TERM RESEARCH PAPER
SCHOOL OF MANAGEMENT, UNIVERSITY AT BUFFALO

Title: Pre and post pandemic adoption of BYOD, migration to Public Cloud (Paas) & effect on productivity tools

Submitted To: Dr Manish Gupta, CISA, CRISC
By: Akhilesh Anand Undralla, Chethana Rangaswamy, Kedar Purushottam Inamdar, Rahul Pratap Singh, Rohan Kandyana

INTRODUCTION:

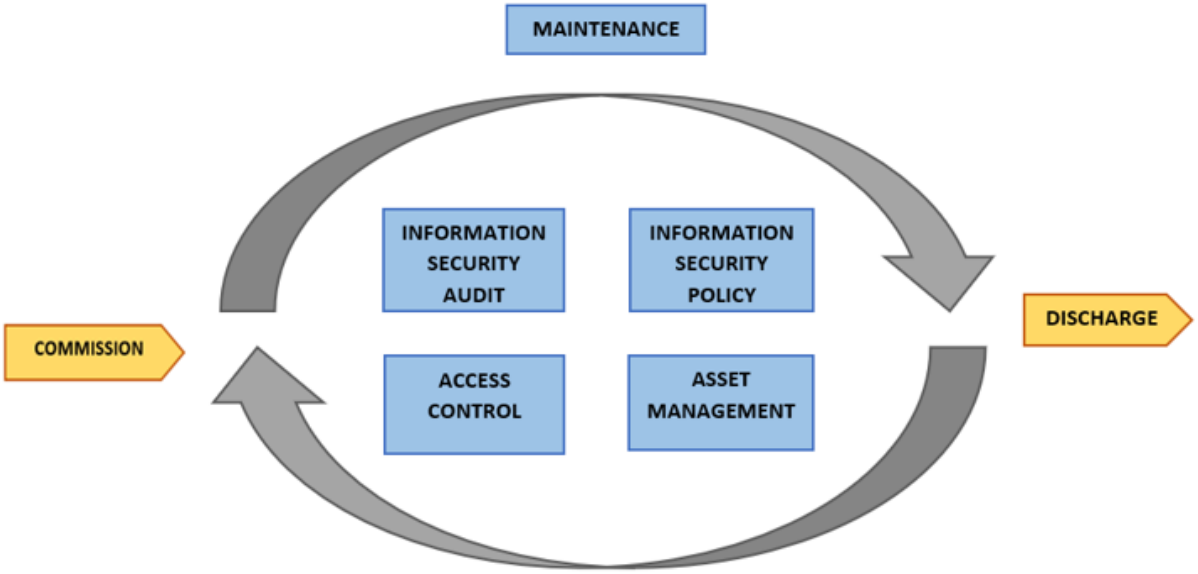
Bring Your Own Device BYOD & working from home (WFH) are a relatively new trend in which employees can work and access enterprise-level software, databases, files & networks through their own electronic devices such as smartphones, tablets, personal digital assistants, through their network instead of a secure intranet provided by the organization. Since several industries are going through massive changes due to the pandemic, BYOD & WFH have become an essential policy to adopt as a strategic restructuring of IT architecture. BYOD & WFH gave rise to reevaluating security policies and adopting cloud technology. This is a relatively new field in data, network and mobile security that derives from the appearance of smartphones and tablets and in particular, introducing such devices in the working environment. This implies devices that are used for both work and personal tasks tends to have shared or duplicated data and network connections.

It's more convenient for employees to choose the best devices & secure network infrastructure for their office work which adds to their productivity and incorporates better work-life integration. Allowing employees to use their own devices & WFH can result in cost savings through reduced hardware costs & operational cost of maintaining workspace. Increased productivity, greater employee morale and potential cost savings are the reasons many IT managers support BYOD & WFH policies.

Some of its challenges are related to security issues concerning data leaks, encryption issues, data theft, secured network risks, access management & physical security of/access to the device which makes corporate information vulnerable. Whereas network congestion, lost devices, regulatory compliance, and user permission issues have become risks for the companies.

SCOPE:

While enterprise governance and risk management have been subject to audits for a considerable time the recent shift in the working environment due to global pandemic has been unforeseen. This research paper attempts to outline the changes to the audit process that need to be brought in owing to this change in the working environment. As a result, the primary focus of this paper will revolve around the changes to the working environment owing to the use of BYOD and/or work from home (WFH) operations, and the need for additional control measures required to mitigate risk.



USER FLOW IN BYOD ENVIROMENT

As the pandemic has affected most if not all industry sectors, the research paper will provide an overview of the risk-based auditing collectively and will not focus on a particular sector or industry. Some of the key focal points of the study will be based on :

- Migration to Cloud into a Hybrid setup
- System Migration and Infrastructure deployment
- IT Asset Management
- Access Management
- Productivity Tools
- Network & Endpoint Security
- Web-based Communication Services (VoIP, Meetings, Social Media)
- Review Business Continuity Planning
- Changes to Audit Process and Priorities

APPROACH:

With our research on said topic, we intend to

- Define working environment (pre-pandemic): what were the IT Audit and Risk Management processes and procedures that were followed?
- Auditing and Risk assessment varies by industry depending on each of their operating environments, business models and how revenues are generated.
- Many organizations use the ERM framework to identify risks with respect to operations, project & strategy, assessing risks, prioritize them and respond to them.
- Assessing various Standards & Controls, which are commonplace in a Hybrid Cloud setup, such as SOC2, HIPAA, ISO 27001, GDPR etc.
- Identify the type of control to test against based on the nature of assurance required, ie. protective, detective & corrective.

- Identify risks to classify them based on their possible impact & likelihood, in a typical Risk-Register.
- Suggesting corrective measures & best frameworks based on the Industry, IT infrastructure, earlier identified controls & risks.

Note: Last 3 steps will be repeated in all Pre-Pandemic, During-Pandemic & Post-Pandemic

- Define working environment (during-pandemic): What are the changes to IT Audit and Risk Management that were carried on earlier? How have the organizations coped up with the changes?
- Digitization: The functioning of almost all thriving businesses have moved online, cloud migration has seen a massive increase in turn raising the risk factors.
- Extensive usage of BYOD, Secure collaboration, identity management, enhanced cloud security.
- Suggest Measures to give Reasonable Assurance: Changes in risks on the Risk Register, Procedures to analyze predictive, corrective and preventive risks & changes in prominent Policies, Standards & Procedures.
- Define anticipated working environment (post-pandemic): What are the anticipated changes in the policy, standards & procedures post-pandemic? Which are expected to be retained?
- Changes in the Audit process, Control parameters, Risk Assessment & Policies
- Suggested Measures: To ensure that the organizations are flexible & prepared to instantly adapt to any similar future events. Explore what policies, standards & procedures should be retained.

