

Assignment

Yichen Huang(2200440)

December 20, 2022

1 Introduction

CoffeeBlend is a company that sells Jamaica coffee and has an extensive global presence. The company uses cloud services to deliver IT services to its staff and clients, and has a large wireless network. Due to the company's large staff and international customer base, it has come under pressure to allow both its staff and customers to use their personal devices to access the company's network and resources. The company is concerned about the security of personal staff and customer data, as well as protecting its intellectual properties. It does not have an established policy covering these security needs.

Information Technology Infrastructure Library (ITIL) is a framework that provides best practices for managing and organizing IT services. It can be used to address the concerns raised in the scenario by establishing a set of policies and procedures for securely allowing the use of personal devices on the company's network. ITIL can help the company ensure that its staff and customers' data is protected, and that its intellectual properties are safeguarded. ITIL can also help the company organize and manage its IT services in a more efficient and effective manner.

There are several reasons why ITIL can be used to address the concerns raised in the scenario: Min (2012)

- ITIL provides a comprehensive set of best practices for managing and organizing IT services, including policies and procedures for securely allowing the use of personal devices on the company's network. This can help the company ensure that its staff and customers' data is protected, and that its intellectual properties are safeguarded.
- ITIL has a proven track record of success in helping organizations manage their IT services in a more efficient and effective manner. By implementing the framework, the company can improve its IT operations and ensure that its services are delivered in a consistent and reliable manner.
- ITIL can help the company improve its communication and collaboration among its staff and customers, enabling them to work together more effectively and efficiently. This can help the company better serve its customers and maintain its competitive edge in the market.
- By implementing ITIL, the company can also reduce its IT costs and improve its return on investment. The framework provides a structured approach for managing and organizing IT services, which can help the company optimize its use of resources and minimize unnecessary expenses.

Overall, ITIL can help the company address its security concerns and improve its IT operations, enabling it to better serve its staff and customers and protect its intellectual properties. The remainder of the article I will introduce the methodology I designed, and analyze why it is good practice to constantly have new or updated regulations and standards.

2 Event Management

Event management aims to reduce the impact of events by effectively identifying, reporting, analyzing, and resolving issues. One way to use ITIL to design a method for event management at CoffeeBlend would be to follow the five-step process outlined in the ITIL framework: Gunawan (2019)

2.1 Identify the event

The first step in using ITIL to design a method for event management at CoffeeBlend would be to identify the event. This involves defining the event, including its scope and objectives, and determining the impact it may have on the company and its customers.

For example, if the event is a network outage, the first step would be to define the scope of the outage, such as which systems or locations are affected. The objective of this step would be to understand the full extent of the event and its potential impact on the company's operations and customers.

To identify the event, CoffeeBlend could use tools and processes such as incident reporting and monitoring, as well as input from staff and customers, to gather information about the event and its potential impact. This information would then be used to define the scope and objectives of the event and determine the appropriate response.

2.2 Classify the event

The second step in using ITIL to design a method for event management at CoffeeBlend would be to classify the event. This involves categorizing the event according to its type, severity, and priority, as well as identifying any potential risks or impacts associated with it.

For example, if the event is a network outage, the second step would be to classify the event according to its type (e.g. network, hardware, software), severity (e.g. low, medium, high), and priority (e.g. urgent, important, routine). This information would help CoffeeBlend determine the appropriate response to the event and prioritize its efforts to resolve the issue.

Classifying the event would also involve identifying any potential risks or impacts associated with it. For example, a network outage could affect the company's ability to process orders or communicate with customers, which could have a negative impact on the company's operations and reputation. By identifying these potential risks and impacts, CoffeeBlend can take appropriate measures to mitigate them and ensure the smooth operation of its IT services.

2.3 Investigate the event

The third step in using ITIL to design a method for event management at CoffeeBlend would be to investigate the event. This involves collecting and analyzing data to understand the root cause of the event and determine the appropriate course of action.

For example, if the event is a network outage, the third step would be to collect data from various sources, such as network logs, performance metrics, and user reports, to identify the root cause of the outage. This could involve using tools and processes such as root cause analysis and problem management to diagnose the issue and identify potential solutions.

Once the root cause of the event has been identified, CoffeeBlend can determine the appropriate course of action to resolve the issue and restore the affected systems or services. This could involve deploying a patch or workaround, or implementing a longer-term solution to prevent similar issues from occurring in the future. The goal of this step is to ensure that the event is properly resolved and the quality of the company's IT services is maintained.

