Research Article: Citation date: 2021/10/08

Establishing Efficient IT Operations Management through Efficient Monitoring, Process Optimization, and Effective IT Policies

2021

Ali T. Atieh

EGM- IT Infrastructure Operation,
Etihad Etisalat – MOBILY

ORCID

How to cite:

Atieh, Ali T. 2021. "Establishing Efficient IT Operations Management through Efficient Monitoring, Process Optimization, and Effective IT Policies." Empirical Quests for Management Essences 1 (1): 1–12.

Received: 2021/08/08
Available online: ***2021/10/08***

Abstract

Every organization is becoming increasingly reliant on IT that is available, dependable, secure, and high-performing. The ability of an IT team to run its operations efficiently is directly and completely contingent on its ability to deliver resilient IT. The IT team must be able to identify, prioritize, execute, and manage the processes that drive operational tasks and activities in particular. IT teams may reach such goals more efficiently and consistently with the help of effective IT Operation Management processes and solutions. This research attempts explore how efficiency can be attained. More specifically, we focus on three broad components of efficient IT Operation management: 1) efficient monitoring 2) process optimization 3) and effective IT policies. IT infrastructure monitoring enables the detection of security threats and the resolution of operational issues before they cause harm to clients. We find that there are three significant practices to achieve efficient monitoring. They are: Organizing and Prioritizing Alerts, Providing Processed Data in a Dashboard, and Selecting a Trustworthy Vendor Partner. We also find that there are four challenges in IT infrastructure monitoring: It is sometimes necessary to take a proactive approach; after all, that's what monitoring is all about. Here are some of the most typical monitoring difficulties that businesses, in general, and IT departments, in particular, face: Being beyond monitoring capacity, the ineffectiveness of outdated monitoring applications, increasing prices, and data capacity. IT process optimization technique identifies the most appropriate ways of satisfying an organization's technological and informational needs on a proactive (and non-responsive) basis, with the main goal of supporting it in the long-term development of value. This research also explains discusses forming efficient IT policies such as policies for IT emergency

intervention and disaster recovery, Security policies for IT infrastructure. Efficient IT policies provide information technology transparency for individuals in a business. IT policies assist to counter risks and manage risk while assuring that operations are efficient, effective, and consistent.

Keywords: *IT infrastructure, IT Monitoring, IT Operations Management, IT Policies, Process Optimization*

1. Introduction

As IT infrastructures become more complicated in today's world, so does a company's capacity to sustain service levels. IT Operations Management is the IT department in charge of efficiently planning, organizing, coordinating, and controlling IT resources. It must, in other words, successfully handle many aspects of the operation, such as people, equipment, information, applications, connection, technology, and so on.

IT operations management is an important part of every company's operations. That's why it's critical to have a solid operational management procedure in place in IT. After all, good operational management provides a far wider picture of how services are consumed by other parts of the firm, as well as how resources are scaled and how they contribute to the company's success. More importantly, it is critical in identifying areas for improvement and supporting a continual and healthy process inside the organization (Liu *et al.*, 2020).

IT operations management establishes the direction in which the department should approach services and support. That is, its primary goal is to ensure that services are available when and when they are required. Companies need IT operations management because the growing need for on-demand IT services, high availability of systems and applications, and business developments lead to the IT operation merging with the company's operations. It must be stated that very few businesses and organizations would exist today without the use of systems and applications.

The new power is availability. Services that can be accessed via portals, mobile apps, apps, or other means must be accessible wherever and whenever they are required. An efficient IT Operation management assist to achieve this.

Any IT-powered organization can profit from efficient IT Operation Management. By enhancing the procedures that drive those efforts, an efficient IT Operation Management can assist optimize the delivery and maximize the quality of business and IT services. It can help IT teams better monitor the health of their company's IT estates and can assist those teams in anticipating and preventing unplanned outages, as well as quickly resolving issues with minimal business disruption. An efficient IT Operation Management can also aid in the reduction of business risk, as well as the enhancement of governance and adherence to legislation and business needs (Rahimi, Møller and Hvam, 2016).

Because an efficient IT Operation Management increases visibility into the IT estate and how it performs, it can provide these and other business benefits. Other IT management functions provide visibility into IT resources and the links that connect them, as well as the services and users they enable. An efficient IT Operation Management expands such visibility to include core operational processes as well as the linkages between them and the IT estate as a whole.