OBJECTIVES:

- How IT Auditing and Risk Management procedures have changed due to pandemic and rapidly increasing demand for BYOD usage at organizations, the kind of impact these changes have had and how organizations have adapted to these changes.
- Impact of cloud in a Hybrid model on PaaS, on security, compliance, databases, files, network, infrastructure, operating cost, access management & processes efficiency.
- Assessing cybersecurity risks, solutions in place on cloud & On-Prem, cost of implementation & operational cost
- Ensuring efficient functioning with the least amount of downtime of productivity tools, such as CRM, ERP, HRMS, etc
- Increase in cybercrime and other security threats during Covid pandemic, what are the measures taken by the organizations to tackle these issues?
- This study will help us compare and analyze the transformed risk management practices that are being followed at present, how it has impacted and how this could be bettered.

1. **BYOD – Pre Covid-Pandemic:**

1.1. The policies enforced by organizations for BYOD usage:

- OS versions and Device platforms – identifying required features as per organizations need and clearly specify the kind of mobile device platform and operating system versions the company is willing to accept
- Device enrolment process – ensuring the BYOD devices are registered and authenticated by the organization before connecting to the company's network, this way the system admins could easily detect any unauthorized device access to the company's network
- Passwords – enforce usage of complex passwords for all BYOD devices; determine the complexity of the password and how often the user should change the password to avoid the system from being compromised. Ensure the repercussion of not following the set regulations is made clear
- Confidential Content – establishing what documents the users are allowed to save, print, email, etc… Setting mobile data leakage prevention policies and monitoring users compliances is essential. Ensuring details on how sensitive data will be handled like usage of a secure content container on the mobile device or laptop.
- Allowed Applications – the organization needs to decide and list the number of apps that are allowed and not allowed (anticipated harmful once) to be used. Ensure the company's critical business apps are secure and segregated on BYOD. Enforce strict action if violated
- Lost devices and theft – there is always a possibility of loss or theft of BYOD devices. Employees are required to notify IT immediately when this happens so the device passwords can be remotely reset or wiped. Even an auto-wipe of certain apps after a certain number of failed login attempts could be enabled. This process has to be in place, and the users need to be aware of the specifics and follow them.
- Encryption of data – ensuring that every sensitive data stored on personal devices is encrypted with strong and full encryption. In case of the infeasibility of full encryption, all sensitive data should be stored in encrypted folders on the device. Employees to be warned on blockage of devices if found non-compliant.
- Employee departure – in order to safely and securely remove all the sensitive data from the user's BYOD, a thorough plan for your employee's departure is enforced that includes either a total device wipe or a selective wipe of certain apps and data. Every employee to be made aware of this during the BYOD enrolment process for compliance purposes.
- User Agreement – Most crucial part of BYOD policy, to ensure every employee has a clear understanding of organizations regulations, rules, processes and policies concerning usage of BYOD and acknowledge the terms by signing an agreement.

Though these discussed policies were known to be in place at many organizations even before the pandemic hit, how effectively were these policies enforced or strictly followed by employees is a question as cyber threats have always been making news worldwide.

1.2. The Risks involved with BYOD usage and the Controls to mitigate these risks:

1.2.1. Data Leakage:

Regardless of whether the employees need to access their corporate/personal email or protected payroll information via mobile, data leakage is a possibility when personal devices come into play. Data can be lost or exposed when devices are misplaced or stolen, or if a personally-owned device has malware on it.

Ways to prevent data leakage include:

- Mobile device management: In case of loss or theft, an MDM program can enable IT to remotely "wipe" a device to ensure sensitive information is not exposed.
- Smarter data provisioning: Minimum necessary access is the smartest way to limit exposure. Role-based provisioning is optimal for security.
- The use of app segregation and/or a VPN: Segregation and VPNs prevent sensitive data from being leaked via sketchy public wireless hotspots, and can create barriers between personal and work content on a personal device.
- File integrity monitoring: Agent-based file integrity monitoring software that operates at the kernel level can notify IT the moment malware gains access to a device, allowing an organization to take action before it impacts the company's network

1.2.2. Sketchy Applications:

Not all personal apps are what they appear to be, or have any business being on end users' mobile devices, they could just be some fake and malicious apps. TechCrunch reported that some of the confirmed malicious apps included titles such as "Pokémon Go Ultimate," "Guide & Cheats for Pokémon GO," and "Install Pokémongo," to appeal and attract game fans from downloading these. In most cases, malicious apps have the potential to take control over the user's mobile device. This can result in surveillance, unexpected data or call charges, or loss of personal or work information.

Ways to prevent this:

User's need to be trained on app best practices. This knowledge-based training should include the importance of only downloading content from genuine/authorized apps stores. In many cases, malicious mirrors or personal apps are downloaded through web pages as well.

1.2.3. Lack of Management:

With any mobile device, employee or company-owned, there are risks associated with a loss of control. When an endpoint walks out of your company's building, it can be difficult to control whether it's used on questionable free wireless connections or whether it will be misplaced and stolen. Protecting mobile and laptop endpoints from exposure requires IT pros to focus on a mix of device security, layered protecting, and smarter provisioning.

Ways to prevent this:

- Mobile device management: MDM allows employees to remotely control the content and security of an employee's device. When coupled with file integrity monitoring, IT pros can establish an optimal level of control.
- Enterprise Apps Stores: Providing employees with easy access to the right apps approved for business use can mitigate the risks of "shadow IT," or employees using apps outside approval or your VPN.
- Single Sign-On: A password-protected lock screen is likely not enough protection for endpoints. By segregating and protecting your mobile apps via a single sign-on (SSO) requirement, IT pros can enable smart user authentication without disrupting productivity.

1.2.4. Device Infection:

The vast majority of users with an infected smartphone don't know their device is carrying malware. Even more concerning, feelings of "app fatigue," or excess exposure to mobile content, can make users care less about mobile security. They may not read the terms of service on new apps or think twice before granting excessive permissions when downloading new content. Outdated mobile operating systems can be a major risk factor, with some of the most vicious forms of malware primarily affecting outdated OS's.