2.4 Respond to the event

The fourth step in using ITIL to design a method for event management at CoffeeBlend would be to respond to the event. This involves implementing the appropriate response to the event, such as deploying a patch or workaround, and ensuring that the event is properly resolved.

For example, if the event is a network outage, the fourth step would be to implement the appropriate response to resolve the issue and restore the affected systems or services. This could involve deploying a patch or workaround to address the root cause of the outage, or implementing a longer-term solution to prevent similar issues from occurring in the future.

To ensure that the event is properly resolved, CoffeeBlend would need to monitor the affected systems or services and conduct testing to confirm that the issue has been resolved and the quality of the company's IT services is restored. This could involve using tools and processes such as incident tracking and service level management to monitor the event and ensure that the appropriate response is being implemented. Overall, the goal of this step is to ensure that the event is properly resolved and the quality of the company's IT services is maintained.

2.5 Review the event

The fifth step in using ITIL to design a method for event management at CoffeeBlend would be to review the event. This involves conducting a post-event review to evaluate the effectiveness of the response and identify any areas

for improvement.

For example, if the event is a network outage, the fifth step would be to conduct a post-event review to evaluate the effectiveness of the response and identify any areas for improvement. This could involve conducting a root cause analysis to determine why the outage occurred and identify any potential vulnerabilities or weaknesses in the company's IT infrastructure.

Based on the findings of the review, CoffeeBlend can implement changes or improvements to its IT systems and processes to prevent similar events from occurring in the future. This could involve updating or upgrading hardware or software, implementing new policies or procedures, or providing additional training or support to staff. Overall, the goal of this step is to ensure that the company's IT services are resilient and can effectively handle any future events or challenges that may arise.

3 Service Catalog

In my approach to meet the need of the company information system security, I think the Service Catalog is also necessary. The Service Catalog is the repository of all IT services provided to users, from simple keyboard requests to complex new server upgrades; it provides complete visibility into the various services each user receives. An efficient service catalog helps service desk technicians simplify the service request management process, enabling users to access services quickly and easily, and to deliver requested services in a timely manner. Ilieva and Nikolov (2020)

3.1 Identify stakeholders

A fundamental step in implementing a service catalog is understanding the goals of the business and the expectations of end users. Start by answering the following questions:

- What is your company's goal?
- Who are the stakeholders (end users, IT technicians, and management) and what are their service needs?
- Let's try to answer the above questions in the context of new employee onboarding.
- What are the goals of the business?
- How to provide effective service to new employees.

This requires a comprehensive review of existing legacy service delivery solutions and a stakeholder survey. In a large enterprise like CoffeeBlend, employees are entitled to different IT services based on their designation, department, location, and other criteria. End users should be able to view and request only those services for which they are eligible. Does it? It is important to determine such boundaries before implementing a service catalog.

3.2 Define and classify service offerings

Next, the services need to be defined and categorized. Assess all the services provided by the IT department, the underlying workflows that support those services, and the turnaround time associated with each service. Proper categorization makes it easier for end users to find and request the services they need. Here's an example:¹

3.3 Create service-specific workflows

Once IT has defined and cataloged the list of service offerings, it's time to create service-specific SLAs and define fulfillment workflows. Setting realistic tasks is key to ensuring smooth service delivery. For example, a workflow that provides employee onboarding services:²

3.4 Design and release

The resulting directory form should be easy for end users to navigate and use to request services. To this end, service offerings should be categorized according to industry best practices and end-user expectations. Create a service catalog that is visually appealing to end users. All attributes offered by the service, such as cost, availability, and expected fulfillment date, should be displayed upfront. Avoid lengthy forms when collecting data from end

Service Categories

Application Login

Services related to application login like creating CRM account, SAP account, MSSQL account, Active

Communication

Services related with communication like requesting for a telephone or DID extension, a mobile phone for on-call

Data Management

Services related to data management like performing backups, restore and clean up data are placed in this

Email

Services related to email like creating an email account, email client installation, password reset for email

Hardware

Services related to hardware purchase, upgrading RAM, requesting a laptop or a desktop, etc., are placed

Internet

Services related to internet access, WiFi access, creating a VPN account, booking a domain, proxy

Software

Services related to software installation/un-installation, software purchase, license purchase, software

User Management

Services related to hiring a new employee, requesting a department/place change, etc., are

Figure 1: An example of service-categories.

