**IT Operations Plan**

|  |
| --- |
| **A. Current Environment Analysis** |
| **SaaS Operation:**  TreasureChest is a software as a service (SaaS) treasury management company that provides treasury functionality via the web to businesses around the world. The company offers a *monthly subscription* based on the number of users per subscription, and *Pro Services* professional services. The company monitors and manages its SaaS systems 24/7 and is currently facing a rapidly growing customer base, as it is increasing the number of large-business customers. This has led to an overwhelming amount of demands for TreasureChest’s SaaS service and a need for the functionality in the service to be more reliable.  The use of disparate systems in the different departments and locations, is causing problems in interoperability, flexibility, scalability, and communication. For example, this includes the use of separate instances of Salesforce.com by the Sales and Marketing Departments, along with a series of custom HTML5 and Force.com. Currently, there is no connection between Salesforce.com and the company’s business services and ERP system. The use of outdated and disparate software, hardware, and technologies means that many of the current IT implementations are no longer supported, which leaves them open to security vulnerabilities. |
| **Hardware:**  Each co-location site is owned by Equinix Systems, but TreasureChest owns the processing *hardware*, business software, and the product applications running on them. Renting the sites and upkeeping the hardware is expensive and requires specialist personnel to remain on duty 24/7. Most of the hardware is outdated and has outdated software installed on it. Newer software cannot be installed on these outdated machines, which hinders the growth of the company’s infrastructure and leaves the company open to security breaches. |
| **Operating Systems:**  TreasureChest develops and hosts its applications in four co-locations. The different applications are not always able to communicate with each other and employees in the different locations around the world, are rarely in steady communication and agreement on methods and protocols. The company’s treasury software application was first developed in 2007 and has been continually enhanced up to the present version. However, the condition of the application is an issue as the architecture has become seriously outdated, and it has become obvious to the company that the application needs rebuilding or re-architecture.  As mentioned above, the company is using outdated software and servers for its databases. There are separate databases and because of this there is a lack of communication among office locations around the word, the different departments, and employees in general. With outdated server technologies the company is vulnerable to security breaches. |
| **Networks:**  The IT operations team uses *OnsOne Ltd*., a banking network provider located in Paris to help monitor TreasureChest’s computing systems and networks 24/7. TreasureChest promises 99.95% availability and uptime in its contracts with its customers. However, that 5% downtime could be detrimental to customers who are trying to run their businesses using TreasureChest’s SaaS services. A growing customer base and an increase in large-business customers has led to an escalation of demands for the SaaS service and a need for increased reliability of the functionality in the service. |
| **Software:**  The use of separate instances of Salesforce.com by the Sales and Marketing Departments, along with a series of custom HTML5 and Force.com, means that there is no connection between Salesforce.com and the company’s business services and ERP system. Also, the company is using an outdated treasury software application (from 2007) on which the SaaS service is built. This means that the condition of the application is an issue because the architecture has become too outdated.  TreasureChest develops and hosts its applications in four co-locations. Disparate software methodologies are being used for development, and disparate software applications and technologies are being used to manage the different departments within the organization. Thus, there are problems with data integrity, communication, and redundance. Having different software technologies, which cannot communicate with each other, or that cannot be updated, is causing major problems with communication among the different departments in the company. These problems also leave the company vulnerable to major security breaches. |
| **Database:**  As mentioned above, TreasureChest is using an outdated software and servers for its databases. There are separate databases and because of this there is a lack of communication among office locations around the word, the different departments, and employees in general. Currently, is not possible to access data from a shared central location. TreasureChest is using outdated software and hardware for its databases. Because of this there is a lack of communication among office locations around the word, the different departments, and employees in general. With outdated server technologies the company is vulnerable to security breaches and extra expenses. |

|  |
| --- |
| B. **Update the technology operational workflow**. |
| **IT Operations Goals:**   1. Implement a Unified Communications system 2. Train the employees in how to use the new UC system 3. Improve and implement a uniform workflow script |

