International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2019): 7.583

IT Infrastructure - Operations, Srategy and Workflow

Anshuman Awasthi

Director –IT Infrastructure Engineering, Restoration Hardware

Abstract: ***IT Operations Management is a perfect mixture of Art, Science, and Technology. A leader needs to be on the lookout for the latest technology, but also he needs to focus on the training of his team members. The technology is changing at a rapid pace and supporting every Business function IT operation needs to adapt automation and be on the path of Continuous Service improvement. A leader needs to run and monitor a process-driven Network Operations Center (NOC) so that his core team can focus on various project initiatives.Let us review an IT Operations template but creating some goals and see some examples on how to achieve them.***

Keywords: IT Operations Strategy, IT Operations Management, IT Operations Template, IT Infrastructure Risk Factors

1. Discussion

This article explains how to create an IT Operations template and process flow for a medium scale Enterprise by creating some futuristic goals.

2. Methods

IT Operational Work Flow as per ITIL,

3. Results/Conclusion

IT Operations Template should be based on the business and strategic goals of an organization. In Order to create an effective IT Operational work flow, we need to understand the existing environment.

3.1 IT Operations Plan Template

In order to create an IT Operations template, let's take an approach of a case study by taking an example of an Organization, which is a software as a service (SaaS) provider which provides HR (Human Resource) application access to it customer, via its web-based applications.Let's say that it is headquartered in San Deigo USA and has over 1600 customers ranging from small to medium -sized businesses.To setup organization strategic goals, it is essential to perform a Business analysis to review the existing environment.

3.2 Current Environment Analysis

Hardware
The organization develops and hosts its applications in four co-locations: San Deigo, California; West Jefferson, Ohio; Singapore, Taiwanand Paris, France; and. Each co-location site is owned by QDS Data Center Services, but organization owns the processing hardware, business software, and the product applications running on them.

SaaS Operation
The organization offers Application Services, professional services at a cost for account configuration and data migration. This is a major revenue stream for the company as most customers utilize some form of the company's App Services for configuration and implementation or reconfiguration. The organization operates anHR application software service with various models as per the customer requirements.

Software
The company's HR application was first developed in 2007 and has been continually enhanced up to the present version. The condition of the application is an issue as the architecture has become monolithic. The organization recognizes that the application needs rebuilding or re-architecture.

The organization writes its own applications software in Java and its communication protocols in Python.The San Deigo is running the enterprise resource planning (ERP), email, and messaging systems.

The Sales and Marketing Departments have taken it upon themselves to select Salesforce (salesforce.com) for sales automation and as a customer resource management (CRM) provider. Both departments have separate instances of Salesforce.com, with a series of custom HTML5 and Force.com applications already written for their instances. At this time, there is no connection between Salesforce.com and the company's business services and ERP system. The ERP system is InTrack, which runs on a server in another office building.

There is also no formal CRM ticketing system in place. Customer service is outsourced to ServiceNow, a cloud-based customer service provider.
As we have understood the existing environment it's time to setup some strategic goals to make the organization ready for possible future expansions, and redefining IT Operations will play a key role.Let's formulate our template based on the below strategic goals.

Strategic Goal I: Update the Technology operational workflow

IT Operations Goals:
1) Setup a 24*7 Network Operation Center (NOC) with monitoring capability in partnership with a service

provider and maintain follow-the-sun working shifts with current staff.
2) Disengage from old network and application monitoring tool and setup Solarwinds as a monitoring tool in the internal Datacenter.
3) Update ServiceNow cloud environment to the latest version and use that as ticketing tool for incident, problem,and change and asset management. Integrate Solarwinds with Servicenow for automatic incident creation. Train NOC and support teams on Servicenow usage.