SLA details

SLA Name

Onboarding SLA

Description

SLA for onboarding permanent employees

SLA Rules

When a new Service Request arrives :

Service Requests should be responded within

: 3 Days 0 Hours 0 Minutes

Service Requests should be fulfilled within

: 15 Days 0 Hours 0 Minutes

☒ Should be fulfilled/responded irrespective of operational hours.
☒ Should be fulfilled/responded irrespective of Holidays.
☒ Should be fulfilled/responded irrespective of Weekends.

If the response time is about to be elapsed/elapsed then escalate:

☒ Enable Level 1 Escalation

Escalate to

\$Ticket Owner

Choose

☒ Escalate Before ☐ Escalate After 1 Days 6 Hours 0 Minutes

[Actions](#)

If the fulfillment time is about to be elapsed/elapsed then escalate:

☒ Enable Level 1 Escalation

Escalate to

Heather Graham

Choose

☐ Escalate Before ☒ Escalate After 2 Days 0 Hours 0 Minutes

[Actions](#)

☐ Enable Level 2 Escalation
☐ Enable Level 3 Escalation
☐ Enable Level 4 Escalation

Figure 2: An example of onboarding-service-level-agreement.

users. Instead, dynamic forms driven by condition-based actions should be implemented to provide a user-friendly interface. Once end users make a service request, they should be provided with the ability to track the status of the request to ensure transparency of the progress made by the service implementation team. Implement such a mechanism in your service catalog and test it as a closed beta.

After extensive testing of the service catalog and its workflows, you need to integrate it with the self-service portal. This portal provides end users with a single gateway for ticketing incidents, service requests and information requests. Keywords should be applied and the most popular services listed at the top to minimize the time spent

4

Services

 Web Development and Hosting includes Stanford Web Services, WWW hosting, content management systems, survey and form tools, and more.	 Support and Training includes ServiceNow online help system, Knowledge Management, Technology Training programs, and more.	A to Z - Account and Access Services - Accounts and Passwords - Active Directory - AFS (Andrew File System) - Anti-Malware for Mac - Anti-Malware for Windows - Apple Developer Connection (ADC) - Application Whitelisting (Carbon Black Protection, formerly Bit9) - Authentication, Kerberos - Authentication, Shibboleth - Authority Manager - Automated Call Distribution (eACD) - Backup (Code42 CrashPlan) - Backup and Recovery Services - Backup, Cloud Storage - Backup, Disk-Based Replication - Backup, Server (BaRS) - BaRS (Backup and Recovery Service) - Bible Sheets (CNSCAD) - Blogs (WordPress) - Box - Build a Meeting Room - Cable TV (Cardinal Cable) - Calendar - Call Recording - Callback Assist - Cardinal Fax - Cardinal Key - Cardinal Print
 Software and Business Applications includes software distribution and licensing, service ordering, and application implementation and/or hosting.	 Servers and Data includes centralized server hosting, system administration, virtual servers, and databases.	
 Security includes desktop and mobile device management, antivirus, disk encryption, and more.	 Consulting and Development includes Business Solutions Consulting and Development, CRC, BigFix, Apple, Dell, and Lenovo bundles, and more.	
 Communications includes Telephones, Cell Phones, Cable TV, and more.	 Business Intelligence and Reporting includes Oracle Business Intelligence - Enterprise Edition (OBIEE).	
 Backup and Storage includes Encryption, Data Storage, and Backup services.	 Document and Digital Asset Management includes G Suite at Stanford, Box, OpenText, and SALLIE.	
 Email and Calendar includes Stanford Email & Calendar, Mailing	 Research Computing includes consulting, server hosting and	

Figure 3: Stanford University service catalog.

by end users searching for services. Ease of access to the catalog is paramount. Your service catalog should be accessible from different platforms and channels, such as mobile apps, emails, and web forms. Implement the catalog first for one department or category of service, then expand it to other departments based on stakeholder feedback.

4 Change management

It is important for CoffeeBlend to implement an effective change management process using the ITIL change management in order to ensure the security of its IT systems and protect its online presence. The ITIL change management process helps to ensure that any changes made to the company's IT systems are properly planned, tested, and implemented in a controlled and coordinated manner. This can help to minimize the risk of disruptions or outages caused by unplanned or poorly managed changes, and help the company to maintain the availability and integrity of its IT services. By following the ITIL change management process, CoffeeBlend can also ensure that its IT systems are compliant with relevant industry standards and regulations, and that they meet the needs of the company and its customers. here are the steps involved in the ITIL change management process: Berger et al. (2020)

- 1 **Change request:** A change request is a request for a change to be made to the IT systems, typically initiated by a business user or IT staff member. This could be a request to add a new feature or service, modify an existing system, or fix a problem. The change request should include detailed information about the proposed change, including its purpose, scope, and impact.
- 2 **Assessment and classification:** Once a change request has been received, it is assessed to determine its impact, risk, and priority. This helps to ensure that the change is properly managed and that resources are allocated appropriately. The change may be classified as high, medium, or low impact or risk, depending on

the potential consequences of the change and the likelihood of those consequences occurring. The change may also be assigned a priority level based on its impact on business operations and the urgency of the change.