Ways to prevent this:

Ensure that mobile operating systems are kept up-to-date. Even new OS's have vulnerabilities, so it's also crucial to use file integrity monitoring to immediately detect and act on device infection.

1.2.5. Poor Policies:

It may be possible to attempt a BYOD program without effective security policies in place, but it's certainly risky. If an organization is required to comply with PCI DSS, HIPAA, or any other regulatory requirements, effective policy is necessary to avoid fines.

Ways to prevent this:

With a combination of written policy and policy-based administration, IT pros should address each of the following:

- Passwords, lock screens, and single sign-on
- Network connectivity
- Required use of a VPN
- Real-time updates and patching
- Location tracking
- Mobile device management

1.2.6 Mixing Personal and Business Use:

With BYOD, mixing business and personal use is inevitable. Organizations can't control whether the employees decide to shop online at compromised websites or whether they will misplace a device. While the companies can educate heavily on security best practices, one can't guarantee that the employees won't loan their device to a friend or use public wireless connections to save data.

Ways to prevent this:

- App segregation: Creating a strong barrier between personal and private use on the device, thereby preventing accidental access to work data.
- Use of a VPN: A VPN can protect communications from interception, even if employees are trying to use a coffee shop's wireless network.
- File integrity monitoring: IT pros can gain access to negative changes to critical system files or security, allowing them to act immediately.

1.2.7 Inability to Control Devices

What if an employee leaves the organization or loses their mobile device? In many BYOD programs, the majority of the security stress comes from a lack of control around devices. Employees are not always careful, and disgruntled staff can do a lot of damage with too much access.

Ways to prevent this:

Usage of Mobile device management and smarter access governance. If an employee is terminated or begins exhibiting questionable behaviours, policy should support the company's ability to immediately revoke access to sensitive data before it's leaked.

2. <u>BYOD – Post-Covid-Pandemic:</u>

Before the covid pandemic, the policies, the risks involved and controls to mitigate risks with BYOD usage were already enforced and followed by many organizations; however, post-pandemic smaller organizations and most other bigger organizations who were not using BYOD, had no choice but to enforce usage of BYOD to keep their businesses afloat. In response to the increasing prevalence of BYOD at the workplace, organisations need to identify all the devices and operating systems used by their employees, as well as the applications that they need to access from personal and mobile endpoints.

Since there has been a significant rise in BYOD usage, to complement this, so is there an intensified and significant rise in cybercrimes. Cyber-attackers see the pandemic as an opportunity to step up their criminal activities by exploiting the vulnerability of employees working from home and capitalizing on people's strong interest in coronavirus-related news (e.g. malicious fake coronavirus related websites). Before the pandemic, human error was already a major cause of 'cyber insecurity' employees would unknowingly or recklessly give access to the wrong people. Also, about 20% of cyberattacks used previously unseen malware or methods. While during the pandemic, the

proportion seems to have risen to 35%. Some of the new attacks use a form of machine learning that adapts to its environment and remains undetected.

So, how have organizations coped with this and ensured to mitigate increasing cybercrimes with increased usage of BYOD?

Organizations must have the ability to monitor employee-owned devices at the device level from the moment they're provided with access to company data and every minute of the time they're used for work or personal activities off-site. To be able to do this and at the same time ensure the cybercrimes and data breaches are kept at bay, the policies as discussed before Covid situation, have been more strictly followed by every organization and stringent action being taken against those being non-compliant to any of the company's BYOD usage policies.

Alongside the security solution need to be backed up by legal agreements to provide a greater degree of protection in the event of something going wrong and extensive usage of classic mobile device management, companies are also adapting usage of

- **Mobile application management (MAM)** - In contrast to MDM, mobile application management (MAM) focuses on securing and protecting company-provided applications if the solution is primarily used from a BYOD perspective to support the day-to-day employee needs – a travelling salesperson who requires access to email or in-house CRM systems for example. To ensure that application data is secure and protected, various company applications are made available for mobile use, which is then managed centrally by security administrators or IT personnel. However, similarly to agent-based MDM solutions, MAM also requires the installation of external software on employee devices. largely because the agent is the only way business data can be remotely wiped if a device is lost. Like many mobile security solutions, MAM also has some limitations, particularly around detecting and blocking shadow IT. While MAM strongly governs many corporate applications, it does not cover popular cloud applications like Gmail, Dropbox and Slack. What's more, a usage policy also needs to be installed to ensure adequate data protection, as the solution does not provide any device management functionality.

- **Agentless mobile security** - Developments in cloud-based security tools have given rise to a new set of mobile security solutions that can protect data without installing an agent on the employee's device. Yet at the same time, these mobile security solutions still provide all MDM functions, including data loss prevention and remote wiping of company data. They can also offer data encryption that can be extended to all popular cloud apps, including G Suite, Office 365, Slack and Salesforce. This simply means that all types of critical data will ultimately be secure, regardless of what application an employee is accessing via their personal device. While all devices accessing corporate data are still required to be centrally managed, security administrators can govern mobile devices without installing intrusive management software or an agent on every individual device, essentially making them "agentless." As a result, rollouts are conducted more quickly while also alleviating many users' privacy concerns or hesitancy in allowing employers to fully access their personal information. In general, these kinds of agentless solutions are largely aimed at businesses

worried about security issues attributed to cloud application access from personal devices. And with the increasing popularity of cloud services, the number of agentless solutions is firmly set to rise – a trend validated by Gartner analysts who predicted in 2015 that more than half of BYOD users with an MDM agent on their device will be managed by an agentless solution that year.

- **Apply new technology and tools** - Companies are using advanced tools such as host checking (a tool to check the security posture of an endpoint before authorizing access to corporate information systems) to reinforce the security of remote working.
- **Intelligence techniques** - proactive usage of cyber threat intelligence to identify relevant indicators of attacks (IOC) and address known attacks.
- **Risk management** - usage of governance, risk and compliance (GRC) solutions for improved risk management. GRC solutions provide a detailed view of the company's risk exposure and help link together the various risk disciplines (e.g. cybersecurity, operational risks, business continuity).
- **Prepare for attacks** - In these high-risk times, companies are carrying out frequent cyber crisis simulation exercises to prepare their response to a cyberattack.
- **Zero Trust** - CISOs and CIOs are implementing a zero-trust approach to cybersecurity. This is a security model where only authenticated and authorized users and devices are permitted access to applications and data. It challenges the concept of "access granted by default".