Strategic Goal II: Improve and upgrade the business system software

IT Operations Goals:
1) Replace the existing Enterprise Resource Program (ERP) with the latest cloud-based ERP application capable of integration with other internal applications like HRM and other CRM applications.Replace existing in-house applications like for product development, accounts receivable, accounts payable, or supply chain with the latest module of ERP platform.
2) Upgrade to the latest version of Salesforce application and integrate with other applications like ERP, to completely automate the existing sales process.Promote usage of this salesforce environment across the organization as a single instance forthe organization's CRM (Customer Resource Management) tool.
3) Migrate existing business communication systems (email, messaging) to Google communication suite that includes Gmail for messaging,Google hangouts for audio and video conferencing along with the chat function.

Strategic Goal 1		
IT Operational Goal	Enhancements needed to support the strategic objective	Planned activities to meet each objective
Goal 1: Setup a 24*7 Network Operation Center (NOC) with monitoring capability in partnership with a service provider.	1) Find out a capable service provider with prior knowledge and experience of running NOC operations for an enterprise. 2) Setup Incident Management and other processes like tickets and shift handover between different shifts and various support teams.	1) Initiate an RFP (Request for proposal) process to get proposals from the different service providers for running NOC Operations. Setup selection criteria for the finalization of a vendor. 2) Once a service provider is shortlisted, finalize an SOW (Statement of Works) listing all the required services along with the targeted SLAs. 3) Work with Internal Support Teams and new service providers to create a project plan for the successful implementation of NOC operations.
Goal 2: Disengage from Old monitoring system and setup Solarwinds as a monitoring tool in internal Datacenter	1) Installation of Solarwinds tool and related modules on a UNIX based server like NPM (Network Performance Monitor) and VMware ESX monitor. 2) Set up a monitoring dashboard and integrate with various communication channels like emails, chat, and pager duty.	1) Work with the selected NOC service provider and internal support teams to develop a transition plan (Project Plan) for the migration of existing support processessetup in the old tool to the new model. 2) Create acomplete server and application inventory with the support of the new service provider and internal support team for proper categorization of incidents as Critical/Medium/High. Setup Alerts in Solarwinds based on the categories.
Goal 3: Update Servicenow cloud environment to the latest version and use that as ticketing tool for Incident,Problem , Change and Asset Management	1)Servicenow software upgrade to the latest version and procure licensing for various modules like Problem, Change, and Asset Management. 2)Promote usage of ServiceNow as a single CRM tool and setup integration with Solarwinds and email system.	1) Take a backup of old incident records from the existing ServiceNow environment. 2) Perform code upgrade to the latest Servicenow code. 3) Add new modules 4) Take a list of the existing CIs (Configuration Item) and work with the internal support team and NOC to create new CIs. 5) Operations Team to work with the ServiceNow development team on integration with Solarwinds.

Strategic Goal 2		
IT Operational Goal	**Enhancements needed to support the strategic objective**	**Planned activities to meet each objective**
Goal 1: Replace the existing Enterprise Resource Program (ERP) with the latest cloud- based ERP application	1)Finalize a new ERP application with capabilities to integrate with various other enterprise applications like sales audit. 2)Integrate various in-house and other cloud-based applications like Salesforce to the new ERP platform	1) Perform research on various ERP solutions and submit an RFP to the shortlisted vendors. 2) Set up selection criteria based on the various features provided by the ERP and organization's expectations from the new solution. 3) Select an ERP solution and work with the professional services to create a project plan for implementation.
Goal 2: Upgrade to the latest version of Salesforce application and integrate with other applications like ERP, to completely	1)Upgrade to the latest version of the Salesforce application. 2) Integrate various modules of Salesforce to other enterprise applications.	1) Take a complete backup of the existing ServiceNow configuration and database. 2) Plan for version upgrade with the professional services. 3) Perform code upgrade and work on integration with various application teams

automate the existing sales process		4) Test integration in the QA environment and plan for changes in the production environment.
Goal 3: Migrate existing business communication systems (email,messaging) to Google communication suite	1) Migrate to a cloud-based communication system Google suite for email, chat,and audio/video conference. 2) Integrate new communication system with other enterprise applications like Salesforce and monitoring tools like Solarwinds	1) Plan for what kind of service model to choose for google suite depending on the number of users, mailbox size, and required services. 2) Take a complete backup of the existing active directory and email database. 3) Create a Project Plan with Professional services for migration. 4) Inform users and provide training on new tools 5) Work with IT operations and application teams on integration with various applications. 6) Decide on the cutover date.

