Remote Auditing in Times of Crisis: Cybersecurity Strategies and Best Practices for Small Audit Firms

Archana Narayanan
School of Computer Science
University of Guelph
Email: anaray02@uoguelph.ca

Bassam Abdulkhalek
School of Computer Science
University of Guelph
Email: abdulkhb@uoguelph.ca

July, 2024

Abstract

The COVID-19 pandemic led to an instant alteration of the audit approach to remote performance—directly affecting small audit firms. This paper analyzes how such cybersecurity challenges translate into best practices for carrying out audits from a remote location during a crisis. Key issues include how small audit firms have been reacting to data integrity challenges, the transition toward work-from-home arrangements, and data security threats. The findings indicate that small firms face barriers such as lack of knowledge, inadequate resources, and increased cyber threats. Effective remote auditing calls for robust digitalization, training, and collaboration, accompanied by comprehensive cybersecurity measures like VPN, multi-factor authentication, and encryption. This study calls for a low-cost best practice that needs to be established and customized for small audit firms to minimize cybersecurity risks and ensure secure and trustworthy processes.

The COVID-19 pandemic revolutionized the paradigm of financial audits, forcing most audit firms to become virtual instantaneously. Small-scale audit firms, already vulnerable and under-resourced, encountered severe adversities in this transition. As verification of accounts and inventories was conducted remotely, new protocols for accessing clients' systems to ensure data veracity became imperative. Unexpected reliance on electronic tools and remote access greatly increased cyber threats, from unauthorized intrusions to data breaches and compromised data integrity. Some studies have shown that barriers to implementing effective cybersecurity practices include inadequate knowledge, overestimation of cost, and underestimation of threat levels. A successful remote audit requires additional tools, such as laptops and a workable data management system for effective communication. Furthermore, communication, collaboration, and organizational culture are necessary for effective auditing. Literature suggests that small businesses do not have the skills and resources to implement these practices effectively, making them prone to cyber threats.

This paper provides a comprehensive analysis of the cybersecurity challenges and best practices for small audit firms in conducting remote audits. It examines the transition to remote work, specific cybersecurity threats, and develops personalized, cost-effective strategies to enhance small audit firms' cyber posture. Lastly, it reassures the integrity and security of remote auditing processes, enabling small firms to operate resiliently and confidently during crises.

Keywords: remote auditing, cybersecurity strategies, cybersecurity solutions, small audit firms, COVID-19, best practices, cost-effective

1 Introduction

The COVID-19 pandemic dramatically transformed the landscape of financial auditing, compelling many audit firms to transition to remote operations almost overnight. The majority of firms globally still find it difficult to comprehend and manage emerging cyber threats in an increasingly intricate digital environment [1]. For small audit firms, this shift posed unique challenges exacerbated by limited resources and pre-existing vulnerabilities. As auditors adapted to verifying accounts and inventories remotely, new protocols for accessing client systems and ensuring data veracity without physical presence became imperative [2]. This sudden reliance on digital tools and remote access heightened cybersecurity risks, exposing small firms to threats such as unauthorized access, data breaches, and compromised data integrity [3]. During the COVID-19 pandemic, there was a sudden spike in hacking attempts through phishing emails [4].

The literature indicates that small businesses, including audit firms, often lack the necessary expertise and resources to implement robust cybersecurity practices effectively. Studies highlight barriers such as insufficient knowledge, misconceptions about threat levels, and cost constraints [5]. Because of the increased cybersecurity risks associated with teleworking, auditors must have additional equipment, including laptops and reliable data management systems to enable effective communication [1]. Add to this the pandemic-induced remote work environment introduced additional complexities, including maintaining communication, collaboration, and organizational culture which are critical for effective auditing [2].