2. **The premise of enterprise applications:**

Organizations have been using productivity tools for ease of business and the value addition they provide for quite some years now. The productivity tools term comprises a variety of different applications that are used for specific or general tasks across an organization often spanning multiple domains. Some of the most common examples include Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), Office Suites, Business Intelligence Tools, and Communication and Collaboration tools among others.

While these tools often depend on the industry the organization is operating in and the specific needs of the company, a more general categorization of these tools can be made based on their deployment that is on-premise and cloud-based. A considerably large number of firms have already shifted parts of their workloads to the cloud whereas other companies are expected to follow suit in coming years. This is evident from the Forbes article stating that 83% of enterprise workloads will be shifted to the cloud by 2020 as compared to just 27% on-premise.

The above premise of distinction becomes necessary to adjust the lens of IT audit to enterprises based on their workload deployment. A further distinction between applications can be self-developed applications and third-party applications. Even here, a majority of the applications are bought from a third party with the additional step of customization.

Enterprise Application 1		
	On-premise	Cloud based
Third Party Application		✖
In-house Developed Application		

Enterprise Application 2		
	On-premise	Cloud based
Third Party Application	✖	
In-house Developed Application		

The above distinctions are important as we divide the associated risks and necessary controls of these applications based on this categorization.

2.1. Application audits

Application audits are done based on audit plans per application and can vary from a period of 6 months to five years based on the criticality of the application. However, audits are defined by the stage at which they are carried out, such as system development, post-implementation and on a regularly scheduled basis. At any level of these audits, the basic necessity lies in gathering reasonable assurance of the degree of control over the data processing which is dependent on the associated risk profile of the data and process. At a minimum, the risk-based audit of applications includes the following key areas,

- Administration
- Inputs, Processing, Outputs
- Logical Security
- Disaster Recovery Plans
- Change Management
- User Support
- Third-Party Services

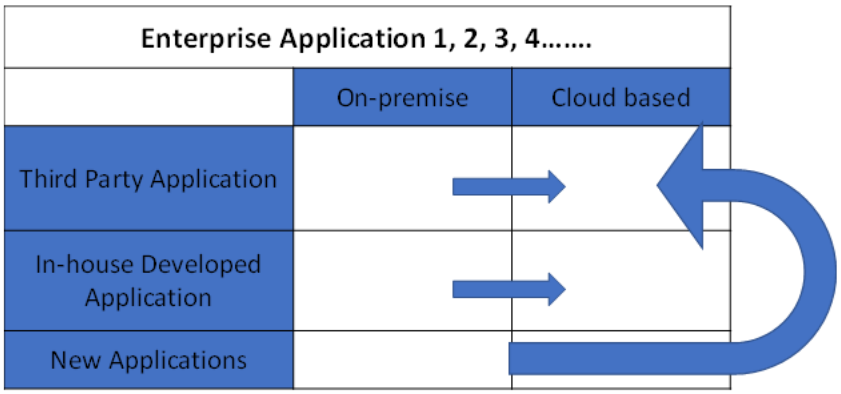
In addition to the above-mentioned sections, any productivity tool can be audited based on a specific audit objective as well such as Compliance audit, Process audit, Risk audit, System audit, and Security audit.

2.2. Covid 19 and the IT environments worldwide

The Covid 19 situation that erupted last year has a certain level of uniqueness in terms of its origin and impact. The event was not of the political or financial crisis and the reaction time offered to companies worldwide was very little. In addition, the very premise of the event being a health and safety-related issue, affected the auditing industry at 2 levels, formal aspects and informal aspects. The formal aspects include the documented aspects such as policies, planned executions and fieldwork whereas informal aspects include communication with the team as well as clients.

As a result, digitalization and cloud adoption have taken a front seat in the enterprise plans and strategies. Driven by the demand for remote work and the need for scalable and cost-effective infrastructure, cloud spending rose by 37% to 29 billion in the first quarter of 2020(2). Most of this change came from shifting workloads to the cloud or by purchase of new web applications. Furthermore, the most important and long-lasting changes to the It environment have been an increase in remote working and a change of consumers to remote interaction channels(3).

In terms of enterprise applications what happened was the literal shift from



The above trend in digital spending across different sectors and industries led to a massive shift to cloud and third-party service providers.

2.3. The effect on IT audit

The effect of the Covid 19 crisis has had two-level effects on the enterprise applications, first the and to a lower extent, the change in policies, standards and guidelines concerning the third-party applications, and secondly to a larger extent the move to cloud-based infrastructure.

2.3.1. Third-party application audit

Numerous organizations opted for the use of third party applications which brought in additional considerations in terms of audit scenario. This change is more or less related to the adoption of applications such as unified communication and collaboration tools. Some of the prominent inclusions that need to be considered for third party application are,

- Vendor access-
  - System administrator functions performed by the vendor
  - Vendor's ability to alter user IDs and data
  - Vendor intervention in emergency and exception events
- Vendor procedures-
  - Audit trail of vendor activities
  - Use of work-related devices and their authorization
- System administration and Segregation of Duties
  - Use of formalized procedures for user access requests
  - Non-use of group IDs or shared IDs
  - Password management and revoking rights
- Single sign-on-
  - IP restriction on vendor applications
  - Exposure of sensitive data to home devices and mobile devices
  - Strong audit trails
  - Purchasing entities control over controls on software
  - Accidental and intentional exposure of data to threats