|  |
| --- |
| C. **Improve and upgrade the business system software** |
| **IT Operations Goals:**   1. Implement a unified ERP and CRM system 2. Train the employees in how to use the new ERP and CRM systems 3. Outsource the company’s software development for professional leased services |

|  |  |  |
| --- | --- | --- |
| D. First Strategic Goal- **B: Update the technology operational workflow.** | | |
| **IT Operational Goal** | **Enhancements needed to support the strategic objective** | **Planned activities to meet each objective** |
| **Goal B:1**  Implement a Unified Communications System | 1. New VOIP hardware device systems will be needed to be installed in all office locations, 2. Update operating systems and computers in all locations so that they could have the ability to run the new UC system. | 1. Once the project is approved, settle and disputes and sign any contracts. 2. Install required hardware and software. 3. Implement the new UC system. |
| **Goal B:2**  Train the employees in how to use the new UC system. | 1. Large screens or projectors will be needed for conference rooms for meetings. 2. A conferencing application which is capable of recording the meetings and providing live conferencing will be needed. | *Note: All meetings will be held virtually for those who cannot be physically present.*   1. Research and train executives in all locations. 2. Plan and schedule employee training sessions, together with at executives in all locations. 3. Procure and set up required equipment and conference locations for meetings. 4. Email the employees about educational sessions. 5. Carry out the training sessions. 6. Be available, along with the trained executive personnel, to assist employees as they begin to use the new system. |
| **Goal B:3**  Implement and enforce uniform workflow scripts | 1. New uniform workflow scripts will be created and implemented for all departments in the company that are IT related. 2. Scripts will need to be automated so that employees could interact and follow them on their devices. | 1. Give assignments to IT related department leaders to write new uniform workflow scripts. 2. Review and approve the workflow scripts 3. Create and install an automated version of the scripts 4. Email all employees who will be affected by the change. 5. Implement the workflow scripts. |

|  |  |  |
| --- | --- | --- |
| D. Second Strategic Goal- **C: Improve and upgrade the business system software** | | |
| **IT Operational Goal** | **Enhancements needed to support the strategic objective** | **Planned activities to meet each objective** |
| **Goal C:1**  Implement a unified ERP and CRM system | 1. Upgrade any computers which do not have the proper ability to run the modern ERP and CRM software. 2. Upgrade the service with internet service providers in all locations, where needed. | 1. Once the project is approved, settle and disputes and sign any contracts. 2. Upgrade computers as needed. 3. Upgrade internet service in all locations where needed. 4. Implement NetSuite’s unified ERP and CRM system. |
| **Goal C:2**  Train the employees in how to use the new ERP and CRM system | 1. Large screens or projectors will be needed for conference rooms for meetings. 2. Create supplemental training PowerPoints for employees to learn how to use the new ERP and CRM system. 3. Create supplemental interactive training quizzes to track employees’ comprehension of training. | *Note: All meetings will be held virtually for those who cannot be physically present.*   1. Research and train executives in all locations. 2. Plan and schedule employee training sessions, together with at executives in all locations. 3. Email the employees about educational sessions. 4. Carry out the training sessions. 5. Be available, along with the trained executive personnel, to assist employees as they begin to use the new system. |
| **Goal C:3**  Outsource the company’s software development for professional leased services | 1. Meetings with NetSuite and signing of contracts will be needed. 2. Professional leased software services, in this case, NetSuite’s SaaS services, will be needed to carry out this goal. | 1. Once the goal is approved, settle and disputes and sign any contracts. 2. Implement the new unified ERP and CRM system. 3. Eliminate unnecessary software development roles. |