This literature review aims to give in-depth information related to the cyber challenges and best practices for small audit firms performing remote audits. Against this background, this paper will seek to empower small audit firms with the right tools to boost their cybersecurity postures by analyzing the shift towards working from home, pointing out particular threats in cybersecurity, and developing customized but cost-effective strategies. Ultimately, this paper wishes to provide a way that ensure small firms can face such crises with confidence and resilience by protecting the integrity and security of their remote auditing processes. These include themes such as the digitalization of audit activities, cybersecurity threats to a remote work environment, and best practices for conducting a remote audit. The review is oriented at making an input to the ongoing debate in remote auditing and cybersecurity as well as at giving insights and practical advice to small auditing companies.

The subsequent sections will delve into the detailed findings from various studies exploring themes such as the digitalization of audit activities, cybersecurity threats in remote work environments, and the development of best practices for remote auditing. Through this review, we aim to contribute to the ongoing discourse on remote auditing and cybersecurity, providing valuable insights and practical recommendations for small audit firms.

2 Research Methodology

2.1 Research Questions

Based on the objectives of the project, the following research questions have been formulated to guide the literature review:

1. How have small audit firms adapted their auditing practices in response to the COVID-19 pandemic, particularly in moving towards remote work?
   This question aims to elicit the change and adaptation taken by small audit firms in their

audit practices due to the pandemic, including the use of digital tools and protocols for remote verification of accounts and inventories.

2. What are the specific cybersecurity threats to small audit firms while performing remote audits?
   This research question aims to identify the type of cybersecurity challenge experienced by small audit firms while conducting audits remotely, such as vulnerabilities related to VPN access, risks of unauthorized access, and issues associated with maintaining the integrity and confidentiality of data.

3. What might be considered best practices in remote auditing that demonstrate a level of concern for cybersecurity yet be cost-effective and practical for a small audit firm to implement?
   This research question will generate a set of best practices that small audit firms can apply in improving cybersecurity while conducting remote audits. The main focus is to devise strategies that would be effective and at the same time economically feasible for small firms.

2.2 Approach

This literature review follows a qualitative approach by embracing ideas from existing literature based on the challenges of cybersecurity and best practices of remote auditing in small audit firms amidst crisis periods such as the COVID-19 pandemic experience. This means we will refer more to peer-reviewed articles and industry reports for a more comprehensive grasp of what it entails.

2.3 Data Collection

The key steps followed in the data collection process are discussed below:

2.3.1 Literature Search

The sources included books and scholarly articles which were searched from academic databases such as Google Scholar, JSTOR, and IEEE Xplore. Keywords used in the quest for papers highly relevant to small audit firms include "remote auditing", "cybersecurity strategies", "cybersecurity solutions", "small audit firms", "COVID-19", "best practices", "cost-effective".

2.3.2 Selection Criteria

The articles selected were based on their relevance to the research topic; thus, studies covered and commented on the transition into remote auditing, the cybersecurity challenges encountered, and best practices that could be adapted for small firms.

2.3.3 Publication date

Preference was given to articles published within the last five years so the most updated research findings and developments could be included.

2.3.4 Inclusion and Exclusion Criteria

- **Inclusion Criteria:** Peer-reviewed journal articles, conference papers, industry reports, and case studies that discuss remote auditing, cybersecurity challenges, and best practices for small audit firms.

- **Exclusion Criteria:** Articles that do not specifically address the intersection of remote auditing and cybersecurity, those that focus exclusively on large firms or non-audit-related contexts, and non-English papers.

2.4 Data Analysis

In analyzing data, the following steps were employed:

1. **Thematic Analysis:** We read thoroughly selected articles and coded them to derive patterns and recurrent themes. Some of the major themes are the consequences of digitalization on remote auditing, specific cybersecurity threats, and possible best practices recommended.
2. **Synthesize the Findings:** We thus integrated the findings from the thematic analysis into a coherent storyline. It consisted of comparisons and contrasts among several studies, the differences underlying common challenges, and the identification of consensus on best practices.
3. **Critical Evaluation:** All the studies were critically evaluated based on methodological rigor, relevance, and contribution toward elucidating the topic under focus. This evaluation helped establish the gaps in the existing literature and areas for further research.