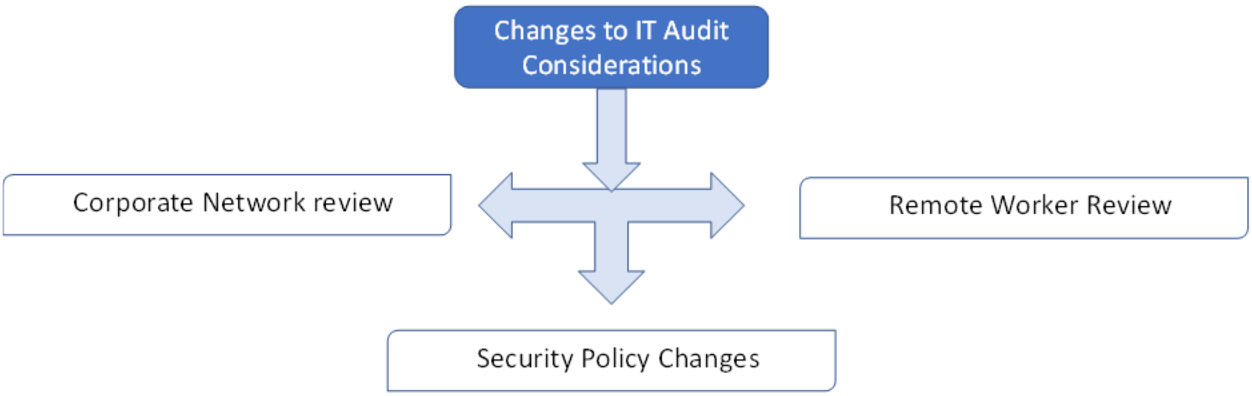
2.3.2. Remote work and use of cloud infrastructure

A larger extent of the pandemic is evident in the use of cloud infrastructure which has brought in need of additional controls and changes to companies' IT environments. The first and foremost being the change in the policies that govern the functioning of IT systems and defining procedures to safely access data and applications through remote access. A prevalent form of providing remote access to employees is through provisioning of Virtual Private Networks (VPN) wherein public telecommunication infrastructure is used to provide secure access to the work environment. VPN provides an isolated tunnel for the company infrastructure and internal networks and hence needs additional authentication. Another important aspect of remote work is the use of virtual desktop capabilities wherein systems connect to a special software system and upon authentication connect to internal servers. Furthermore, additional options such as file transfer software, session sharing tools and third party services are also available and widely in use.

Remote working conditions have increased the vulnerability of the IT environments as home networks and sometimes the use of authorized devices are easy prey to hackers. However large and small companies alike have to comply with SOC2 activities to ensure the integrity of services. Some of the key changes to IT audit consideration due to remote work include,

Audit areas	Changes to consider
Security	AICPA trust services criteria have to be met including confidentiality privacy and security
Risk Assessment	Identifying the gaps to existing risk assessment in this novel environment and changes to security controls to mitigate them
Encrypted hard drives	Any switch to remote work should also include the use of encrypted hardware including laptops smartphones and mobiles
Two-factor authentication	Verification and authorization of users based 2FA especially for the email accounts and file sharing
Remote work policy	Changes to organization IT security policies and cybersecurity requirements and its communication to employees

At a deeper level changes to the IT environment are necessary to exhibit at three different levels including

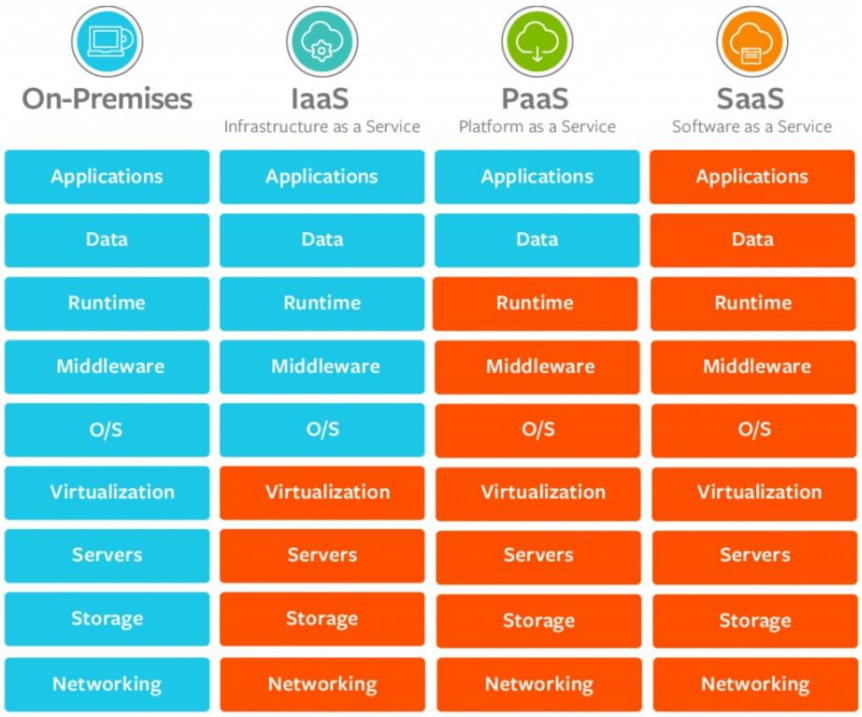


While the changes to policy or network and remote user environments are dependent on the enterprise application, the level of access to users and the sensitivity of data, some certain checks and controls can be evaluated in a remote work environment.

IT audit changes	Domains
Security policy changes	Updated software and patches Revival of training regarding cybersecurity practices Limiting the use of work equipment to work activities (Acceptable use policy) Establishing procedures for IT security incidents and mitigation (BYOD policy and remote working policy update) Changes to IT strategic plan
Corporate network changes	Firewall configuration changes External penetration testing Remote access security review Securing remote connections such as VPN and RDP Mobile device management solution usage Logging and monitoring of network Remote user access approvals and procedures Remote tool inventory
Remote worker IT environmental changes	Change in system requirements including, Password, multi-factor authentication, encryption And antivirus System hardening for computing and networking devices External vulnerability assessments Secure connection or secure WiFi Data backups and storage restrictions Host IPS and Network IPS usage Patch management software usage

3. Platform as a Service (PaaS) Cloud Migration

Platforms as a service remove the need for organizations to manage the underlying infrastructure, usually, hardware and operating systems, database, networking, files, compute, virtualization & DevOps platform, and allow you to focus on the deployment and management of your applications. This helps you be more efficient as you don't need to worry about resource procurement, capacity planning, software maintenance, patching, or any of the other undifferentiated heavy lifting involved in running your application.



3.1. **Advantages of Migrating to Cloud (PaaS)**

By delivering infrastructure as a service, PaaS offers the same advantages as IaaS. But its additional features—middleware, development tools, and other business tools—give you more advantages:

Cut coding time. PaaS development tools can cut the time it takes to code new apps with pre-coded application components built into the platform, such as workflow, directory services, security features, search, and so on.

Add development capabilities without adding staff. Platform as a Service components can give your development team new capabilities without your needing to add staff having the required skills.