|  |  |
| --- | --- |
| E. Sustainability Plan | |
| **One Year** | Throughout year one, the stage of which the company will be going through primarily isthe *Service Strategy* stage*.* ITIL will be introduced to “combat limitations or issues within current support processes” (Nyhuis, 2020). The objective of year one is to improve previous disparate processes and workflows used by the different departments, and especially to improve *efficiency* throughout the entire company. ITIL will be used to implement Comcast’s Unified Communications system, and to develop and monitor the new simple uniform workflow scripts.  In the beginning of the year, training sessions will be held to teach employees how to use the UC system and the workflow scripts. Throughout the year, quarterly meetings will be held with the department heads to determine how well the UC and the scripts are working. Based on these meetings, notes will be taken, and any improvements will be made. Ongoing training sessions for employees will be carried out as needed. The implementation of the UC system and of workflow scripts, using the ITIL framework will ensure uniformity and set “best-practice procedures and processes for IT and digital service management” (Nyhuis, 2020). |
| **Three Year** | Throughout year three, TreasureChest, will have implemented NetSuite’s unified CRM and ERP system, and would have outsourced the company’s software development for NetSuite’s leased professional services. The stages of ITIL which the company will be going through primarily are *Service Design* and *Transition.* It will be in a good position to set standards and best practices for the use of ITIL guidelines for employees using the CRM and ERP system throughout the company. Training sessions will take place throughout the company to ensure that employees know how to properly work with the unified CRM and ERP system. New ITIL guidelines will be implemented and improved as needed, on how employees use and operate the CRM and ERP system.  The objective of year three is to improve previous standards of efficiencyset in place by the improved workflow scripts and the use of the UC system from year one, and especially to *align services with the customers’ needs.* Throughout the year, quarterly meetings will be held with the department heads to determine how well the ITIL Framework is working, as the employees use the CRM and ERP system according to the new ITIL guidelines. Department heads will also be required to get ITIL certifications. Based on these meetings, notes will be taken, and any improvements will be made to the guidelines. |
| **Five Year** | Throughout year five, TreasureChest, will have been using NetSuite’s unified CRM and ERP system according to the improved ITIL guidelines, which were introduced in year three. The stages of ITIL which the company will be going through primarily are *Service Operation* and *Continual Service Improvement.* The objective of year five is to “produce a clear model for *ongoing success”* (Nyhuis, 2020). The company will focus on educating all employees in IT related departments on the ITIL Framework. Non-Executive employees will be encouraged to get ITIL certifications and regular, *ongoing* ITIL workshops will be held for all employees. |