2.5 Validity and Reliability

In this literature review, we implemented Validity and Reliability through:

- **Multiple Sources:** The review included multiple sources of evidence, including peer-reviewed articles and industry reports to provide a balanced and comprehensive perspective.
- **Cross-Verification:** Findings were cross-verified with multiple studies to ensure consistency and accuracy.
- **Transparent Criteria:** The selection and analysis criteria were clearly defined and consistently applied to minimize bias and enhance the credibility of the review.

2.6 Limitations

While the literature review in this paper is helpful, it is still constrained by the following limitations:

- **Scope of the literature review:** The review is limited to available literature and this might not capture all emerging trends and recent developments in remote auditing and cybersecurity.
- **Focus on small audit firms:** Findings from the study may not be generalized to the more prominent firms or other industries as the study focuses more on small audit firms.
- **Rapidly Evolving Field:** Cybersecurity is a rapidly changing environment; new threats and solutions may have come up that have not been covered in this review.

3 Literature Review

To overcome this increased risk of cybersecurity threats, micro and small audit firms need to break through some significant barriers such as being concerned about costs, misconceptions about the severity of threats and lack of security awareness. These firms, having the weakest defenses due to limited resources, are even more exposed to data integrity risks related to unauthorized access and data breaches. The literature shows that small audit firms face constraints based on cost, underestimation of threat levels, and inadequate knowledge. Small and micro-enterprises often run on very meager budgets, and the idea of making huge investments into cybersecurity may feel burdensome. For example, even basic cybersecurity tools such as antivirus software or firewalls or having secure communication channels for these organizations are expensive. This resource constraint often results in their dependence on archaic systems and minimal security, thus leaving them even more exposed.

- **Resource Scarcity:** Organizations that are larger can ramp up their cybersecurity more quickly—a step that small firms find hard to implement given the budget and staff scarcities. This is further accentuated by the additional risks posed by working from a remote location. Home networks, in many cases less secure than corporate ones, reveal more vulnerabilities that small business owners may have overlooked.

- **Implications of Remote Work:** COVID-19 has caused a huge shift towards remote work and raised the stakes for security. The literature shows that frequent increases in cyber attacks translated into successful cyber attacks. Some of the specific problems related to issues in data management, poor endpoint protection, and inadequate access management, which called for the immediate development of a comprehensive cybersecurity strategy in line with the needs and limitations of small audit firms.

- **Incident Response Plan:** Small audit firms usually have neither an incident response plan nor a continuous monitoring system, hence being poorly prepared for dealing with and responding to cyber incidents. In addition, individually owned work devices without secure remote working policies pose higher risks of unauthorized access and data breach.

- **Risks Associated with Compliance:** Compliance risks arise when business interests become more significant than cybersecurity, leading to the compromise on audit data credibility. The studies reveal that lack of cybersecurity awareness and training makes small audit firms prone to cyber-attacks.

Addressing these challenges requires a multifaceted approach:

- **Development of Formal Security Policies:** There must be some formal security policies along with incident response plans in place. Organization policies should define protocols on how to work remotely in a secure way, personal device use, and how to back up data with the recovery procedure. These are two areas where small and micro audit firms can increase their strength in cybersecurity resilience and better protect themselves from dynamic threat environments.

- **Small Firm Scalable and Cost-effective Security Solution:** Seek security solutions for small, cost-effective firms that can scale with the firm while at the same time offering protection against the threats faced by large enterprises without requiring a significant amount of on-premises infrastructure.

- **Managed Security Services Adoption:** Small firms should take advantage of third-party managed security services, which will provide professional cybersecurity measures without the need for heavy internal investment. Managed services can offer continuous monitoring, incident response, and regular security assessments tailored to the firm's specific needs.
- **More Effective Awareness and Cybersecurity Training:** Investment in end-to-end awareness training regarding cybersecurity can be a solution for small audit firms to improve their security stance. Continuous training sessions may enhance the awareness of phishing, social engineering attacks, and safe remote working practices.