Develop for multiple platforms—including mobile—more easily. Some service providers give you development options for multiple platforms, such as computers, mobile devices, and browsers making cross-platform apps quicker and easier to develop.

Use sophisticated tools affordably. A pay-as-you-go model makes it possible for individuals or organizations to use sophisticated development software and business intelligence and analytics tools that they could not afford to purchase outright.

Support geographically distributed development teams. Because the development environment is accessed over the Internet, development teams can work together on projects even when team members are in remote locations.

Efficiently manage the application lifecycle. PaaS provides all of the capabilities that you need to support the complete web application lifecycle: building, testing, deploying, managing, and updating within the same integrated environment.

3.2. During Pandemic Implementation of PaaS (Public/Private Cloud & On-Prem Infrastructure) :

During the pandemic, which started in 2019, the cloud migration ensured many benefits over the On-Prem infrastructure.

Pros:

- Reduced maintenance
- Reduced Human effort
- Reduced expense of acquiring Infrastructure
- Current Industry-standard level infrastructure & policy maintenance
- SLA to ensure availability & business continuity.
- Risk transfer to CSP (Cloud Service Provider)
- Disaster recovery, Incidence management & business continuity assurance provided by CSP
- Flexibility for change management, allowing alteration or up-gradation in IT infrastructure, at no additional expense for acquiring IT infrastructure
- Existing infrastructure continues to add value to the organization

Cons:

- Integration to the CSP's services, could be a challenge based on the current IT infrastructure and that provided by the CSP.
- Contractual obligations
- Reduced control over hardware
- Increased dependency on Internet Service provider.
- Software, Middleware, OS & Hardware compatibility
- Data Import cost
- RBAC has to be defined and managed extensively by the organization
- Data Migration

Commonly used Frameworks by CSPs

- HIPPA HITRUST 9.2
- ISO 27001, NIST SP 800 - 53 R3
- NIST SP 800 - 171 R2
- PCI-DSS v3.2.1
- SWIFT CSP-CSCF

3.3. Concerns:

- What are the various applications employees permitted to access from their devices?
- Ensuring do and don'ts for personal devices and organizations involved in checking every security aspect with a BYOD device security policy.
- Asserting responsibilities for personal device owner apropos to level of access of sensitive data and assets.
- Granting access to the right personnel on cloud and on-prem resources.
- Ensuring employees that work remotely connect via secure networks.
- Enforcing endpoint protection policies or software in place to protect personal devices.
- Presence of security controls such as SSL certificates for authentication of personal devices, remote wiping for potential theft of devices.

3.4. Process Controls:

- Prevent confidential and sensitive corporate data ending up on devices of unidentified security clearances of the organization.
- Authenticate employees for device access through a WiFi infrastructure that includes implementing a VPN, network monitoring and access management to check who owns each BYOD device on an allowed network.
- Administering guidelines for cross-device compatibility i.e Windows, Mac, Linux platforms through proper policies, encryption rules and other rules specific to operating systems.
- Setting up a system to archive logs including Windows logs, Firewall logs, Email server logs, Active Directory logs to track login attempts and authentications.

3.5. Suggested Measures for BYOD:

- Implement a system that monitors employee’s internet traffic and GPS location of all BYOD devices.
- Adopting pertinent security solutions that can provide service through controlling applications, user access, networks and devices, data encryption, that ensures enterprise security in the BYOD landscape.
- Establish a security component where the organization executes guidelines to encrypt data for the entire data lifecycle i.e in-transit and at-rest. This safeguards data in case of a security breach.
- Companies should mandate appropriate measures, procedures, protocols for identifying and enforcing policies related to the evaluation of the risks associated with BYOD devices that access company data for verifying the installation of security solutions on all devices accessing company data and budgetary allocation should be made based on resources implemented.
- Aligning the company’s Acceptable Use Policy(AUP) with BYOD policies

3.6. Controls Pre-Pandemic:

- Tracking the employee's IP address was a common way to authenticate within geographical limitations that needed extra controls such as location-based service (LBS), WiFi positioning system (WiPS) to ensure data security.
- Pre-pandemic companies avoided BYOD due to increased security risks across devices that may not comply with the same controls as corporate assets and needed to look over security updates and patches for BYOD devices separately on a case by case basis.
- Remote network connections made it difficult to function with Endpoint Detection and Response (EDR) tools, Anti-virus while sending system logs to a central server for collection and monitoring.
- For corporate security operations centres (SOC), the budgetary risk to secure IT infrastructure to acquire advanced threat-intelligence upgrades, behavioural analytics to combat social engineered cyber threats.

3.7. Controls Post-Pandemic:

- More emphasis on remote access anomalies because of the need to track the employee from a variety of networks from multiple locations.
- Shift to cloud products post-pandemic has impacted IT Service Management to constantly monitor on-premise end-point and network logs that will be stored directly in the cloud server.
- Remote employees are subject to phishing attacks, malware, virus centred around the theme of the pandemic.
- New normal has mandated frequent auditing of company IT assets that include network, workstation, and remote device patch and update management over virtual private networks (VPNs) with increased database load.
- Need for review and revision of business continuity and disaster recovery policies suitable to potential pandemic-type events.

3.8. Service Level Agreement SLA

3.8.1. Typical SLA's provided by Public CSP

- Active Directory (AD): 99.99% The service is able to process user sign-up, sign-in, profile editing, password reset and multi-factor authentication requests. Developers are able to create, read, write and delete entries in the directory.
  At least 99.9% of Active Directory Domain Services requests for domain authentication of user accounts belonging to the Managed Domain, LDAP bind to the root DSE, or DNS lookup of records will complete successfully.
- API Management Service instances running in the various tier deployments scaled within a single region will respond to requests to perform operations at least 99.95% of the time, in the best tier category.