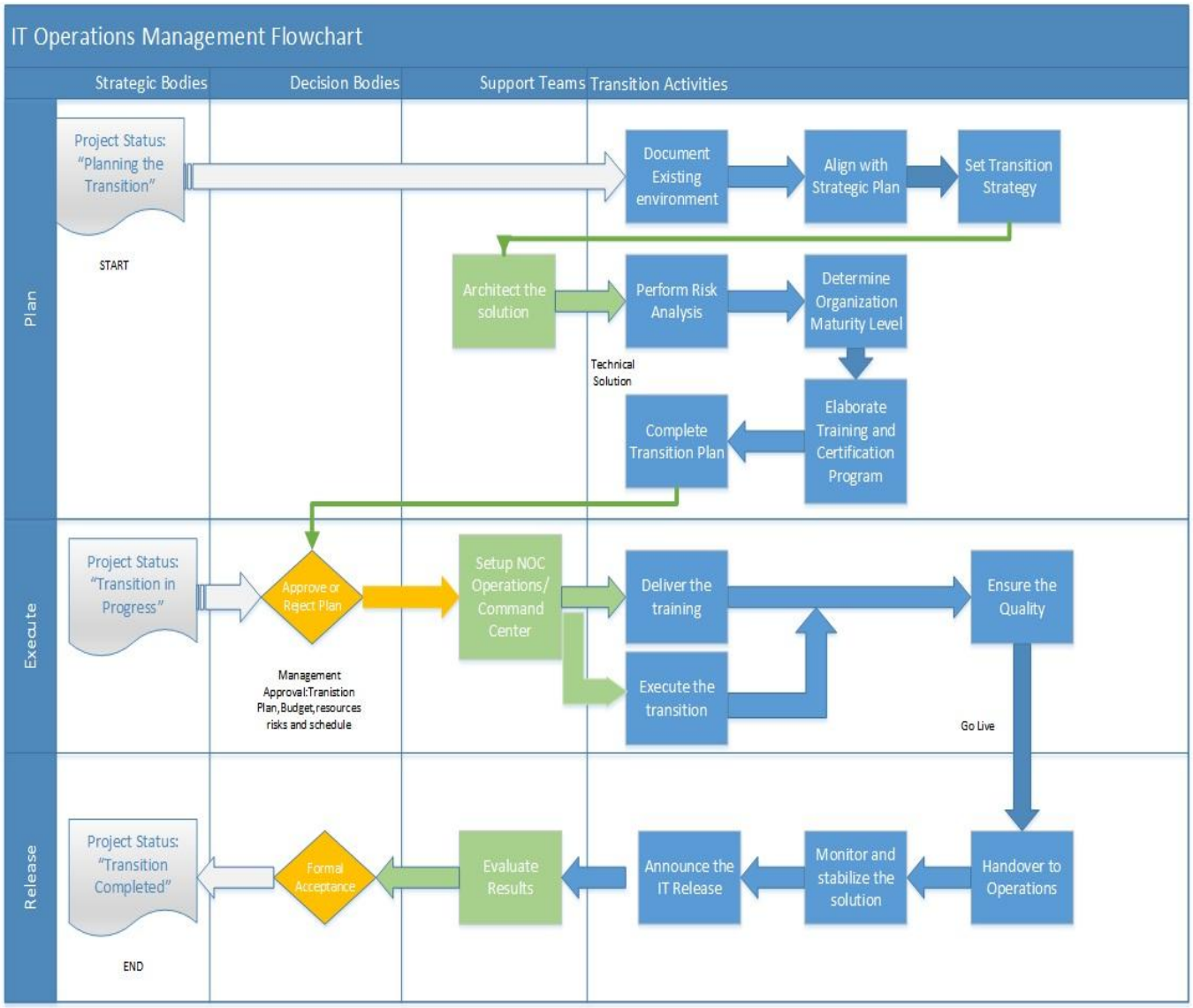
Sustainability Plan	
One Year	Planning & Design Phase followed by Release Phase In this phase, Executives (Directors and VPs) of the organization and various Information Technology team leaders will work along with CIO and Infrastructure Architect to layout the design of the application and underlying infrastructure landscape that is desired to fulfill the Strategic Goals of the company. It is a very critical phase as the cost of making any changes is low as we are still in the design and planning phase.The executive team should meet with businesses to know their expectation for application runtime, desired features, and reliability requirements. In this phase,the IT organization will decideits internal Service Level Agreements (SLAs) for different Configuration Items (CIs) in their service catalog based on the feedback received from the business. In case any services are outsourced or hosted on the cloud organization needs to execute an agreement with the vendor, which should have clear SLAs and associated penalties incase SLAs are not met. Once the organization has worked on the internal application architecture and has finalized the infrastructure requirements, it needs to decide on how one application will talk to the other. Depending on the number of activities involved organization can also start planning on individual release dates or cutover dates to the new environment.
Three Year	ContinuesPlanning followed by Release and ongoing Maintenance Phase In the first year,the enterprise usuallyspends a lot of time in designing and architecting their application and infrastructure landscape which will be followed by the release of the individual products (cutover to new services) or release of the newly made integration among two or more services and eventually enhancements to the existing services or integrations.This comes under the ongoing Maintenance Phase, which is needed to keep the application or the infrastructure up to date. Ongoing maintenance can be categorized into five types of major activities. Enhancements: When the organization decides to add more features to the existing release of the product, this request most of the time comes from the business and is mainly required to further optimize the process or reduce the steps in an existing workflow. Code Upgrade:When the applicate suite or a module inside the application suite needs to be upgraded to the latest code due to old module going out of support, or there is a need in the organization to utilize the new features available in the latest code. Security Patching:This is mainly required to keep the application and infrastructure up to date from a security perspective.The organization should install a vulnerability scanning tool like Tenable and generate reports on applicable vulnerabilities in their environment. This is essential to keep the application and infrastructure environment secure. Bug Fixes: We can spend a lot of time testing the new application or code in the QA environment, but the real test happens when it is released for the actual users. The more amount of users use the application, they will identify more bugs, and that needs to be rectified in the code or application to ensure smooth operations. Infrastructure Upgrade: In order for the application to run smoothly, it needs a supporting infrastructure that consists of the server,database, operating system, hardware, and network components. The organization will be installing Solarwinds as an infrastructure and application attribute monitoring tool which can help the team in finding out the bottlenecks and recommend for necessary upgrade or modifications. The generated alerts should be used to perform Capacity Planning.

