process, because without the TPM being turned on, the recovery keys have no place to be stored. Now, there is a possible USB storage solution, however, to keep project costs (and TCO) low, the TPM chip has been selected as the best, cheapest recovery key storage option. This milestone will be complete when all TPM chips have been enabled. The deliverable will be a report stating the status of all TPM chips. |
| TPM Management | After the TPM chips have been enabled, the step stage of the process will be to collect Bitlocker recovery keys. Because I have chosen not to buy a Bitlocker management system, I will use code I have created to manage the retrieval and storage of Bitlocker recovery information. For this step, I will use SCCM or LANDesk (desktop management software) to deploy my TPM management scripted application. The TPM management does four things (1) Activates the TPM Chip, (2) takes ownership of the TPM, (3) adds protectors to the TPM, and (4) starts and pauses Bitlocker encryption. The deliverables for this milestone is a report verifying that TPM Management was indeed successful and a user manual explaining the segments of code used in Bitlocker reporting and management. |

## 10.0 Project Risk Assessment

While Bitlocker is already built-in to most of Microsoft’s active operating systems, some problems may arise due to hardware or software failure. It is important to note, overall risks are very low because if the Bitlocker process does not work, in nearly 100% of the cases the user’s computer is fine to use; they just will not have Bitlocker. For the machines that Bitlocker was not installed, refer to the following chart.

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk** | **Description** | **Mitigation** | **Role** |
| Failed TPM due to outdated BIOS | In rare cases, less than 1%, the computer’s BIOS may need to be updated to enable TPM. | BIOS will be manually updated. | Local Technician |
| Failed TPM due to motherboard | In rare cases, less than 1%, the computer’s motherboard will not have a TPM Chip. | Computer will be replaced with either a loaner machine or new computer. | Local Technician |
| Failed key import into Active Directory | The recovery key does not get imported into Active Directory | Try automated process again. Import key manually. | IT Specialist |
| Failed key import into Active Directory | The recovery key does not get imported into Active Directory | Verify computer is in a domain, and is in the proper OU.Or, enable, ‘Turn on TPM backup to Active Directory Domain Services’ in Local Group Policy | IT Specialist |
| Failed transport of key via email | The recovery key does not transport email service account | Try automated process again. Copy key from Active Directory, or FTP. Transfer manually. | IT Specialist |
| Failed transport of key to FTP server | The recovery key does not transport to FTP server | Try automated process again. Copy key from Active Directory or email. Transfer manually. | IT Specialist |
| Failed key import into LANDesk | The recovery key does not get imported into LANDesk Desktop Management Software | Reinstall LANDesk Agent. Try automated TPM Management. | Local Technician |
| User is receiving prompt to enter Bitlocker Recovery Password | When the user restarts their machine, they may receive a prompt to enter the Bitlocker Recovery Key | Enter the key from AD, FTP, Email, or LANDesk. Check TPM Chip status. Try automated TPM Management | IT Specialist |
| TPM cannot continue due to ownership error | The TPM ownership must be set before adding protectors to the TPM Chip | Take ownership of the TPM Chip, manually. Try automated TPM Management | IT Specialist |

## 11.0 Communication Plan

Due to the magnitude of the Bitlocker project, and the impact it will have on client users, the business must communicate to end-users what Bitlocker is and why encryption is important. The users must also be notified that encryption will become mandatory and enforced via company policy. The communication plan can be seen in the following table.

|  |  |
| --- | --- |
| **Title** | **Communication** |
| CIO | Will communicate to the enterprise via email and in quarterly meetings. A summary of the project will be sent out to employees to prepare them for Bitlocker deployment. |
| IT Team Leader | Will create documentation and train IT staff on Bitlocker maintenance and administration. |
| IT Specialist | Will train the IT Team Leader and demonstrate Bitlocker in Stakeholder meetings. Will also be responsible for weekly status updates via email to Stakeholders. |
| IT Manager | Will go over the current status of the Bitlocker in bi-weekly IT meetings. |

# Approval and Authority to Proceed

We approve the project as described above, and authorize the team to proceed.

|  |  |  |
| --- | --- | --- |
| Print Name | Title | Sign |
| Daryl Smith | CFO | Daryl Smith |
| John Brown | CIO | John Brown |
| Tina Pippins | Change Management | Tina Pippins |
| Larry Johnson | Senior Software Developer | Larry Johnson |
| Dalia Stoffer | IT Manager | Dalia Stoffer |
| Leslie Lee | IT Team Lead | Leslie Lee |

## Milestone Reports

**Milestone 1 Report**

 In milestone 1, the primary focus is on software development. The development stage includes programming the scripts necessary for Bitlocker deployment and administration, performing all unit testing, and completing user acceptance testing, or UaT. The development portion is broken down as follows:

* A script to report the status on TPM chips
* A script to manage recovery key imports
* A script to report on Bitlocker compliance
* A script for support staff (to pull a Bitlocker password)
* A script to perform the backup of Bitlocker passwords

Rather than providing the code for the scripts—which can be viewed in the *Bitlocker Coding* section of this project—the general ideas and concepts in the development process are discussed. To reduce problems associated in the software development stage, i.e. software quality and scope creep, it is common that a standardized, proven methodology will be applied to the coding process. One of these methodologies is known as SDLC. SDLC, or software development life cycle, was used as a guideline in milestone 1. Because the design, development, and testing of the scripts were essential to reaching milestone 1, the SDLC methodology became critical to the overall development process. Specifically, the script development included analyzing what was needed, then a scripted design was created around those needs, the code was developed and tested, and eventually, the process reached the final stage. The SDLC flow chart can be seen in Figure 1.