- Each Application Gateway Cloud Service having two or more medium or larger instances, or deployments capable of supporting autoscale or zone redundancy, will be available at least 99.95% of the time
- At least 99.9% availability of the Automation DSC agent service
- Virtual Machines that have two or more instances deployed in the same Availability Set,
- Virtual Machine Connectivity to at least one instance at least 99.95% of the time
- At least 99.9% availability of Azure DevOps Services for paid DevOps Services users
- Firewall will be available at least 99.95% of the time, when deployed within a single Availability Zone & at least 99.99% of the time, when deployed within two or more Availability Zones in the same region.
- At least 99.99% of the time Front Door will respond to client requests and deliver the requested content without error.
- At least 99.9% availability of the backup and restore the functionality of the Azure Backup service.
  99.9% of the time the Bot Service will successfully receive and respond to REST API calls to the Channels API Endpoint.
- Connectivity to the Cache Endpoint at least 99.9% of the time.
- At least 99.9% of the time CDN will respond to client requests and deliver the requested content without error.
- At least one role instance will have Role Instance Connectivity at least 99.95% of the time.
- At least 99.9% of the time successfully process requests to perform Data Share API operations will happen.
- At least 99.9% availability for all databases & related services.
- DDoS Protection Service will be available at least 99.99% of the time.

3.9. Controls in Hybrid PaaS – as per SOC 2:

While migrating to the cloud have its pros and cons, control ownership of some important controls transfer to shared or entirely owned by either the CSP or the CSC(Cloud Service Consumer).

3.9.1. Following are some important controls:

Audit and Assurance Policy and Procedures - Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.
Ownership of the Control: Shared between CSP & CSC

Independent Assessments - Conduct an independent audit and assurance assessments according to relevant standards at least annually.

Ownership of the Control: Shared between CSP & CSC

Risk-Based Planning Assessment - Perform independent audit and assurance assessments according to risk-based plans and policies.
Ownership of the Control: Shared between CSP & CSC

Requirements Compliance - Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.
Ownership of the Control: Shared between CSP & CSC

Audit Management Process - Define and implement an Audit Management process to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence.
Ownership of the Control: Shared between CSP & CSC

Remediation - Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, review and report remediation status to relevant stakeholders.
Ownership of the Control: Shared between CSP & CSC

Application and Interface Security (AIS)

Ownership of Control: Shared between CSP & CSC	**Ownership of Control: CSP**
• Business Continuity Management Policy and Procedures • Risk Assessment and Impact Analysis • Business Continuity Strategy • Business Continuity Planning • Documentation • Business Continuity Exercises • Communication • Backup	• Disaster Response Plan • Response Plan Exercise • Equipment Redundancy

Change Control and Configuration Management

- Change Management Policy and Procedures
- Quality Testing
- Change Management Technology
- Unauthorized Change Protection
- Change Agreements
- Change Management Baseline
- Detection of Baseline Deviation
- Exception Management
- Change Restoration

Ownership of the Control: Shared between CSP & CSC

Cryptography, Encryption and Key Management

Encryption and Key Management Policy and Procedures	CSC Key Management Capability
CEK Roles and Responsibilities	Encryption and Key Management Audit
Data Encryption	Key Generation
Encryption Algorithm	Key Purpose
Encryption Change Management	Key Rotation
Encryption Change Cost Benefit Analysis	Key Revocation
Key Archival	Key Destruction
Key Compromise	Key Activation
Key Recovery	Key Suspension
Key Inventory Management	Key Deactivation

Ownership of the Control: Shared between CSP & CSC

Governance, Risk and Compliance

- Governance Program Policy and Procedures
- Risk Management Program
- Organizational Policy Reviews
- Policy Exception Process
- Information Security Program
- Governance Responsibility Model
- Information System Regulatory Mapping

Ownership of the Control: Shared between CSP & CSC

- Special Interest Groups

Ownership of the Control: CSP

Data Security and Privacy Lifecycle Management

Ownership of Control: Shared between CSP & CSC	Ownership of Control: CSC
• Security and Privacy Policy and Procedures • Data Classification • Data Flow Documentation • Data Ownership and Stewardship • Data Protection by Design and Default • Data Protection Impact Assessment • Sensitive Data Transfer • Personal Data Access, Reversal, Rectification and Deletion • Limitation of Purpose in Personal Data Processing • Personal Data Sub-processing • Disclosure of Data Sub-processors • Limitation of Production Data Use • Data Retention and Deletion • Sensitive Data Protection • Disclosure Notification • Data Location	• Secure Disposal • Data Inventory • Data Protection by Design and Default

Identity and Access Management

Ownership of Control: Shared between CSP & CSC

Identity and Access Management Policy and Procedures	Segregation of Privileged Access Roles
• Strong Password Policy and Procedures	• Management of Privileged Access Roles
• Identity Inventory	• CSCs Approval for Agreed Privileged Access Roles
• Separation of Duties	• Safeguard Logs Integrity
• Least Privilege	• Uniquely Identifiable Users
• User Access Provisioning	• Strong Authentication
• User Access Changes and Revocation	• Passwords Management
• User Access Review	• Authorization Mechanisms

Security Incident Management, E-Discovery, and Cloud Forensics

- Security Incident Management Policy and Procedures
- Service Management Policy and Procedures
- Incident Response Plans
- Incident Response Testing
- Incident Response Metrics
- Event Triage Processes
- Security Breach Notification
- Points of Contact Maintenance

Ownership of Control: Shared between CSP & CSC

Logging and Monitoring

Ownership of Control: Shared between CSP & CSC	Ownership of Control: CSP
• Logging and Monitoring Policy and Procedures • Audit Logs Protection • Security Monitoring and Alerting • Audit Logs Access and Accountability • Audit Logs Monitoring and Response • Logging Scope • Log Records • Log Protection • Encryption Monitoring and Reporting • Transaction/Activity Logging • Failures and Anomalies Reporting	• Clock Synchronization • Access Control Logs

Infrastructure and Virtualization Security

- Infrastructure and Virtualization Security Policy and Procedures
- Capacity and Resource Planning
- Network Security
- OS Hardening and Base Controls
- Production and Non-Production Environments
- Segmentation and Segregation
- Network Architecture Documentation
- Network Defense

Ownership of Control: Shared between CSP & CSC

- Migration to Cloud Environments

Ownership of Control: CSP

CONCLUSION AND FUTURE WORK:

The information Technology scenario has changed drastically since the pandemic began. Hence, it has had a lasting effect on the IT audit landscape including different aspects such as device security, cybersecurity, productivity tools, as well as cloud security. The biggest risk when it comes to home devices usage is data security. While working from home, despite having the data within the organization's premises and having top-end security mechanisms in place, many companies fall prey to cyberattacks. Since most businesses have moved online due to pandemic, almost all business meetings (via Zoom, Webex etc), transactions happen online leading to seemingly increased data security risk due to hacking, malware threats and data leakage.