4 Findings

- **Budget Constraints and Scaling up:** Literature has shown that poor decision-making by approval authorities, in combination with budget limitations, seriously hampers digitalization for small companies [2]. In practice, the firms rarely have the required resources and expertise to build an effective cybersecurity environment. This leaves them significantly exposed to cyber risks [5]. In this context, small audit firms find it challenging to scale remote audits just like their larger counterparts due to a lack of requisite solutions and processes involved in conducting secure remote audits [6]. This is further exasperated by the absence of critical processes in the detection of cyber risks—those of continuous monitoring and formal incident response plans [7].
- **Operationalizing a Security Culture Framework:** Designing a Security Cultrure framework is crucial for an organisation. This involves in the need for designing and institutionalizing cybersecurity so that all employees feel that cybersecurity is of value [8].
- **Remote Access Hygiene:** Remote working policies are largely missing leading to dismal remote access hygiene [9]. Organizations must therefore strategize VPN licensing so that this facilitates safe and constant remote access [4]. Systems, when left unconfigured, lead to ad-hoc change and, due to this fact, exposes the companies to a high risk of data breach [10].
- **Perception of Cybersecurity Checks:** Auditors in small firms do not consider the checks of cybersecurity as part of their work; therefore, they become victims of cyber-attacks. According to the literature, it must come with an attitude or perception change whereby auditors realize cybersecurity forms part of the inclusions in their job [9].
- **Common Issues:** Common issues run from issuing new devices without security controls to ignoring new technology and neglecting the risks that are already in existence. For example, a small firm does issue laptops to their employees without them being loaded with important security software; therefore, these laptops are surely exposed to any kind of vulnerability and impending cyber-attacks [10].
- **Risk to Personal Devices:** Using personal devices for work involves quite significant risks, as it is quite possible that a firm does not control proprietary information located on non-secured devices of auditors. This brings out the aspect of very strict personal device usage policies [6].
- **Security Awareness:** Users' susceptibility to attacks increases as users with no security awareness get subjected to phishing and social engineering, which naturally leads to unauthorized access. Indeed, it is very common that foes steal data and demand a ransom; therefore, backup and data recovery need to be part of the game [7].

- **Relating to the Literature Review:** The findings closely resonate with the literature review, which outlined the main challenges and, laid insights into the risk that small audit firms face. Issues outlined fall in line: resource constraints, impacts of remote work, and need for formal security policies discussed in the literature review.

5 Discussion

5.1 Cybersecurity Solutions Plan

These small audit firms need three essential components in place for conducting secure remote audits: Security Governance, Technology and Infrastructure, Security awareness. These act as a bridge for small audit firms to perform Secure Remote auditing (See Figure 1).

- **Security Governance:** This comprises seven domains: Strategic planning, Access management, Asset management, Security operations, Data backup and recovery, and Incident response planning. This dimension focuses on directing efforts to safeguard the firm from cyber-attacks and non-compliance issues.
- **Technology and Infrastructure:** This includes the domain of Endpoint Security which concentrates on protecting endpoints from adversaries.
- **Security Awareness:** This emphasizes user education, ensuring adherence to Security best practices in the workplace.

A toolkit is designed to encompass all three phases of an audit—before, during, and after the remote audit—integrating cybersecurity measures. The toolkit contains Cost-effective tools, Controls checklist and Security Awareness.