Five Year	Maintenance Phase and the start of application/infrastructure Retirement phase One of the most important best practices recommended by the ITIL is CSI (Continuous Service Improvement), which consists of all the maintenance activities listed in the earlier section but governed by a dedicated person in the leadership team to ensure continuous progress and tracking. No matter how good a tool or an application is, the reality is, it comes with an expiration date. In the real world, demands are always changing, and to stay in the market; the enterprise needs to have an Agile application environment that is continuously evolving. When an organization decides on its strategic goals, especially for IT, they usually plan for three to five years. The company leaders should plan for application/infrastructure retirement to fulfill any changes in the organization's strategy due to customer demands. Anorganization should start planning for application retirement if they think that it is not creating any new values in the coming time, or the old suite cannot take any new enhancements. While the leaders are planning for application retirement, it is essential to keep the existing environment up to date to ensure it is working as expected, and the team is still meeting all agreed SLAs.As per the listed operational goals,the organization should move it's few critical applications like ERP and business communication systems to cloud-based, during this phase organization leaders will review whether they should continue to use the existing applications (Cloud providers are usually good in keeping their application suite up to date) or they can also choose to go to a new provider if it is providing any new features which are missing on the existing application landscape. Usually, migration from one cloud provider to another is less complicated as compared to the in-house hosted infrastructure,a lot of tools are available for data migration, and there is no lift and shift is involved.