- 3 **Change evaluation:** The change is then evaluated to determine whether it can be implemented safely and effectively. This may involve reviewing the change request and any supporting documentation, consulting with relevant stakeholders, and conducting a risk assessment. The change evaluation should identify any potential issues or risks that may need to be addressed in order to ensure the success of the change.
- 4 **Planning:** Once the change has been evaluated and approved, a plan is developed to outline the steps that will be taken to implement it. This may include testing, training, communication, and other activities necessary to ensure the change is successful. The plan should also include contingency measures in case something goes wrong, and should be reviewed and approved by relevant stakeholders before implementation begins.
- 5 **Implementation:** The change is then implemented according to the plan, with appropriate testing and monitoring in place to ensure its success. This may involve coordinating with different teams or departments, or working with external vendors or partners.
- 6 **Review:** After the change has been implemented, it is reviewed to determine whether it was successful, and to identify any lessons learned that can be applied to future changes. The review should consider the effectiveness of the change, any issues or challenges encountered during implementation, and the overall impact on the business.

By following this process, CoffeeBlend can ensure that its IT systems are updated and improved in a controlled and coordinated manner, while minimizing the risk of disruptions or outages.

5 Service Asset and Configuration Management

One way that ITIL could be used to provide a solution for information security for CoffeeBlend would be to follow the process outlined in the ITIL Service Asset and Configuration Management (SACM) stage. This stage focuses on the identification, control, and maintenance of IT assets, including hardware, software, and documentation. Some specific steps that could be taken to address information security using ITIL within the SACM stage include:

- 1 **Identifying and cataloging the company's IT assets:** This step involves creating an inventory of all the hardware, software, and documentation that the company uses in its IT operations. This could include physical assets like servers, laptops, and networking equipment, as well as software licenses, user manuals, and technical documentation. By creating an inventory of its IT assets, the company can have a clear understanding of what it has and where it is located, which is important for managing and protecting those assets. It may be helpful to use a tool or database to track and manage the inventory, such as an asset management system or a configuration management database (CMDB).
- 2 **Establishing policies and procedures for managing IT assets:** The company should develop policies and procedures for managing its IT assets, including guidelines for their use, maintenance, and disposal. These policies and procedures should be documented and communicated to all relevant personnel. They should outline the roles and responsibilities of different staff members in relation to the IT assets, as well as the procedures for requesting and obtaining access to those assets. For example, the policies and procedures might specify who is responsible for installing and configuring new hardware or software, or for decommissioning or disposing of old assets.
- 3 **Implementing controls to ensure the security of IT assets:** To ensure the security of its IT assets, the company should implement controls such as access controls and authentication measures. Access controls can include things like user accounts and permissions, which can be used to grant or restrict access to specific IT assets. For example, an employee might have permission to access a certain server or database, but not to other systems. Authentication measures, such as passwords or biometric authentication, can be used to verify the identity of individuals attempting to access the assets. These measures can help prevent unauthorized access to sensitive information or systems.

- 4 **Monitoring and reviewing the security of IT assets:** The company should establish processes for regularly reviewing and monitoring the security of its IT assets to ensure that they remain protected. This could involve conducting security audits, penetration testing, and other testing methods to identify potential vulnerabilities. The results of these reviews should be used to identify any necessary security improvements and to update the company's policies and procedures as needed. For example, if a security audit reveals a weakness in the company's access controls, the company might need to update its policies to address the issue or implement additional security measures. Regular monitoring and review can help ensure that the company's IT assets are secure and compliant with relevant regulations and standards.