**■ Figure 1 SDLC Flow Chart**


Once all the coded pieces passed the user acceptance stage, the key stakeholders signed off the development stage and the go-live stage was approved.
 Considering each script, there were five scripts coded for the business, these were based upon business need and technical support requests. The scripts include (1) check TPM status, (2) TPM management, (3) Bitlocker compliance, (4) helpdesk support, and (5) backup Bitlocker Passwords. The basic flow and thought process behind these scripts can be seen in the following chart.

|  |  |
| --- | --- |
| **Script** | **Reasoning/Business Requirement** |
| Check TPM Status | Before enabling Bitlocker, a script is required to query the current status of the chip. If off, enable chip. |
| TPM Management | After the TPM chip has been enabled, ownership of the TPM must be taken, protectors must be added to the TPM, and the recovery information needs to be imported into Active Directory and LANDesk. |
| Bitlocker Compliance | There needs to be a way to verify which workstations do and do not meet Bitlocker compliance. |
| Helpdesk Support | Support staff will need an easy way to retrieve a single Bitlocker password, independently of accessing Active Directory or LANDesk. |
| Backup | There is a business need to maintain a backup of Bitlocker passwords for disaster recovery. This should be in form of a simple text file. |

Each of these scripts were completed on time and within budget. As stated, the SDLC methodology was used to guide the development and testing process. The stages of programming went through alpha, beta, and pilot phases. In the alpha and beta phases, software issues were identified, they were fixed, and each script was tested again. At the end of those two phases a status email was sent to the stakeholders. The email can be seen in Figure 2.
**■ Figure 2 Email Sent to Stakeholders**

In the pilot phase, which was the officially the UaT stage, five test users were selected from each site—Ohio, Arizona, and Florida. These users received the TPM Status and TPM Management scripts without any pending issues. Additionally, the Compliance, Helpdesk Support, and Backup scripts were evaluated for proper operation. All scripts worked as intended, consequently leading to the go-live approval from the stakeholders. Lastly, the technical documentation was transferred to the IT Team Leader, to be reviewed, updated, and disseminated accordingly. Milestone 1 is now considered complete.

**Milestone 2 Report**

*Report to be added here.*

**Milestone 3 Report**

*Report to be added here.*

## Lessons Learned

*Slides to be added here.
slide 1*

*Slides to be added here.
slide 2*

*Slides to be added here.
slide 3*

*Slides to be added here.
slide 4*

*Slides to be added here.
slide 5*

*Slides to be added here.
slide 6*

*Slides to be added here.
slide 7*

*Slides to be added here.
slide 8*

*Slides to be added here.
slide 9*

*Slides to be added here.
slide 10*

## Technical Documentation

*Preface*

This documentation is setup in the form of Problem and Solution; the Problem being a Bitlocker reporting or maintenance need, and the Solution being a script that has been developed and implemented in a production environment. Because this particular implementation of Bitlocker is not utilizing MBAM, MDOP, SQL, or any other reporting and compliance solution, customized scripts were created to fulfil the needs of Company X. The business requirements included reporting the current status of the TPM chip, enabling the TPM chip, importing the critical Bitlocker recovery information into Active Directory and LANDesk, and other miscellaneous support tools. The primary reason these scripts were engineered were to avoid current and future costs related to owning and operating a Microsoft or third party management solution, i.e. licensing and software support fees. Although every effort has be made to ensure the reliability and efficiency of the scripts, all the code should be tested in a lab before being introduced into a production environment. The documentation includes scripts coded in PowerShell, batch shell, and VBScript. It is also important to note, all the scripts where compiled into secure EXE files before entering a live environment.

**Bitlocker Coding**

**Check TPM Status**

Problem

Before starting the Bitlocker encryption process, a workstation must first have a working, enabled TPM chip. The TPM chip is used to securely store the Bitlocker recovery information. So, the question is: How can the status of the TPM be checked to verify that it is indeed on? Also, if the TPM status is disabled, steps should be taken to attempt to enable the chip, as well as a ‘failed’ status should be reported to LANDesk. If the chip is enabled, a ‘passed’ status should be reported to LANDesk.

SolutionCreate a batch script that uses *manage-bde.exe* to output the status of Bitlocker; that output will be scanned for specific a specific keyword: ‘not’(as in TPM *not* found). If ‘not’ is found, the script uses the HP BIOS Utility [*BIOSConfigUtility.exe*](http://ftp.hp.com/pub/caps-softpaq/cmit/whitepapers/HP_BCU_FAQ.pdf)to set a BIOS password, which is required by some computers to enable the TPM Chip. Next, the script runs the Microsoft VBScript [*EnableBitlocker.vbs*](https://gallery.technet.microsoft.com/scriptcenter/780d167f-2d57-4eb7-bd18-84c5293d93e3) to enable the TPM. The ‘FAILED’ status of the TPM is sent back to LANDesk and is also stamped in the registry. Now, if ‘not’ cannot be found, it is assumed that the TPM is enabled. Consequently, a ‘PASSED’ status will be returned to LANDesk as well as being stamped in the registry. This batch script was created to run from LANDesk *before* continuing to the Bitlocker recovery key import stage. By first ensuring that TPM chips are enabled, the import process will go much smoother. A TPM Status Check can be observed in Figure 3.