|  |  |
| --- | --- |
| F. Enhancements and Security Risks | |
| **Enhancements** | **Security Risks and Plans to Address Risk** |
| **For Goal B:1** | **Implement a Unified Communications System** |
| 1. **New VOIP hardware device systems will be needed to be installed in all office locations** | * **Risk 1**   Unauthorized levels of access by employees.  ***Plan To Address Risk 1***  Roles and frequent password changes for all employees will be implemented, so that they can only access information according to their roles, and it will be difficult for other employees to track and use their secure authorizations.   * **Risk 2**   VOIP devices could be wire-tapped by an unlawful or unauthorized person to secretly listen in to private company information.  ***Plan to Address Risk 2***  Set up private VLAN in all locations. “The private VLAN acts as a single access and uplink point to connect the device to a router, server, or network” (Marvin, 2021). |
| 1. **Update operating systems and computers in all locations so that they could have the ability to run the new UC system.** | * **Risk 1**   Operating system updates and firmware updates for computers may not be properly downloaded and installed on some computers. This means that the computers and operating systems may be more vulnerable to malware or other security concerns.  ***Plan to Address Risk 1***  Assign experienced IT personnel to properly install any updates to computers in all locations and to take an inventory of the latest versions of operating systems and computers.   * **Risk 2**   Although Employees may be using updated computers and operating systems, employees may access and or download malicious software that could be a security threat to the entire system.  ***Plan to Address Risk 2***  Enforce a clear policy concerning personal use of the company’s computers and install antivirus and antispyware software in all company locations. |
| **For Goal B:2** | **Train the employees in how to use the new UC system.** |
| 1. **Large screens or projectors will be needed for conference rooms for meetings.** | * **Risk 1**   Some employees may miss the training and lack the information they need. Other employees may inform them in a misconstrued way, and thus employees’ actions may cause security concerns.  ***Plan to Address Risk 1***  Meetings will be mandatory and during regular business hours. Employees who miss the training will be required to attend a recording of the training sessions they missed and take a quiz to ensure that they understand the material.   * **Risk 2**   Employees may record the meetings on a cell phone or hidden device and share it with unauthorized personnel.  ***Plan to Address Risk 2***  Give the employees clear instructions that they are not allowed to record the meeting in any format, and nor use cell phones or other devices during the meetings. Have an assistance executive as a standby during the meeting to discreetly monitor employees’ activities during the meetings. |
| 1. **A conferencing application which is capable of recording the meetings and providing live conferencing will be needed.** | * **Risk 1**   The recorded meetings may be accessed or manipulated in some other way by employees, placing the confidentiality and security of the meeting information at risk.  ***Plan to Address Risk 1***  “Provide training to ensure employees understand the legal implications and also understand how to use the technology platform” (Paisner, 2021). Employees need to be given a clear message of the consequences of sharing the company’s confidential information, such as termination and legal charges.   * **Risk 2**   Those employees who missed the meetings will have access to the recorded version of the meeting. These employees may download, or screen-record the meeting, and then share it with unauthorized personnel, placing the company’s information and security at risk.  ***Plan to Address Risk 2***  Make the videos available only on the company’s network and set permissions and levels of access to prevent users from being able to download or record the videos. Also, as mentioned for Risk 1, “Provide training to ensure employees understand the legal implications and also understand how to use the technology platform” (Paisner, 2021). |
| **For Goal B:3** | **Implement and enforce uniform workflow scripts** |
| 1. **New uniform workflow scripts will be created and implemented for all departments in the company that are IT related.** | * **Risk 1**   Some employees may be hesitant to follow the newly implemented workflow scripts because they prefer the old way of doing things. Outdated processes are vulnerable to security breaches.  ***Plan to Address Risk 1***  Employees must be given clear and concise messages that the implementations are mandatory, and that there will be penalties such as termination if the new implementations are not used.   * **Risk 2**   User’s may gain unauthorized access to the management set of tools which created the workflow scripts, and “what these tools allow users to do can affect the integrity of the data and transactions in the system” (Wear, 2021).  ***Plan to Address Risk 2***  The uniform workflow scripts will be closely monitored for any changes that can compromise security (Wear, 2021). |
| 1. **Scripts will need to be automated so that employees could interact and follow them on their devices.** | * **Risk 1**   Changes could be made to source files by unauthorized personnel if the scripts are not secured properly.  ***Plan to Address Risk 1***  “The script deployment record identifies when the script should run as well as the users who can initiate it” (Wear, 2021). Scripts will be secured with user permissions to prevent this risk.   * **Risk 2**   If an unauthorized user found a way to bypass permissions, there may be no way of identifying unauthorized personnel who make changes to the scripts and thus no way of identifying the malicious actions.  ***Plan to Address Risk 2***  “A saved search in NetSuite can be used to view all source files that have been changed, including the date the change was made and the user who made the change” (Wear, 2021). In this way, users’ actions will be monitored and recorded. |
| **For Goal C:1** | **Implement a unified ERP and CRM system** |
| 1. Upgrade any computers which do not have the proper ability to run the modern ERP and CRM software. | * **Risk 1**   Since the solution is cloud-based, employees can access from anywhere in the world and from any device. Unauthorized individuals may gain access to the company’s data.  ***Plan to Address Risk 1***  Employees must be trained on what they can do to keep the company’s information secure. Establish company VPN access through which employees must access data.   * **Risk 2**   Since the solution is cloud-based, employees can access from anywhere in the world and from any device, employees with malicious intents, may gain unauthorized access virtual management tools, which is a security concern.  ***Plan to Address Risk 2***  Carefully assess employees’ situations who may be working remotely. Educate the employees on proper, secure, and legal use of the company’s data. Apply multi-level authentication to employee accounts on all levels. |