6 Managing and Protecting Sensitive Information

In addition to the ITIL framework, the company could also consider using the International Organization for Standardization (ISO) 27000 series of standards, which provide a framework for managing and protecting sensitive information. The ISO 27000 series of standards provides a framework for managing and protecting sensitive information, including personal and confidential data. To use these standards to protect the privacy of sensitive information within the company, the following steps can be taken: Monica et al. (2020)

- 1 **Establish an information security management system (ISMS):** The ISO 27001 standard outlines the requirements for establishing an ISMS, which is a framework for managing and protecting sensitive information. The company can use this standard to establish policies, procedures, and controls for managing its information security, including the protection of sensitive and personal data.
- 2 **Conduct a risk assessment:** The ISO 27005 standard provides guidance on how to conduct a risk assessment to identify and evaluate the potential risks to the company's assets, including the risk of unauthorized access to or disclosure of sensitive information. This will involve identifying the company's key assets, evaluating the likelihood and impact of potential threats, and implementing controls to mitigate those risks.
- 3 **Implement controls:** The ISO 27002 standard provides a list of general controls that can be used to protect against a range of information security threats. These controls can be customized to meet the specific needs of the company and can include things like access controls, encryption, and incident response plans.
- 4 **Establish a data protection policy:** The company should establish a clear policy outlining how it handles personal and sensitive data, including what data is collected, how it is used, and how it is protected. This policy should be communicated to all employees and should be consistently enforced.
- 5 **Ensure compliance with relevant regulations:** The company should ensure that it is compliant with any relevant privacy regulations, such as the General Data Protection Regulation (GDPR) in the European Union. This will involve implementing appropriate controls and procedures to ensure that the company is meeting these requirements.

By following these guidelines and implementing appropriate controls and procedures, the company can effectively protect the privacy of sensitive information and meet its compliance obligations. It will be important to regularly review and monitor the effectiveness of these measures to ensure that they are adequate and up to date.

7 why it is good practice to constantly have new or updated regulations and standards

It is good practice to constantly have new or updated regulations and standards for a number of reasons:

- 1 **Technology and threats evolve:** As technology and the threats faced by organizations evolve, it is important to have regulations and standards that reflect these changes. For example, as cyber threats become more sophisticated, new regulations and standards may be developed to help organizations protect against these threats. Similarly, as new technologies emerge, such as cloud computing or the Internet of Things, new regulations and standards may be developed to ensure that these technologies are used in a secure and responsible way.

- 2 **Improved security and compliance:** By regularly updating regulations and standards, organizations can ensure that they are following best practices for information security and compliance. For example, if a new data protection regulation is introduced, an organization that updates its policies and procedures to meet the requirements of the new regulation will be better protected against data breaches and more compliant with the law. Similarly, if a new standard for secure coding is introduced, an organization that updates its development processes to follow the standard will be better protected against security vulnerabilities in its software.
- 3 **Increased confidence and trust:** By demonstrating a commitment to security and compliance, organizations can build trust with customers, employees, and other stakeholders. For example, if a company updates its privacy policy to meet the requirements of a new data protection regulation, customers may be more confident in the company's commitment to protecting their personal information and more likely to do business with the company. Similarly, if a company updates its security policies and procedures in response to a new standard, employees may be more confident in the company's commitment to protecting their personal data and more likely to trust the company with sensitive information.
- 4 **Improved efficiency and effectiveness:** Regularly updating regulations and standards can help organizations streamline their processes and systems, resulting in improved efficiency and effectiveness. For example, if a company updates its security policies and procedures to follow a new standard, it may be able to eliminate unnecessary controls and streamline its processes, resulting in cost savings and improved efficiency. Similarly, if a company updates its policies and procedures to meet the requirements of a new data protection regulation, it may be able to simplify its data management processes, resulting in improved effectiveness and quality.

Overall, constantly having new or updated regulations and standards is good practice because it helps organizations stay current with the latest developments in technology and threats, improve their security and compliance posture, build trust with stakeholders, and become more efficient and effective.

References

- Berger, D., Shashidhar, N., and Varol, C. (2020). Using itil 4 in security management. In *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*.
- Gunawan, H. (2019). Strategic management for it services using the information technology infrastructure library (itil) framework. In *2019 International Conference on Information Management and Technology (ICIMTech)*.
- Ilieva, R. Y. and Nikolov, Y. P. (2020). It service management framework to improve business information structures. In *2020 XI National Conference with International Participation (ELECTRONICA)*.
- Min, Z. (2012). Research and design of an itil based it service management framework. *Information Security and Technology*.
- Monica, R., Henry, Q., Estela, M., and Washington, F. (2020). Why implement continuity plans in organizations? approach of a prospective study based on itil. In *2020 International Conference on Intelligent Systems and Computer Vision (ISCV)*.