An efficient IT Operation Management can also help with crucial operational process execution. And can decrease or eliminate inconsistencies and errors that plague manual processes by automating repetitive components of process execution. An efficient IT Operation Management with automation can extend the reach of limited, expensive human experts and free staffers for more sophisticated or higher-value work.

Every company is seeking or exploring digital transformation in some way. Because digital technologies are changing the way practically everything is made, bought, and sold, as well as how consumers and partners expect to do business, this is a business imperative (Rahimi, Møller and Hvam, 2016).

An efficient IT Operation Management boosts profits. One of the primary benefits of implementing an efficient IT Operation Management is that it allows a company to operate better. As we all know, when a company performs better, it can reap greater earnings as a result of better configuration management and increased internal and external security (Boynton, Zmud and Jacobs, 1994).

A business is a vulnerable target for fraudsters, and if companies don't manage their security appropriately, infrastructure components could be jeopardized. A lack of an efficient IT Operation Management, along with a lack of infrastructure, will undoubtedly place an organization behind competition (Pilorget and Schell, 2018).

The consumer will have a better experience if an organization's networking and connectivity elements are improved through an efficient IT Operation Management. If a company is offering a tech-based service like SAAS, the constancy of service can make or break business. An efficient IT Operation Management enables company to manage company's capacity, performance, and availability without putting in a lot of effort. This is owing to the challenge of tying together the diverse threads of organization's virtual presence utilizing traditional IT approaches.

Operations management is also critical for minimizing any downtime that a company may face. If a company is not available to consumers, there's a significant possibility they will look elsewhere for similar services that they can be confident are more trustworthy.

Using technologies like performance monitoring, efficient IT Operation Management facilities can verify that infrastructure is appropriately maintained. When a company have the necessary tools to monitor the crucial operations that keep everything afloat, the issues it encounters will be considerably easier to manage.

Integrating an efficient IT Operation Management in company means that it can run a productive help desk/service desk that can quickly resolve difficulties for employees. This will boost company's productivity and provide its staff more independence because they won't have to rely on IT team to fix problems. As a result, company's capabilities will be enhanced, and it will be able to provide better results.

An efficient IT Operation Management may also assist in ensuring that company is resilient enough to withstand any disaster. In most circumstances, this manifests itself as either a major data breach or simultaneous server and backup failures.

Even if this is an uncommon occurrence, it's better to be prepared for the worst, especially if the management is working with sensitive data that company might not be able to recover. IT operations management can assist in ensuring that everything is backed up on a regular basis.

Improved asset management, which is connected with an efficient IT Operation Management deployment, can also help get more productivity out of company's personnel, particularly IT team. This is usually accomplished by increasing the visibility of the processes that company relies on to run properly.

2. Gaining efficiency through effective monitoring

1. Monitoring IT infrastructure

Businesses and organizations that rely on IT to supply their products and services must construct and manage an IT infrastructure. All of the assets required to supply and support IT services are included in IT infrastructure: computer hardware and software, storage, data centers, servers, networks, and other infrastructure. While IT infrastructure include both physical and virtual assets (software, virtual machines, virtual servers, and so on), IT policies and processes, as well as human resources, are not included.

Specialized solutions are used by IT organizations to collect data in the form of event logs from across the organization's IT infrastructure. In reaction to network traffic or user activity, apps or devices on the network generate event logs automatically. The time and date of the event, the user who was logged into the machine, the name of the computer, a unique identifier, the source of the event, and a description of the event type are all stored in these log files. Depending on the application from which the log files were generated, some log files may contain additional information (Srinivasan and Parlikad, 2013).

Aspects of an efficient Monitoring of IT Infrastructure

A malicious actor wishing to obtain access to organization's sensitive or proprietary data can use any endpoint or application linked to the network as a potential attack vector. Even hardware equipment should be checked on a regular basis for health issues, especially if a hardware failure could result in unforeseen downtime or income loss.

Hardware monitoring software collects information from sensors in computers and other machines. Battery life information, power and load sensors, current and voltage sensors, fan speed sensors, and user-defined artificial sensors that collect data on the operating system are examples of these (Hernantes, Gallardo and Serrano, 2015).

Network monitoring ensures that company's internal network is operating properly and provides the speed and performance. Operation manager team may check the transmission rate and connectivity levels that users are experiencing on the network, as well as monitor incoming and outgoing connections, using IT infrastructure monitoring tools. When an illegal person tries to access network, network monitoring can assist IT department respond quickly (Barth, 2008).