**■ Figure 3 TPM Status Check in LANDesk**



The Script

@**ECHO** ON

REM CHECK TPM STATUS - IF TPM 'NOT' FOUND IS RETURNED, GOTO FAILED ELSE GOTO PASSED

C:\windows\system32\manage-bde -tpm -TurnOn **|** findstr /f "**not**" && **GOTO** :FAILED

**GOTO** :PASSED

**:FAILED**

**CLS**

COLOR 0c

**ECHO** ERROR: A compatible Trusted Platform Module (TPM) was not detected.

**ECHO**.

REM SEND FAILED TO LANDESK

**IF EXIST** "C:\Program Files (x86)\LANDesk\LDClient\SDCLIENT.EXE" "C:\Program Files (x86)\LANDesk\LDClient\SDCLIENT.EXE" /msg**=**"FAILED"

**IF EXIST** "C:\Program Files\LANDesk\LDClient\SDCLIENT.EXE" "C:\Program Files\LANDesk\LDClient\SDCLIENT.EXE" /msg**=**"FAILED"

**ECHO** **%DATE%** **%TIME%** Sent FAILED message to LANDesk**>>**C:\Bitlocker\log.dat

C:\windows\system32\REG.exe ADD HKLM\SOFTWARE\Bitlocker /v TPM\_Status /d FAILED /t REG\_SZ /f

C:\windows\system32\REG.exe ADD HKLM\SOFTWARE\Bitlocker /v Timestamp /d "**%DATE%** **%TIME%**" /t REG\_SZ /f

REM IF TPM ENABLER IS FOUND (A SCRIPT FROM MICROSOFT), RUN SCRIPT WITH 'ON' OPTION AND SET BIOS PASSWORD USING SETPW.EXE

REM WIN7

**IF EXIST** "C:\Program Files (x86)\LANDesk\LDClient\sdmcache\apps\Bitlocker\\enablebitlocker.vbs" (

REM HP BIOS CONFIGURATION UTILITY - SET BIOS PASSWORD - REQUIRED TO ENABLE SOME TPM CHIPS

"C:\Program Files (x86)\LANDesk\LDClient\sdmcache\apps\Bitlocker\BIOSConfigUtility.exe" /nspwdfile:""C:\Program Files (x86)\LANDesk\LDClient\sdmcache\apps\Bitlocker\password.bin"

REM ENABLE TPM

"C:\Program Files (x86)\LANDesk\LDClient\sdmcache\apps\Bitlocker\enablebitlocker.vbs" /on:tpm /l:c:\setup\bitlocker.log

)

REM XP

**IF EXIST** "C:\Program Files\LANDesk\LDClient\sdmcache\apps\Bitlocker\enablebitlocker.vbs" (

REM SET BIOS PASSWORD - REQUIRED TO ENABLE SOME TPM CHIPS

"C:\Program Files\LANDesk\LDClient\sdmcache\apps\Bitlocker\BIOSConfigUtility.exe" /nspwdfile:""C:\Program Files\LANDesk\LDClient\sdmcache\apps\Bitlocker\password.bin"

REM ENABLE TPM

"C:\Program Files\LANDesk\LDClient\sdmcache\apps\Bitlocker\enablebitlocker.vbs" /on:tpm /l:c:\setup\bitlocker.log

)

REM LAUNCH RESTART COMPUTER PROMPT - SIMPLE EMPTY REBOOT HTA

**IF EXIST** "C:\Program Files (x86)\LANDesk\LDClient\sdmcache\apps\Bitlocker\RESTART.hta" (

start "" "C:\Program Files (x86)\LANDesk\LDClient\sdmcache\apps\Bitlocker\RESTART.hta"

)

**IF EXIST** "C:\Program Files\LANDesk\LDClient\sdmcache\apps\Bitlocker\RESTART.hta" (

start "" "C:\Program Files\LANDesk\LDClient\sdmcache\apps\Bitlocker\RESTART.hta"

)

**EXIT** /B 0

**:PASSED**

REM SEND PASSED TO LANDESK

**IF EXIST** "C:\Program Files (x86)\LANDesk\LDClient\SDCLIENT.EXE" "C:\Program Files (x86)\LANDesk\LDClient\SDCLIENT.EXE" /msg**=**"PASSED"

**IF EXIST** "C:\Program Files\LANDesk\LDClient\SDCLIENT.EXE" "C:\Program Files\LANDesk\LDClient\SDCLIENT.EXE" /msg**=**"PASSED"

**ECHO** **%DATE%** **%TIME%** Sent PASSED message to LANDesk**>>**C:\Bitlocker\log.dat

REM WRITE PASSED STATUS TO REGISTRY

C:\windows\system32\REG.exe ADD HKLM\SOFTWARE\Bitlocker /v TPM\_Status /d PASSED /t REG\_SZ /f