| 1. Upgrade the service with internet service providers in all locations, where needed. | * **Risk 1**   Just by nature of being on the internet, the company’s network and thus web security is vulnerable to external security threats. “A report by Risk Based Security found that nearly 85% of penetration attacks on network and IT infrastructure are external” (Atkinson, 2020).  ***Plan to Address Risk 1***  Implement the use of *Zero Trust Security* so that there will be no automatic trust of anything inside or outside the company’s network. This means require validation for everyone and everything that tries to access the network (Atkinson 2020).   * **Risk 2**   Employees are subject to human vulnerability of social engineering fraud such as phishing: for example, through emails which may look legitimate but are phishing scams.  ***Plan to Address Risk 2***  Employees will be educated about how to recognize, report, and avoid malicious software; for example, malicious software that may be in emails or links. |
| **For Goal C:2** | **Train the employees in how to use the new ERP and CRM system** |
| 1. Large screens or projectors will be needed for conference rooms for meetings. | * **Risk 1**   Some employees may miss the training and lack the information they need. Other employees may inform them in a misconstrued way, and thus employees’ actions may cause security concerns.  ***Plan to Address Risk 1***  Schedule mandatory training sessions during regular business hours. Employees who miss the training will be required to study informational PowerPoints to replace the training sessions, which they missed. Plus, they will need to take a quiz to ensure they understand the material.   * **Risk 2**   Employees may record the meetings on a cell phone or hidden device and share it with unauthorized personnel.  ***Plan to Address Risk 2***  Give the employees clear instructions that they are not allowed to record the meeting in any format, and nor use cell phones or other devices during the meetings. Have an assistance executive as a standby during the meeting to discreetly monitor employees’ activities during the meetings. |
| 1. Create supplemental training PowerPoints for employees to learn how to use the new ERP and CRM system. | * **Risk 1**   The training PowerPoints may be accessed or manipulated in some other way by employees, placing the confidentiality and security of the meeting information at risk.  ***Plan to Address Risk 1***  “Provide training to ensure employees understand the legal implications and also understand how to use the technology platform” (Paisner, 2021). Employees need to be given a clear message of the consequences of sharing the company’s confidential information, such as termination and legal charges.   * **Risk 2**   Those employees who missed the meetings will have access to the training PowerPoints. These employees may download the PowerPoints, and then share them with unauthorized personnel, placing the company’s information and security at risk.  ***Plan to Address Risk 2***  Make the PowerPoints available only on the company’s network and set permissions and levels of access to prevent users from being able to download them. |
| 1. Create supplemental interactive training quizzes to track employees’ comprehension of training. | * **Risk 1**   The supplemental interactive training quizzes source files may be accessed or manipulated in some other way by employees, placing the confidentiality and security of the company’s data at risk.  ***Plan to Address Risk 1***  “Provide training to ensure employees understand the legal implications and also understand how to use the technology platform” (Paisner, 2021). Employees need to be given a clear message of the consequences of unlawfully accessing or manipulating the quizzes or sharing the company’s confidential information. For example, consequences would be termination and legal charges.   * **Risk 2**   Those employees who missed the meetings will have access to the supplemental interactive training quizzes. These employees may download the quizzes, and then share them with unauthorized personnel, placing the company’s information and security at risk.  ***Plan to Address Risk 2***  Make the supplemental interactive training quizzes available only on the company’s network and set permissions and levels of access to prevent users from being able to download the quizzes. |
| **For Goal C:3** | **Outsource the company’s software development for professional leased services** |
| 1. Meetings with NetSuite and signing of contracts will be needed. | * **Risk 1**   Meetings may be recorded by attendees and then accessed by unauthorized personnel.  ***Plan to Address Risk 1***  Give the executive employees clear instructions that they are not allowed to record the meeting in any format, nor use cell phones or other devices during the meetings.   * **Risk 2**   Meetings may be subject to eavesdropping devices by a person inside or outside the organization with malicious intentions.  ***Plan to Address Risk 2***  Alert employees of the signs of eavesdropping devices, control physical access by outsiders, inspect any physical items that may have been newly installed (NOAA, 2001). |
| 1. Professional leased software services, in this case, NetSuite’s SaaS services, will be needed to carry out this goal. | * **Risk 1**   Since the company is using leased services, much of company’s cloud security, will be out of the company’s control.  ***Plan to Address Risk 1***  Allow NetSuite to do its part in securing the cloud, according to the contract. NetSuite is known for its high security measures and is trusted by many large corporations who have found success in using its services. “Operations of an organization using NetSuite is protected via 24\*7 monitoring tools, controls and policies, aided by a security team that makes sure that the operational data is always safe” (Inspirria, 2020).   * **Risk 2**   Although NetSuite will share the responsibility for securing the cloud on which company data is stored, the data itself is still subject to security vulnerabilities, from unauthorized access etc.  ***Plan to Address Risk 2***  The data will be protected from security threats by securing access to it. “Determining who can enter data into the cloud, tracking resource modifications to identify abnormal behaviors…adding network analysis…” (McAffee, 2021), are measures that will be taken to protect the company’s data stored in the cloud. |