Monitoring applications is an important part of IT infrastructure monitoring. Members of IT organization or clients of the firm may use programs installed on servers. In either scenario, applications are a possible vector of attack for a hostile actor as well as a valuable source of operational and business knowledge. Organizations can monitor user activity on applications using today's IT infrastructure monitoring solutions to gain operational insights and uncover business opportunities (Lee, Levanti and Kim, 2014).

Monitoring Enterprise IT Infrastructure Efficient methods

IT infrastructure monitoring allows to detect security threats and resolve operational issues before they have a detrimental impact on consumers.

The following are three best methods to assist attaining and maximizing the benefits of IT infrastructure monitoring:

1. Organizing and Prioritizing Alerts: IT infrastructure produces massive volumes of data in the form of event logs every day. Organizations need to set up program so that it sends out notifications for specified categories of events. It is crucial to decide which types of notifications are given the highest priority, as these are the ones that require immediate attention. Major occurrences, such as server outages and probable security breaches, should be quickly reported to team, but less serious incidents should be treated with less urgency (Sabeur *et al.*, 2017).

2. Providing Processed Data in a Dashboard: IT infrastructure monitoring software products can be configured to display processed data in a dashboard. A dashboard is nothing more than a visual representation of data. Dashboards can be set up to display operational data, provide business insights, or highlight unusual activities that may indicate security issues. Customize dashboards for each job, such as a security dashboard for IT security analysts, operational dashboard for IT Ops, and a financial or business metrics dashboard for salesmen or organization's CFO, to efficiently exploit this data (Mayer and Weinreich, 2017).

3. Selecting a Trustworthy Vendor Partner: When it comes to IT infrastructure monitoring, businesses with established IT operations confront a difficult decision about buying or building their own. A trustworthy vendor partner can provide one-on-one support and consultancy to help configure and maximize the value of IT infrastructure monitoring solution. Their experience and understanding are well worth the money (Özer and Zheng, 2017).

Challenges in Infrastructure Monitoring

It is sometimes necessary to take a proactive approach; after all, that's what monitoring is all about. Here are some of the most typical monitoring difficulties that businesses, in general, and IT departments, in particular, face:

1. Being beyond Monitoring capacity

The expanding number of devices and networks to monitor is the most typical concern with infrastructure monitoring. Infrastructure evolves in tandem with the organization's growth. Keeping track of which devices and apps make up the organization's IT ecosystem difficult enough. But, on top of that, keeping track of each of them adds to the difficulty (Levinson, 2000).

Organizations might as well cease monitoring altogether if the monitoring instrument or team is unable to obtain actual performance monitoring. With this level of complexity, evaluating genuine performance and identifying problems before they become more serious becomes more difficult.

Many businesses have scattered systems all across the world, which exacerbates the problem. IT staff in charge of infrastructure monitoring may also have to deal with code, server, and service issues remotely.

Solution: Scalable monitoring application is required to keep up with the developing infrastructure. organizations need a system that can track and monitor services from beginning to end, as well as consolidate data from multiple sources into a single dashboard. This essentially means that organizations need monitoring software that has a number of distinct monitoring tools that all work together to provide the overall image (Jain and Chandrasekaran, 2020).

2. Ineffectiveness of outdated Monitoring application

Monitoring teams in many organizations are finding that the monitoring tools they're employing aren't up to the task of keeping up with growing infrastructure or the new types of technologies that are continuously being introduced into the IT ecosystem.

Some legacy infrastructure monitoring technologies were never meant to be used on the internet. They don't even give the actionable metrics that web performance teams want. They may provide log data and reporting warnings, but sifting through log data for anomalies is a time-consuming process (Commerce and Staff, 2002).

The solution to this widespread problem is a modern, versatile, and scalable monitoring technology. If companies truly want to enhance efficiency and avoid technical traps, they must rethink their objectives and put their money where their mouth is.

3. Increasing Prices

Rising infrastructure expenditures are also a major concern for many businesses. In some firms, infrastructure monitoring is also associated with cost reduction. For example, how to increase the efficiency of various systems while lowering expenses. Similarly, spotting a problem early on and correcting it before it becomes a major issue can save a company money. When a company's servers go down, it loses productivity and income. It all comes down to money and monitoring.

Slow and ineffective monitoring would be ineffective, resulting in higher expenditures due to data loss or IT infrastructure repairs. This isn't so much a monitoring issue as it is a security risk. However, monitoring tools should assist in identifying infrastructure issues that are causing money to leak.