Post-Pandemic the requirement to working remotely became a necessity instead of a choice. The benefit of moving into cloud are significant for an organization with major underlying infrastructure. The move to cloud enables shifting control ownership to the the CSP, which also allows for a transfer of Risk. This further improves the risk appetite of the organization, while reducing the fixed cost associated with IT Infrastructure purchase & maintenance.

We have discussed how we can mitigate these risks with the changes due to online-only workflows and how companies can better secure their IT infrastructure. We have discussed the risks of BYOD and what tools, technologies must be used to mitigate these risks. In addition, we have analysed the changes in the IT environment with respect to the enterprise applications and its possible migration to cloud in coming years. While the scope of this paper only scraps the surface of the changes in IT audit due to pandemic much work needs to be done to identify the newborn risks and the associated challenges for the audit community. With this paper we have tried to establish a foundation for the audit community to start and base their individual in-depth audits.

REFERENCES:

Ali, M. I., Kaur, S., Khamparia, A., Gupta, D., Kumar, S., Khanna, A., & Al-Turjman, F. (2020). Security Challenges and Cyber Forensic Ecosystem in IoT Driven BYOD Environment. *IEEE Access, 8*, 172770-172782. doi:10.1109/access.2020.3024784

Anant, V., Caso, J., & Schwarz, A. (2020, November 06). COVID-19 crisis shifts cybersecurity priorities and budgets. Retrieved from https://www.mckinsey.com/business-functions/risk/our-insights/covid-19-crisis-shifts-cybersecurity-priorities-and-budgets#

Chang, S., Yen, D. C., Chang, I., & Jan, D. (2014). Internal control framework for a compliant ERP system. *Information & Management, 51*(2), 187-205. doi:10.1016/j.im.2013.11.002

Albitar, K., Gerged, A. M., Kikhia, H., & Hussainey, K. (2020). Auditing in times of social distancing: The effect of COVID-19 on auditing quality. *International Journal of Accounting & Information Management, 29*(1), 169-178. doi:10.1108/ijaim-08-2020-0128

Ritchey, D. (2020, June 1). How COVID-19 has Transformed InfoSec. *Security Magazine*.

Hughes, J. R., & Beer, R. (n.d.). A Security Checklist for ERP Implementations. *EDUCAUSE Quarterly*.

Barlette, Y., Jaouen, A., & Baillette, P. (2021). Bring Your Own Device (BYOD) as reversed IT adoption: Insights into managers' coping strategies. *International Journal of Information Management, 56*, 102212. doi:10.1016/j.ijinfomgt.2020.102212

Vorakulpipat, C., Sirapaisan, S., Rattanalerdnusorn, E., & Savangsuk, V. (2017). A Policy-Based Framework for Preserving Confidentiality in BYOD Environments: A Review of Information Security Perspectives. *Security and Communication Networks*, *2017*, 1-11. doi:10.1155/2017/2057260

29, A., 19, A., 11, M., & 9, M. (2021, May 11). IT auditing and controls: A look at application controls [updated 2021]. Retrieved from https://resources.infosecinstitute.com/topic/it-auditing-and-controls-a-look-at-application-controls/

Service Level Agreements Summary. (2021). Microsoft Azure. https://azure.microsoft.com/en-us/support/legal/sla/summary/

Private Cloud vs Public Cloud vs Hybrid Cloud - Which is best? (2019, September 24). Retrieved from https://vianalabs.com/private-cloud-vs-public-cloud-vs-hybrid-cloud-which-is-best/

Types of cloud computing. (2021). Amazon Web Services, Inc. https://aws.amazon.com/types-of-cloud-computing/

What is PaaS? *Platform as a Service*. (2021). Microsoft Azure. https://azure.microsoft.com/en-us/overview/what-is-paas/

Martin, K. (2019, May 1). Access Controls Over Third-Party Applications. *ISACA Journal*, *3*(2019).

10, U. O. (2020, March 10). COVID-19: Keeping Auditing & Compliance on Track with Remote Working. Retrieved from https://www.ispartnersllc.com/blog/coronavirus-covid-19-remote-auditing-compliance/

Remote Work Security Assessment. (n.d.). Retrieved from https://sbscyber.com/auditing/remote-work-security-assessment

Mariia, N., & Viktoriia, M. (2020). Digitalization Of Audit In The Conditions Of The Covid-19. *Herald of Kyiv National University of Trade and Economics*, *131*(3), 123-134. doi:10.31617/visnik.knute.2020(131)09

Checklist: Virtualizing Your Employees' Offices. (2021, January 08). Retrieved from https://dgtechllc.com/checklist-virtualizing-your-employees-offices/

BYOD security: What are the risks and how can they be mitigated? (2020, September 26). Retrieved from https://www.comparitech.com/blog/information-security/byod-security-risks/

16, U. O. (2020, May 16). Overcoming Cybersecurity Challenges to the WFH SOC. Retrieved from https://www.ispartnersllc.com/blog/wfh-soc-audits-cybersecurity/

Rajendran, S. (2019, May 1). Three Ideas for Cybersecurity Risk Management. *ISACA Journal*, *3*(2019). Retrieved from https://www.isaca.org/resources/isaca-journal/issues/2019/volume-3/three-ideas-for-cybersecurity-risk-management.

Singleton, T. W. (2012, January 1). Auditing Applications, Part 1. *ISACA Journal*. Retrieved from https://www.isaca.org/resources/isaca-journal/past-issues/2012/auditing-applications-part-1.

B. R., Shubhamangala., & Saha, S. (2016, March 1). Application Security Risk: Assessment and Modeling. *ISACA Journal*, *2*(2016).

Contributor. (2020, January 20). Three ways to achieve data security whilst enabling BYOD. Retrieved from https://securitybrief.com.au/story/three-ways-to-achieve-data-security-whilst-enabling-byod

Mareco, D. (2020, January 27). Top 10 BYOD Policy Considerations and Best Practices. Retrieved from https://www.securedgenetworks.com/blog/top-10-byod-policy-considerations-and-best-practices

Ogden, J. V. (n.d.). The 7 Scariest BYOD Security Risks (and How to Mitigate Them!). Retrieved from https://www.cimcor.com/blog/7-scariest-byod-security-risks-how-to-mitigate

Author Cedric Nabe Impact of COVID-19 on Cybersecurity. Retrieved from https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html