C:\windows\system32\REG.exe ADD HKLM\SOFTWARE\Bitlocker /v Timestamp /d "**%DATE%** **%TIME%**" /t REG\_SZ /f

**EXIT** /B 0

**TPM Management**

Problem

Once the TPM chip have been enabled, the next stage is to perform TPM management. Managing the TPM includes taking ownership of the TPM chip, adding protectors to the TPM, and importing the Bitlocker recovery information into Active Directory and LANDesk. Before starting the actual Bitlocker encryption process, it is critical that the recovery information be stored in central repositories (such as Active Directory). The consequence of not storing recovery information could prove disastrous, as Bitlocker requires a 48-digit recovery password to be entered under certain recovery circumstances (such as hard drive restoration and partition access from WinPE). The 48-digit recovery password will look something like this: 749474-424079-255893-309697-487611-671444-219460-369961.

Solution

To address each of the management requirements, a batch file was created that uses manage-bde, along with some branch logic. The script works by being deployed from LANDesk, and then is executed in the computer’s system account. Upon execution, it verifies the machine is online, and if so, takes ownership of the TPM, adds protectors to the TPM, and then proceeds to import the Bitlocker recovery information into Active Directory and LANDesk. Successful imports can be seen in Figure 4 and Figure 5.

**■ Figure 4 Successful Active Directory Import**

****

**■ Figure 5 Successful LANDesk Import**



The Script

@**ECHO** OFF

**CLS**

TITLE TPM Management

COLOR 0E

**SET** MyVar0**=**

**SET** MyVar1**=**

**SET** MyVar2**=**

**SET** FOUND**=**FALSE

**SET** CurDir**=%CD%**

SETLOCAL ENABLEDELAYEDEXPANSION

REM EXTRACTS FILES - CONTAINS ALL SOURCE FILES

**if exist** "C:\Program Files (x86)\LANDesk\LDClient\sdmcache\apps\Bitlocker\tpmman.exe" "C:\Program Files (x86)\LANDesk\LDClient\sdmcache\apps\Bitlocker\tpmman.exe"

**if exist** "C:\Program Files\LANDesk\LDClient\sdmcache\apps\Bitlocker\tpmman.exe" "C:\Program Files\LANDesk\LDClient\sdmcache\apps\Bitlocker\tpmman.exe"

REM PRIMARY PATH CHANGE

**Set** CurDir**=**C:\Bitlocker

REM SECONDARY PATH CHANGE

**C:**

**CD** C:\Bitlocker

REM TEST FOR ONLINE STATUS

**:VERIFYCOM**

**CLS**

**ECHO** Detecting Internet connectivity...

ping -n 4 127.0.0.1**>nul**

REM CHECK ONLINE STATUS - google.com

ping www.google.**com** -n 1 **|** find "Reply" && **SET** FOUND**=**TRUE

**IF** [**%FOUND%**] EQU [TRUE] **GOTO** :FOUND ELSE

**CLS**

COLOR 0C

**Echo** No Internet Connection Found. Exiting now...

ping -n 10 127.0.0.1**>nul**

**exit** /b 1

**:FOUND**

**CLS**

COLOR 0A

**ECHO** Internet Connection Found. Loading TPM Management...

ping -n 10 127.0.0.1**>nul**

**CLS**

COLOR 0B

**ECHO** Checking TPM Compliance...started

**ECHO** Taking Ownership of TPM...pending

**ECHO** Adding TPM Protector...pending

**ECHO** Adding TPM Recovery Password Protector...pending

**ECHO** Importing recovery information into Active Directory...pending

**ECHO** Importing recovery information into LANDesk...pending

REM CHECKS TO SEE IF TPM HAS ALREADY BEEN SETUP...IF YES, SKIP TO END, IF NO, CONTINUE TO CHECK1

**FOR** /f "tokens**=**1" **%%f in** ('"C:\windows\system32\manage-bde.exe -status"') **DO SET** MyVar0**=%%f**

**IF** ["**%MyVar0%**"] EQU ["Numerical"] **GOTO** :PASSED2

**IF NOT EXIST** C:\Bitlocker (

**MD** C:\Bitlocker

**ECHO** **%DATE%** **%TIME%** Created C:\Bitlocker folder.**>>**C:\Bitlocker\log.dat

)

**:CHECK1**

REM TAKE OWNERSHIP

C:\windows\system32\manage-bde -tpm -takeownership AddYourPasswordHere

REM CHECK TO SEE IF TPM HAS NO PROTECTORS

**for** /f "skip**=**4 tokens**=**2 delims**=**:" **%%g in** ('"C:\windows\system32\manage-bde.exe -protectors -get c:"') **do set** MyVar1**=%%g**