Solution: To cut expenses, many businesses are turning to serverless computing. Serverless computing, is essentially a pay-per-use service that allows for easy expansion and flexibility. It does away with provisioning and management, replacing it with dynamic resource assignment as needed. This technique has ramifications for surveillance as well.

4. Data Capacity

Monitoring solutions with a centralized design and a one-size-fits-all architecture frequently fail to process, assemble, and analyze large amounts of data. With ever-expanding infrastructure comes ever-increasing data. However, if monitoring systems can only manage a certain quantity of data, this causes a bottleneck, resulting in inaccurate performance statistics.

Another issue with infrastructure monitoring tools is that many of them use skewed data. If organizations rely on batch data rather than a continuous stream, they may not be able to discover problems right away. Organizations essentially expecting that the problem, if it exists, will manifest itself in the data organizations received.

The majority of today's networks are software-defined, which means they must assess data in real time to discover any lags or errors. In today's organizations, data samples aren't going to cut it in the dynamic tech ecosystem.

The Solution of this challenge is to use an API-expandable monitoring program. Cloud-based computing, virtualization, and the Internet of Things (IoT) are examples of modern technology advancements that necessitate practically automatic infrastructure adjustments to address issues (Santoro *et al.*, 2018) (Marinakis *et al.*, 2015).

3. Gaining efficiency through IT process optimization

It is a strategic component for modern businesses that are becoming increasingly reliant on the usage of information technology in their operations in order to achieve their goals. Technologies such as cloud computing, collaborative software, and, in some more specialized areas, Big Data and Machine Learning, provide significant support for IT process optimization (Del Castillo, 2007).

IT process optimization encompasses more than just programming methodologies, software domains, and hardware understanding. The goal of IT process optimization in this situation is considerably more predictive than simply providing technical support and answering calls.

On the contrary, IT process optimization must be idealized in order for calls to become progressively obsolete. Even in contingency situations, situations of usage and provisioning of systems and software must fulfill the needs of the firm. To do this, IT managers must understand the organization's strategic objectives and how they add value to the solutions it provides to external and internal customers, ensuring that they are constantly satisfied.

The following steps should be taken to optimize the processes (Pyötsiä, 2005)**.**

• Assessing available technological resources

• Determining the organization's current inadequacies in regard to the resources that prevent it from reaching its objectives

• Reversing this trend by implementing these improvements and optimizations in the IT department.

• Organizing improvements in a holistic manner.

• Evaluating necessity of new IT process optimizations by monitoring the results.

• If required, taking calls and look for ways to reduce the number of times this happens.

Three ITIL process models are typically used
Information Technology Infrastructure Library (ITIL) is an acronym for Information Technology Infrastructure Library. The name was initially used by the British government in the 1980s, when it documented and printed hundreds of best practices in IT service management. ITIL is now a stand-alone phrase, not referring to the "Information Technology Infrastructure Library." (Dabade, 2012)

1: Workflow for the ITIL Service Desk

The management of IT services encompasses a wide range of operations in addition to managing changes and responding to incidents. Among these, we should not overlook customer service (the Service Desk), which follows an ITIL-recommended procedure. The flow begins with the call's opening, which can go through two levels of support. It is only completed when the user who initiated the call verifies that the issue has been resolved (Soomro and Hesson, 2012).

2: Using ITIL to manage changes

As a natural result of IT process optimization, some modifications will always be required when managing IT services. The objective here is to facilitate change with as minimal disturbance to IT service provision as feasible. ITIL provides for six agents, including two committees (one for emergency adjustments), to work together in this way: Initiator of a Change, Change Agent, Change Execution, Implementer of Change, Change Advisory Council, Advisory Committee on Change

3: Incident Management (ITIL)

The purpose of using the ITIL technique to manage an event is to not only promptly resolve it, but also to establish a knowledge base so that similar issues can be avoided in the future. As a result, it attempts to provide speedy responses in the event that problems arise again, because the system keeps track of beneficial remedies. The ITIL model of IT service management proposes six methods to do this: Detection of Incidents, Resolution, Closing, Monitoring, Classification, Diagnosis (Barafort, Di Renzo and Merlan, 2002).

4. Gaining efficiency through Devising efficient IT policies

Policies for IT emergency intervention and disaster recovery: Business continuity plan and disaster recovery policy: Natural and man-made disasters can imperil a company's operations and future, therefore it's vital to design a plan to ensure that business activities continue in the event of a disaster. Policy for severe weather and crises: This policy outlines procedures for dealing with severe weather and other emergencies.