Enhancement	**Security Risk and Plan to Address Risk**
Find out a capable service provider with prior knowledge and experience of running NOC operations.	Security Risk:The identified/Shortlisted partner is not following all the necessary security norms, and its network devices are vulnerable to attacks like phishing. Plan to Address Risk: When an organization is in the process of selecting a partner,we can ask the vendor to present the current vulnerability report and what process they have in place to address any security threats to their environment. We can also include a clause in the agreement to ensure the vendor is keeping their infrastructure/application landscape up to date on the security patches.
Setup Incident Management and other processes like tickets and shift handover between different shifts and various support teams.	Security Risk:Identified vendor may not have adequate staff/expertise to handle security incidents or may miss acting on incidents as expected due to process gaps. Plan to Address Risk: During the vendor selection process,the organization's leadership team should ask for the past experience vendor has in handling security incidents, what is the level of experience their staff has and what certifications they have. Once a vendor is selected, we can ask for the best practices they follow to ensure there are no gaps in transition and even do a mock drill to identify any process gaps.
Installation of Solarwinds tool and related modules on a UNIX based server like NPM set up monitoring dashboard and integrate with various communication channels	Security Risk: Whenever we install a monitoring tool, there can be a security risk as some unauthorized devices can use the same communication protocols to gain access to the network. Also, if a network breach happens and an attacker can get access to the monitoring tool server, he can transfer malicious files to the whole network as the server is allowed access to other devices for monitoring purposes. Plan to Address Risk: We can mitigate this security risk by installing the monitoring tool environment behind a network firewall and only allowing access to the authorized devices and that too on selected network ports. It is also essential to keep the underlying infrastructure and operating system up to date on the security patches.
Set up a monitoring dashboard and integrate with various communication channels	Security Risk: In the process of integrating Solarwinds monitoring tool with other application there is a security risk of network breach through other applications Plan to Address Risk: Only authorized applications should be allowed to talk to Solarwinds and only on secured protocols like https.Unsecured communication should not be allowed. It is also essential to keep the underlying infrastructure and operating system up to date on the security patches. Application access and traffic should be monitored on a regular basis.
ServiceNow software upgrade to the latest version and procure licensing for various modules like Problem, Change, and Asset Management.	Security Risk: When an organization decides to use any services on the cloud, like for example, ServiceNow there area lot of risks as to access the services you need to transfer the data on WAN (Wide Area Network) or using the internet which is considered insecure as compared to LAN (Local Area Network). Plan to Address Risk:To mitigate this security risk, it is essential to secure the organization's LAN by installing network firewalls and using these devices as gateways and monitor any traffic coming in and going out of the network. The organizaion's IT team can also install an IDS/IPS device (Intrusion Detection/Protection).
Finalize a new ERP application with capabilities to	Security Risk: When an organization decides to use any services on the cloud like for example ERP services hosted on the cloud there is a lot of risks as to access the services you need to transfer the data on WAN (Wide Area Network) or using the internet which is considered insecure as compared to LAN (Local Area Network).In