C:\windows\system32\ping.exe -n 10 127.0.0.1**>nul**

**IF** ["**%MyVar1%**"] EQU [" No key protectors found."] **GOTO** :TPMMGN

**GOTO** :ADIMP

**:TPMMGN**

**ECHO** **%DATE%** **%TIME%** No Key Protectors Found.**>>**C:\Bitlocker\log.dat

**ECHO** **%DATE%** **%TIME%** Starting TPM Management.**>>**C:\Bitlocker\log.dat

REM THIS IS THE TPM MANAGEMENT ROUTINE

**CLS**

**ECHO** Checking TPM Compliance...DONE.

**ECHO** Taking Ownership of TPM...started

**ECHO** Adding TPM Protector...pending

**ECHO** Adding TPM Recovery Password Protector...pending

**ECHO** Importing recovery information into Active Directory...pending

**ECHO** Importing recovery information into LANDesk...pending

**ECHO**.

**ECHO**.

C:\windows\system32\manage-bde -tpm -takeownership AddYourPasswordHere

**ECHO** **%DATE%** **%TIME%** Taking Ownership of TPM.**>>**C:\Bitlocker\log.dat

**CLS**

**ECHO** Checking TPM Compliance...DONE.

**ECHO** Taking Ownership of TPM...DONE.

**ECHO** Adding TPM Protector...started

**ECHO** Adding TPM Recovery Password Protector...pending

**ECHO** Importing recovery information into Active Directory...pending

**ECHO** Importing recovery information into LANDesk...pending

**ECHO**.

**ECHO**.

**ECHO** **%DATE%** **%TIME%** Adding TPM Protector.**>>**C:\Bitlocker\log.dat

C:\windows\system32\manage-bde.exe -protectors -add C: -tpm

**CLS**

**ECHO** Checking TPM Compliance...DONE.

**ECHO** Taking Ownership of TPM...DONE.

**ECHO** Adding TPM Protector...DONE.

**ECHO** Adding TPM Recovery Password Protector...started

**ECHO** Importing recovery information into Active Directory...pending

**ECHO** Importing recovery information into LANDesk...pending

**ECHO**.

**ECHO**.

**ECHO** **%DATE%** **%TIME%** Adding Recovery Password Protector.**>>**C:\Bitlocker\log.dat

C:\windows\system32\manage-bde.exe -protectors -add C: -recoverypassword

**GOTO** :CHECK2

**:CHECK2**

**for** /f "skip**=**4 tokens**=**2 delims**=**:" **%%h in** ('"C:\windows\system32\manage-bde.exe -protectors -get c:"') **do set** MyVar2**=%%h**

C:\windows\system32\ping.exe -n 10 127.0.0.1**>nul**

**IF** ["**%MyVar2%**"] NEQ [" No key protectors found."] **GOTO** :ADIMP

**ECHO** **%DATE%** **%TIME%** Adding Protectors failed. TPM has not been enabled.**>>**C:\Bitlocker\log.dat

**GOTO** :FAILED

**:ADIMP**

REM IMPORT RECOVERY INFO INTO AD

**CLS**

**ECHO** Checking TPM Compliance...DONE.

**ECHO** Taking Ownership of TPM...DONE.

**ECHO** Adding TPM Protector...DONE.

**ECHO** Adding TPM Recovery Password Protector...DONE.

**ECHO** Importing recovery information into Active Directory...started

**ECHO** Importing recovery information into LANDesk...pending

**ECHO**.

**ECHO**.

**ECHO** **%DATE%** **%TIME%** Starting AD Recovery Import.**>>**C:\Bitlocker\log.dat

C:\windows\system32\manage-bde.exe -protectors -adbackup c: -id**%MyVar2%** && **GOTO** :LDIMP

REM LOG

**ECHO** **%DATE%** **%TIME%** AD Recovery Import failed**>>**C:\Bitlocker\log.dat

REM STAMP REGISTRY

C:\windows\system32\REG.exe ADD HKLM\SOFTWARE\Bitlocker /v AD\_Import /d FAILED /t REG\_SZ /f

C:\windows\system32\REG.exe ADD HKLM\SOFTWARE\Bitlocker /v LD\_Import /d FAILED /t REG\_SZ /f

**GOTO** :FAILED

**:LDIMP**

REM LOG

**ECHO** **%DATE%** **%TIME%** AD Recovery Import was successful.**>>**C:\Bitlocker\log.dat

REM STAMP REGISTRY

C:\windows\system32\REG.exe ADD HKLM\SOFTWARE\Bitlocker /v AD\_Import /d PASSED /t REG\_SZ /f

REM IMPORT RECOVERY INFO INTO LANDESK

**CLS**

**ECHO** Checking TPM Compliance...DONE.

**ECHO** Taking Ownership of TPM...DONE.

**ECHO** Adding TPM Protector...DONE.

**ECHO** Adding TPM Recovery Password Protector...DONE.

**ECHO** Importing recovery information into Active Directory...DONE.

**ECHO** Importing recovery information into LANDesk...started

**ECHO**.

**ECHO**.

**ECHO** **%DATE%** **%TIME%** Starting LANDesk Recovery Import.**>>**C:\Bitlocker\log.dat

**if exist** "C:\Program Files (x86)\LANDesk\LDClient\sdmcache\apps\Bitlocker\tpmman.exe" **call** "c:\Bitlocker\LDCustom64.cmd"

**if exist** "C:\Program Files\LANDesk\LDClient\sdmcache\apps\Bitlocker\tpmman.exe" **call** "c:\Bitlocker\LDCustom32.cmd"

C:\windows\system32\ping.exe -n 10 127.0.0.1**>nul**

REM ADD TEST FOR LD STILL HAVE TO DO THIS VERIFICATION ROUTINE

REM LOG

**ECHO** **%DATE%** **%TIME%** LANDesk Recovery Import was successful.**>>**C:\Bitlocker\log.dat

C:\windows\system32\REG.exe ADD HKLM\SOFTWARE\Bitlocker /v LD\_Import /d PASSED /t REG\_SZ /f