Policy on data and resource recovery: All personnel should be familiar with the procedures for retrieving data if it is lost, inaccessible, or compromised. This policy outlines the procedures for retrieving data from company-owned or purchased resources, equipment, and/or services.

Unauthorized access to a workplace network or campus network, whether launched with criminal intent or not, is an all-too-common event. Every company should establish a strategy for assessing and then recovering from unwanted network access. This policy serves as a framework upon which IT operation team can create their own procedures (Schneider, 2000) (Goguen and Meseguer, 1982).

Security policies for information technology

The Security Incident Response Policy outlines the organization's process for minimizing and mitigating the effects of an IT security-related incident, such as a data leakage, malware infection, insider infringement, distributed denial of service (DDoS) attack, or even equipment loss or theft. The policy's goal is to establish the procedure to be followed when an IT-security issue occurs for employees, IT department staff, and users.

Policies related to Data encryption: The purpose of the data encryption policy is to define the encryption requirements to be used on all computer, server, network storage, and storage area network disks and drives that access or store organization information in order to prevent unauthorized access to organization communications, email, records, files, and databases for employees, computer users, and IT department staff.

Policy on information security: IT is responsible for safeguarding company's private and confidential data, which includes everything from sales records to employee social security numbers. To do so, organizations need to define acceptable and undesirable system usage, as well as assign tasks to employees, IT professionals, and supervisors/managers. This policy lays out a detailed plan for setting standards, rules, and guidelines for safeguarding company's sensitive information.

Policy in order to protect Identity theft and remote access: This policy helps safeguard staff and customers from identity theft with an identity theft policy. This policy outlines risk-reduction

measures, warning signals to look for, and what to do if IT operation team suspect identity theft. This policy provides the procedures and standards for requesting, gaining, using, and terminating remote access to the organization's networks, systems, and data.

Perimeter security policy: While security principles should be used throughout the company, securing the perimeter and ensuring that only necessary connections are allowed is a particularly important goal. This policy outlines procedures for securing the network perimeter of company against potential threats (Gil-García, 2004).

Security consciousness and training policy: The value of a security policy is determined by the knowledge and efforts of people who follow it, whether they are IT personnel or regular users. This policy is intended to assist information technology team in assisting employees in understanding and following best security practices that are relevant to their job duties in order to avert a potential security issue (Ward and Smith, 2002).

5. Conclusion

IT Operations Management is the process of continuously monitoring all aspects of an organization's IT infrastructure. An efficient IT Operations Management aids in the improvement of corporate processes and services' availability, proficiency, and performance. Organizations can't afford to rely on antiquated processes and ineffective, overlapping instruments when so much is at stake. They ought to focus on efficient IT Operations Management technologies. This one version of the truth will allow IT leaders to identify bottlenecks, assess how the IT infrastructure responds to specific changes, and discover early warning signals of any issues that could affect performance. It's the only way to avoid downtime and maximize the value of IT operations.

An efficient IT Operations Management assist in attaining reduced outages and faster response times, increased productivity, resulting in a better client's experience. An efficient IT Operations Management can improve Efficiencies by streamlining the administration of infrastructure and service components and improving operational agility, time can be saved. Through An efficient IT Operations Management, employee workflows and productivity are preserved, partner relationships are improved, and end customers receive better service.

The past, present, and foreseeable future of IT Operations Management -related advancements all point to the same conclusion. IT management must become totally operationally focused and directed by business objectives and goals in order to optimize its business value and agility .IT Operations Management that is truly efficient is a significant step toward that goal. It's also an important part of laying a solid, adaptable basis for company's future IT enhancements and digital transformation activities.

References

Atieh, A. T. (2021a) 'Assuring the Optimum Security Level for Network, Physical and Cloud Infrastructure', *Rsearchberg Review of Science and Technology*, 1(1), pp. 15–30. Available at:

https://researchberg.com/.

Atieh, A. T. (2021b) 'The Next Generation Cloud technologies: A Review On Distributed Cloud, Fog And Edge Computing and Their Opportunities and Challenges', *ResearchBerg Review of Science and Technology*, 1(1), pp. 1–15. Available at: https://researchberg.com/.

Bacelar, M. (2021) 'Monitoring bias and fairness in machine learning models: A review', *ScienceOpen Preprints*.

Barafort, B., Di Renzo, B. and Merlan, O. (2002) 'Benefits resulting from the combined use of ISO/IEC 15504 with the Information Technology Infrastructure Library (ITIL)', in *International conference on product focused software process improvement*. Springer, pp. 314–325.