integrate with various other enterprise applications like sales audit.	addition to the risk to the company's data, a lot of times, ERP database has customer records which increase the organization's liability. Plan to Address Risk: To mitigate this security risk, it is essential to secure the organization's LAN by installing network firewalls and using these devices as gateways and monitor any traffic coming in and going out of the network. The organization's IT team can also install an IDS/IPS device (Intrusion Detection/Protection).Only authorized systems should be allowed to access ERP application on the selected protocols.
Upgrade to the latest version of Salesforce application and integrate with other enterprise applications	Security Risk:The biggest security risk for CRM application is how to ensure data security as most of the time it contains confidential customer records. When we are planning to upgrade salesforce to a newer version we need to ensure we are not making any compromises on data security. Plan to Address Risk: We can mitigate this risk by following below practices in the Salesforce environment Phishing and Malware Salesforce displays real-time information on system performance and security on the trusted site at http://trust.salesforce.com. This site provides live data on system performance, alerts for current and recent phishing and malware attempts, and tips on best security practices for your organization. Security Health Check IT admin can use Health Check to identify and fix potential vulnerabilities in your security settings, all from a single page. A summary score shows how an organization can measure against a security baseline, like the Salesforce Baseline Standard. Organization's Salesforce admin can upload up to five custom baselines to use instead of the Salesforce Baseline Standard. Auditing Auditing provides information about the use of the system, which can be critical in diagnosing potential or real security issues.IT admin should do regular audits to detect potential abuse. Salesforce Shield Salesforce Shield is a trio of security tools that organization's admins and developers can use to build a new level of trust, transparency, compliance, and governance right into business-critical apps. It includes Platform Encryption, Event Monitoring, and Field Audit Trail. Transaction Security Policies Policies evaluate activity using events that you specify. For each policy, the organization's salesforce admin can define real-time actions, such as notify, block, force two-factor authentication, freeze user, or end a session.
Migrate to cloud-based communication system Google suite for email, chat and audio/video conference. Integrate various applications /monitor tools with new communication systems	Security Risk:There are quite a few security risks that organization should consider before moving to a cloud-based communication suite like Google, unauthorized access control, chances of the data breach, and data loss. Once an unauthorized person gains access to files in G Suite they could potentially cause all manner of damage by editing or deleting files and gaining access to sensitive information. Plan to Address Risk:The best way to protect G Suite from unauthorized access is to practice good password security and other general online security awareness, such as knowing how to recognize a phishing attempt. Organizations should ensure their staff isthoroughly trained in these security essentials. The only way to ensure your data is truly safe in G Suite is to use Spin backup cloud-to-cloud backup. This way a backup of your files will remain, even if they are permanently deleted from G Suite, and your data can be recovered to an earlier point in history, before the data loss occurred, and deploy the cutting-edge data loss prevention solutions.

Operational Workflow



References

[1] The Definitive Handbook of Business Continuity Management
[2] Corporate Risk Management-By Tony Merna
[3] https://strategiccfo.com/
[4] https://www.fosterfuelsmissioncritical.com
[5] https://www.tandfonline.com/doi/pdf/10.1080/21693277.2014.882804
[6] https://www.ijsr.net/archive/v9i3/SR20321012229.pdf (DOI: 10.21275/SR20321012229)
[7] https://disastersafety.org
[8] https://www.ijsr.net/archive/v9i1/ART20204296.pdf (DOI: 10.21275/ART20204296)
[9] https://www.business.qld.gov.au
[10] https://www.aferm.org/erm_feed/the-business-impact-of-trump-tariffs/
[11] https://www.ijsr.net/archive/v9i3/SR20312083156.pdf (10.21275/SR20312083156)
[12] https://www.nyu.edu
[13] http://recentscientific.com/sites/default/files/15397-A-2019.pdf(DOI: http://dx.doi.org/10.24327/ijrsr.2019.1012.4930
[14] http://www.emergency-response-planning.com
[15] https://searchdisasterrecovery.techtarget.com
[16] https://propelplm.zendesk.com/hc/en-us/article_attachments/205786177/salesforce_security_impl_guide.pdf https://propelplm.zendesk.com/hc/en-us/article_attachments/205786177/salesforce_security_impl_guide.pdf

Author Profile

Anshuman Awasthi, Director, Infrastructure Engineering at Restoration Hardware, responsible for IT infrastructure management and new implementations. Member of Forbes Technology Council.