**GOTO** :PASSED

**:PASSED**

REM THIS IS FOR 1st PASS

**ECHO** **%DATE%** **%TIME%** TPM Compliance PASSED. Numerical ID was created.**>>**C:\Bitlocker\log.dat

**CLS**

**ECHO** Checking TPM Compliance...DONE.

**ECHO** Taking Ownership of TPM...DONE.

**ECHO** Adding TPM Protector...DONE.

**ECHO** Adding TPM Recovery Password Protector...DONE.

**ECHO** Importing recovery information into Active Directory...DONE.

**ECHO** Importing recovery information into LANDesk...DONE.

**ECHO**.

**ECHO** Computer meets TPM Compliance.

**ECHO**.

REM STAMP REGISTRY

C:\windows\system32\REG.exe ADD HKLM\SOFTWARE\Bitlocker /v TPM\_Status /d PASSED /t REG\_SZ /f

C:\windows\system32\REG.exe ADD HKLM\SOFTWARE\Bitlocker /v Timestamp /d "**%DATE%** **%TIME%**" /t REG\_SZ /f

REM SEND MESSAGE TO LANDESK

**if exist** "C:\Program Files (x86)\LANDesk\LDClient\SDCLIENT.EXE" "C:\Program Files (x86)\LANDesk\LDClient\SDCLIENT.EXE" /msg**=**"PASSED"

**if exist** "C:\Program Files\LANDesk\LDClient\SDCLIENT.EXE" "C:\Program Files\LANDesk\LDClient\SDCLIENT.EXE" /msg**=**"PASSED"

**ECHO** **%DATE%** **%TIME%** Sent PASSED message to LANDesk.**>>**C:\Bitlocker\log.dat

manage-bde -on c: -s

C:\windows\system32\ping.exe -n 10 127.0.0.1**>nul**

manage-bde -pause c:

**CLS**

**ECHO** Passed.

C:\windows\system32\ping.exe -n 6 127.0.0.1**>nul**

**GOTO** :END

**:PASSED2**

REM THIS IS FOR 2nd PASS

**ECHO** **%DATE%** **%TIME%** TPM Compliance PASSED. Found Numerical ID.**>>**C:\Bitlocker\log.dat

**CLS**

**ECHO** Checking TPM Compliance...DONE.

**ECHO** Taking Ownership of TPM...DONE.

**ECHO** Adding TPM Protector...DONE.

**ECHO** Adding TPM Recovery Password Protector...DONE.

**ECHO** Importing recovery information into Active Directory...DONE.

**ECHO** Importing recovery information into LANDesk...DONE.

**ECHO**.

**ECHO** Computer meets TPM Compliance.

**ECHO**.

REM SEND MESSAGE TO LANDESK

**if exist** "C:\Program Files (x86)\LANDesk\LDClient\SDCLIENT.EXE" "C:\Program Files (x86)\LANDesk\LDClient\SDCLIENT.EXE" /msg**=**"PASSED"

**if exist** "C:\Program Files\LANDesk\LDClient\SDCLIENT.EXE" "C:\Program Files\LANDesk\LDClient\SDCLIENT.EXE" /msg**=**"PASSED"

**ECHO** **%DATE%** **%TIME%** Sent PASSED message to LANDesk.**>>**C:\Bitlocker\log.dat

C:\windows\system32\REG.exe ADD HKLM\SOFTWARE\Bitlocker /v TPM\_Status /d PASSED /t REG\_SZ /f

C:\windows\system32\REG.exe ADD HKLM\SOFTWARE\Bitlocker /v Timestamp /d "**%DATE%** **%TIME%**" /t REG\_SZ /f

manage-bde -on c: -s

C:\windows\system32\ping.exe -n 10 127.0.0.1**>nul**

manage-bde -pause c:

**ECHO** Passed.

C:\windows\system32\ping.exe -n 6 127.0.0.1**>nul**

**GOTO** :END

**:FAILED**

manage-bde -protectors -delete c:

**ECHO** **%DATE%** **%TIME%** TPM Compliance FAILED. Check TPM.**>>**C:\Bitlocker\log.dat

**ECHO** **%DATE%** **%TIME%** Deleted Recovery Info to start over**>>**C:\Bitlocker\log.dat

**CLS**

**ECHO** FAILED!

REM SEND MESSAGE TO LANDESK

**if exist** "C:\Program Files (x86)\LANDesk\LDClient\SDCLIENT.EXE" "C:\Program Files (x86)\LANDesk\LDClient\SDCLIENT.EXE" /msg**=**"FAILED"

**if exist** "C:\Program Files\LANDesk\LDClient\SDCLIENT.EXE" "C:\Program Files\LANDesk\LDClient\SDCLIENT.EXE" /msg**=**"FAILED"

**ECHO** **%DATE%** **%TIME%** Sent FAILED message to LANDesk**>>**C:\Bitlocker\log.dat

C:\windows\system32\REG.exe ADD HKLM\SOFTWARE\Bitlocker /v TPM\_Status /d FAILED /t REG\_SZ /f