Barth, W. (2008) *Nagios: System and network monitoring*. No Starch Press.

Boynton, A. C., Zmud, R. W. and Jacobs, G. C. (1994) 'The influence of IT management practice on IT use in large organizations', *MIS quarterly*, pp. 299–318.

Del Castillo, E. (2007) *Process optimization: a statistical approach*. Springer Science & Business Media.

Commerce, G. B. O. of G. and Staff, O. of G. C. (2002) *ICT Infrastructure Management*. Stationery Office (IT infrastructure library). Available at: https://books.google.nl/books?id=K9DXQgAACAAJ.

Dabade, T. D. (2012) 'Information technology infrastructure library (ITIL)', in *Proceedings of the 4th National Conference*, pp. 25–26.

Gil-García, J. R. (2004) 'Information technology policies and standards: A comparative review of the states', *Journal of Government Information*, 30(5–6), pp. 548–560.

Goguen, J. A. and Meseguer, J. (1982) 'Security policies and security models', in *1982 IEEE Symposium on Security and Privacy*. IEEE, p. 11.

Hernantes, J., Gallardo, G. and Serrano, N. (2015) 'IT infrastructure-monitoring tools', *IEEE Software*, 32(4), pp. 88–93.

Jain, S. and Chandrasekaran, K. (2020) 'Industrial automation using internet of things', in *Security and privacy issues in sensor networks and IoT*. IGI Global, pp. 28–64.

Lee, S., Levanti, K. and Kim, H. S. (2014) 'Network monitoring: Present and future', *Computer Networks*, 65, pp. 84–98.

Levinson, D. M. (2000) 'Monitoring infrastructure capacity'.

Liu, X. *et al.* (2020) 'Using Language Models to Pre-train Features for Optimizing Information Technology Operations Management Tasks', in *International Conference on Service-Oriented Computing*. Springer, pp. 150–161.

Marinakis, V. *et al.* (2015) 'Advanced ICT platform for real-time monitoring and infrastructure efficiency at the city level', in *2015 6th International Conference on Information, Intelligence, Systems and Applications (IISA)*. IEEE, pp. 1–5.

Mayer, B. and Weinreich, R. (2017) 'A dashboard for microservice monitoring and management', in *2017 IEEE International Conference on Software Architecture Workshops (ICSAW)*. IEEE, pp. 66–69.

Özer, Ö. and Zheng, Y. (2017) 'Establishing trust and trustworthiness for supply chain information sharing', in *Handbook of information exchange in supply chain management*. Springer, pp. 287–312.

Pilorget, L. and Schell, T. (2018) *IT Management*. Springer.

Pyötsiä, J. (2005) 'ICT opportunities and challenges for remote services', in *IFIP Working Conference on Industrial Applications of Semantic Web*. Springer, pp. 213–225.

Rahimi, F., Møller, C. and Hvam, L. (2016) 'Business process management and IT management: The missing integration', *International Journal of Information Management*, 36(1), pp. 142–154.

Sabeur, Z. *et al.* (2017) 'Large scale surveillance, detection and alerts information management system for critical infrastructure', in *International Symposium on Environmental Software Systems*. Springer, pp. 237–246.

Santoro, G. *et al.* (2018) 'The Internet of Things: Building a knowledge management system for open innovation and knowledge management capacity', *Technological forecasting and social change*, 136, pp. 347–354.

Schneider, F. B. (2000) 'Enforceable security policies', *ACM Transactions on Information and System Security (TISSEC)*, 3(1), pp. 30–50.

Shaheen, M. Y. (2021a) 'Adoption of machine learning for medical diagnosis'.

Shaheen, M. Y. (2021b) 'AI in Healthcare: medical and socio-economic benefits and challenges'.

Shaheen, M. Y. (2021c) 'Applications of Artificial Intelligence (AI) in healthcare: A review'.

Soomro, T. R. and Hesson, M. (2012) 'Supporting best practices and standards for information technology Infrastructure Library', *Journal of Computer Science*, 8(2), p. 272.

Srinivasan, R. and Parlikad, A. K. (2013) 'Value of condition monitoring in infrastructure maintenance', *Computers & Industrial Engineering*, 66(2), pp. 233–241.

Ward, P. and Smith, C. L. (2002) 'The development of access control policies for information technology systems', *Computers & Security*, 21(4), pp. 356–371.