|  |
| --- |
| **Service & Delivery**  Disparate systems used  Low communication  Company needs more reliable functionality  **Resilience & Security**  Third party rented warehouses make it difficult to scale globally.  Outdated & disparate technologies makes company prone to security vulnerabilities.  **Scalability & Flexibility**  SaaS Services cannot handle growing customer base  Outdated/unsupported technologies are preventing company growth & globalization.  **Interoperability**  Disparate development methodologies & systems cannot communicate properly.  No uniform way of communicating.  **TRANSITION**  Implement NetSuite’s Uniform ERP & CRM  Exchanged software development for professional leased services.  Implement uniform workflow scripts  Implement Comcast’s UC system  Ongoing employee training, continuous improvements & ITIL  **Service & Delivery**  NetSuite’s Unified CRM & ERP System  High communication  Reliable functionality  Continuously Increasing Customer base  **Resilience & Security**  NetSuite’s Unified CRM & ERP System is highly resilient, trusted, and secure.  **Interoperability**  Outsourced professional, leased services are cloud-based and unified.  Unified Technologies  Comcasts Unified Communications System  **Scalability & Flexibility**  NetSuite’s Unified CRM & ERP System is highly scalable and flexible  Latest technologies |

**G. Operational Workflow**

**Resources**

Atkinson, (2020, April 29). *A practical guide to internet vulnerabilities threatening enterprise security.* Retrieved from https://blog.equinix.com/blog/2020/04/29/a-practical-guide-to-internet-vulnerabilities-threatening-enterprise-security/

Inspirria. (2020, January 24). *NetSuite takes security seriously: this is how NetSuite protects your data.* Retrieved from <https://inspirria.com/blog/netsuite-takes-security-seriously-how-netsuite-protects-your-data>

Marvin, R. (2021, January 7). *The do’s and don’ts of securing your voip communications.* Retrieved from https://www.pcmag.com/news/the-dos-and-donts-of-securing-your-voip-communications

*McAfee. (2020). Cloud computing security issues.* Retrieved from https://www.mcafee.com/enterprise/en-us/security-awareness/cloud/security-issues-in-cloud-computing.html

*(NOAA).2001, November 28). Detecting and preventing eavesdropping.* Retrieved from https://www.wrc.noaa.gov/wrso/security\_guide/detect.htm

Nyhuis, M. (2020, October 1). *What is the ITIL framework.* Retrieved from <https://insights.diligent.com/compliance/what-is-the-itil-framework/>

Paisner, B. (2021, September 30). *Risky business: recording board meetings.* Retrieved from <https://www.jdsupra.com/legalnews/risky-business-recording-board-meetings-8151208/>

Wear, Z. (2021). *Improve NetSuite Security.* Retrieved from <https://www.gofastpath.com/blog/tracking-changes-in-scripts-and-workflows-to-improve-netsuite-security>