C:\windows\system32\REG.exe ADD HKLM\SOFTWARE\Bitlocker /v Timestamp /d "**%DATE%** **%TIME%**" /t REG\_SZ /f

C:\windows\system32\ping.exe -n 10 127.0.0.1**>nul**

**ECHO** Failed.

C:\windows\system32\ping.exe -n 6 127.0.0.1**>nul**

**GOTO** :END

**exit** /b 0

**:END**REM PERFORM CLEANUP

**IF EXIST** c:\bitlocker\LDCustom32.cmd **DEL /Q** c:\bitlocker\LDCustom32.cmd

**IF EXIST** c:\bitlocker\LDCustom64.cmd **DEL /Q** c:\bitlocker\LDCustom64.cmd

**IF EXIST** c:\bitlocker\LDSCNHLP32.INI **DEL /Q** c:\bitlocker\LDSCNHLP32.INI

**IF EXIST** c:\bitlocker\LDSCNHLP64.INI **DEL /Q** c:\bitlocker\LDSCNHLP64.INI

**EXIT** /B 0

**Active Directory Bitlocker Compliance Report**

Problem

Once TPM Chips have been enabled, and TPM Management has been carried out, Bitlocker encryption can be started. Although the Bitlocker recovery information is being stored in Active Directory, there is no built-in way to audit and report on Bitlocker compliance throughout the enterprise. Thus, steps must be taken to create an automated method of reporting Bitlocker compliance.

SolutionTo address the Active Directory Bitlocker compliance request, a PowerShell script was created to scan computer objects in Active Directory, and return ‘true’ or ‘false’ on the status of Bitlocker. The recovery key and owner information are returned and outputted to a CSV file. This script is meant to be ran by the compliance officer or Bitlocker administrator. The compliance report can be seen in Figure 6.

**■ Figure 6 Active Directory Bitlocker Compliance Report**



The Script

#SET REPORT NAME

$CsvFilePath **=** "REPORT\_AD\_BitLockerCompliance.csv"

#LOAD COMPUTER OBJECTS BASED ON OBJECT PROPERTIES

$BitLockerEnabled **=** Get**-**QADObject **-**SizeLimit **0** **-**IncludedProperties Name**,**ParentContainer **|** Where**-**Object **{**$\_.type **-**eq "msFVE-RecoveryInformation"**}** **|** Foreach**-**Object **{**Split**-**Path **-**Path $\_.ParentContainer **-**Leaf**}** **|** Select**-**Object **-**Unique

$strComputers **=** Get**-**QADComputer **-**SizeLimit **0** **-**IncludedProperties Name**,**OperatingSystem**,**msTPM**-**OwnerInformation **|** Where**-**Object **{**$\_.operatingsystem **-**like "Windows 7\*" **-**or $\_.operatingsystem **-**like "Windows Vista\*"**}** **|** Sort**-**Object Name

#CREATE ARRAY TO HOLD COMPUTER INFORMATION

$ExportToArray **=** @**()**

foreach **(**$strComputer in $strComputers**)**

 **{**

 #Create object for each computer

 $strComputerObj **=** New**-**Object **-**TypeName psobject

 $HOST.UI.RawUI.ReadKey**(**"NoECHO,IncludeKeyDown"**)** **|** OUT**-**NULL

 $HOST.UI.RawUI.Flushinputbuffer**()**

 #Add name and OS

 $strComputerObj **|** Add**-**Member **-**MemberType NoteProperty **-**Name Name **-**Value $strComputer.Name

 $strComputerObj **|** Add**-**Member **-**MemberType NoteProperty **-**Name OperatingSystem **-**Value $strComputer.operatingsystem

 #SET HasBitlockerRecoveryKey to true or false

 if **(**$strComputer.name **-**match **(**'(' + [string]::Join(')|(', $bitlockerenabled) + ')')) {

 $strComputerObj **|** Add**-**Member **-**MemberType NoteProperty **-**Name HasBitlockerRecoveryKey **-**Value $true

 **}**

 else

 **{**

 $strComputerObj **|** Add**-**Member **-**MemberType NoteProperty **-**Name HasBitlockerRecoveryKey **-**Value $false

 **}**

 #SET HasTPM-OwnerInformation to true or false

 if **(**$strComputer."msTPM-OwnerInformation"**)** **{**

 $strComputerObj **|** Add**-**Member **-**MemberType NoteProperty **-**Name HasTPM**-**OwnerInformation **-**Value $true

 **}**

 else

 **{**

 $strComputerObj **|** Add**-**Member **-**MemberType NoteProperty **-**Name HasTPM**-**OwnerInformation **-**Value $false

 **}**

#Add the computer object to the array

$ExportToArray **+=** $strComputerObj

 **}**

#Export the array with computer information
$ExportToArray **|** Export**-**Csv **-**Path $CsvFilePath **-**NoTypeInformation

**Helpdesk Support/Tech Support**

Problem

Although the Bitlocker recovery information is in Active Directory, not everyone will have the Active Directory User console installed on their machines. This presents a support challenge in the scenario that helpdesk or other support personnel need access to the 48-digit Bitlocker password.

Solution
To address this ease of access issue, a PowerShell script has been created to allow support staff to enter a specific computer name and the Bitlocker recovery password will be returned. The scripting input and output can be seen in Figure 7.

**■ Figure 7 Support Staff Recovery Script**


The Script

clear

#Retrieve user input

$strComputer = Read-Host 'Enter Computer Name'

#Import AD commands

Import-Module ActiveDirectory

#Check AD Object

$strComputerObject = Get-ADComputer -Filter {cn -eq $strComputer} -Property msTPM-OwnerInformation, msTPM-TpmInformationForComputer

if($strComputerObject -eq $null){

 Write-Host "Computer object not found. EXITing the script..."

 %compspec% /c PAUSE

 EXIT

}

#msTPM-OwnerInformation attribute

if($strComputerObject.'msTPM-OwnerInformation' -eq $null){

 #Check TPM info is backed up to AD

 if($strComputerObject.'msTPM-TpmInformationForComputer' -ne $null){

 # Retrieve TPM Owner Password

 $TPMObject = Get-ADObject -Identity $strComputerObject.'msTPM-TpmInformationForComputer' -Properties msTPM-OwnerInformation

 $TPMKey = $TPMObject.'msTPM-OwnerInformation'

 }else{

 $TPMKey = '<not SET>'

 }

}else{

 #TPM Owner Password

 $TPMKey = $strComputerObject.'msTPM-OwnerInformation'

}

#Check computer object AD BitLocker Recovery Password

$BitLockerObject = Get-ADObject -Filter {objectclass -eq 'msFVE-RecoveryInformation'} -SearchBase $strComputerObject.DistinguishedName -Properties 'msFVE-RecoveryPassword' | Select-Object -Last 1

if($BitLockerObject.'msFVE-RecoveryPassword'){

 $BitLockerKey = $BitLockerObject.'msFVE-RecoveryPassword'

}else{

 $BitLockerKey = '<not SET>'

}

#Return Info to screen

clear

Write-Host 'Recovery Password:' $BitLockerKey

#Export TPM Owner Password File

if($strComputerObject.'msTPM-TpmInformationForComputer' -ne $null){

 $ExportToArrayToFile = Read-Host 'Would you like to export the recovery key [y or n]'

 if($ExportToArrayToFile -ne 'y'){

 EXIT

 }

 $TPMFile = '<?xml version="1.0" encoding="UTF-8"?><ownerAuth>' + $TPMKey + '</ownerAuth>'

 $TPMFile | Out-File "TPMOwnerPasswordFile.tpm"

}else{

 Cmd /c PAUSE

}

**Backup Bitlocker Passwords**

Problem

The Bitlocker recovery information is in Active Directory and in LANDesk, however there may be need to export or backup the Bitlocker passwords. This will useful for disaster recovery, and is considered best practice to maintain a secondary or even tertiary copy of the Bitlocker passwords. Thus, measures should be taken to back up the passwords to a text or CSV file.

Solution
To address the backup requirement, a PowerShell script was written which uses the Import-Module ActiveDirectory cmdlet. A sample report can be observed in Figure 8. Note, this text file is comma delimited, which can be easily converted to an Excel or CSV report.

**■ Figure 8 Backup of Bitlocker Passwords**



The Script

Import-Module ActiveDirectory

**$ou** **=** Get-ADObject **-Filter** **{** ObjectClass **-**eq 'organizationalunit' **}** **-**SearchBase "OU=Workstations,,DC= YourDomainName,DC=com"

**foreach** **($obj** **in** **$ou)** **{**

Get-ADComputer **-Filter** 'ObjectClass -eq "computer"' **-**SearchBase **$obj** **-**ErrorAction SilentlyContinue **-**ResultPageSize 2000 **|** foreach-object **{**

**$Computer** **=** **$\_.**name

#Check if the Computer Object exists

**$Computer\_Object** **=** Get-ADComputer **-Filter** **{**cn **-**eq **$Computer}** **-**Property msTPM-OwnerInformation**,** msTPM-TpmInformationForComputer

#Check if the computer object has had a BitLocker Recovery Password

**$Bitlocker\_Object** **=** Get-ADObject **-Filter** **{**objectclass **-**eq 'msFVE-RecoveryInformation'**}** **-**SearchBase **$Computer\_Object.**DistinguishedName **-**Properties 'msFVE-RecoveryPassword' **|** Select-Object **-**Last 1

**if($Bitlocker\_Object.**'msFVE-RecoveryPassword'**){**

 **$Bitlocker\_Key** **=** **$Bitlocker\_Object.**'msFVE-RecoveryPassword'

**}else{**

 **$Bitlocker\_Key** **=** '<not set>'

**}**

#Display Output

**$strToReport** **=** **$Computer** **+** "," **+** **$Bitlocker\_Key**

Write-Host **$strToReport**

#Save to Report

**$strToReport** **|** Out-File Report**.**txt **-**append

 **}** # end for-each

**}** # end for-each

 References

BenefitOf. (n.d.). Benefits of Bitlocker. Retrieved from http://benefitof.net/benefits-of-bitlocker/

Brown, Dehayes, Hoffer, Martin, & Perkins. (2012). *Managing information technology,* 7th ed. Prentice Hall, Pearson.

Venkata. (2012). What is sdlc? Retrieved from http://www.sdlc.ws/what-is-sdlc/