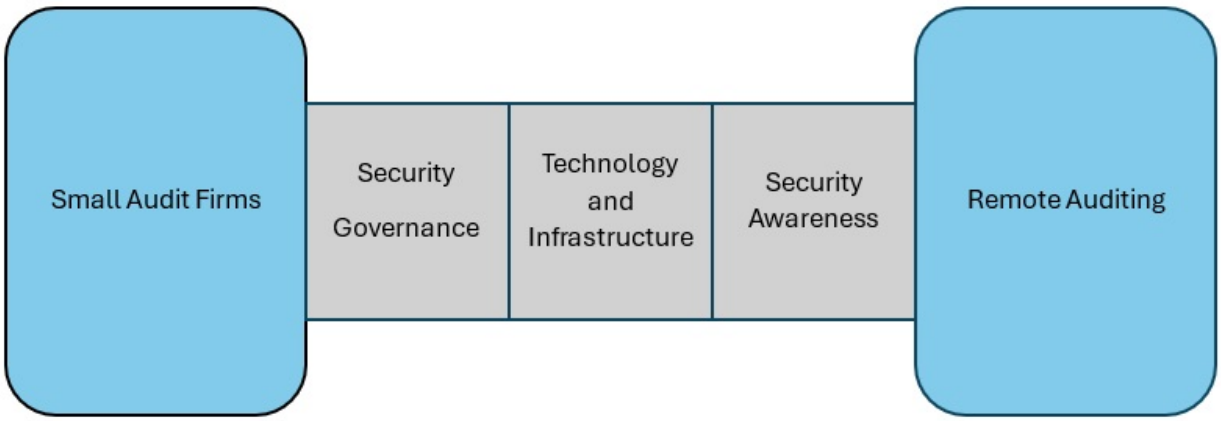

Figure 1: Cybersecurity Solutions plan

5.2 Best Practices for Remote Auditing

The literature addressing these cybersecurity challenges presents various best practices suitable for small audit firms. These highlight good value for money and feasibility:

- **Digital Tools and Protocols:** Employ digital tools and protocols to support remote auditing through secure document-sharing platforms and video conferencing tools for remote interviews and meetings [11].
- **Cybersecurity Measures:** Implement strong cybersecurity measures including Virtual Private Networks (VPNs), multi-factor authentication, encryption of sensitive data, firewalls, intrusion detection systems, and endpoint protection software.
- **Training and Awareness:** Conduct regular training and awareness campaigns for staff to ensure they follow cybersecurity protocols and stay informed of emerging threats.
- **Penetration Testing and Vulnerability Assessments:** Perform regular penetration testing and vulnerability assessments to detect and fix potential threats.
- **Collaboration and Knowledge Sharing:** Encourage collaboration and knowledge sharing within the firm and externally to enhance cybersecurity practices. This includes co-sourcing and utilizing internal audit staffing pools to address skills shortages.
- **Framework:** Organizations need relevant frameworks and procedures to implement information security measures alongside digital technology advancements [7]. This includes developing a foundation that integrates essential cybersecurity elements [8].
- **Cost-Effective Solutions:** Open-source cybersecurity tools, although complex and requiring technical know-how, offer a less expensive alternative to costly commercial solutions [12].

5.3 Toolkit Guide

To enable small audit firms to access these resources, we have prepared a holistic toolkit guide presented in three prominent files:

- **Cost-Effective Tools Guide File:** This file lists cost-effective cybersecurity tools suitable for small audit firms, elaborating on implementation details and application of tools such as open-source VPNs, encryption software, and endpoint protection solutions. This document is meant to assist small businesses in establishing a robust cybersecurity control environment economically (Refer to Appendix A).
- **Controls Checklist:** This checklist furnishes a structured way to ensure all relevant cybersecurity controls are applied, including access management, data protection, and periodic security assessments. Organizations can use the checklist to ensure they follow best practices in cybersecurity and regulatory compliance (Refer to Appendix B).
- **Cybersecurity Awareness:** Appendix C designed to sensitize auditors to their roles concerning cybersecurity during remote audits. It provides practical guidance on using tools safely, managing passwords, identifying phishing attacks, and securely managing company devices. This section can be used to create the presentation slides as part of Security awareness training that needs to be provided to auditors(Refer to Appendix C).

5.4 How to Use the Toolkit Guide?

- **Step 1:** Use the Controls checklist to ensure all the minimal controls mentioned are in place.

- **Step 2:** Select the best tool selection approach for your organization using the options mentioned in the cost-effective tools guide.
- **Step 3:** Install cost-effective tools on all auditors' systems. Use free AI tools like ChatGPT and Gemini for step-by-step installation guidance.
- **Step 4:** Ensure the tools are working smoothly.
- **Step 5:** Preplan the remote audit and inform the auditee well in advance to have the same collaborative tools in their system.
- **Step 6:** Train auditors with security awareness to make them follow security best practices at work.

6 Tips for Future Studies

- **Human Factors:** Investigate the impact of training, awareness, and organizational culture on cybersecurity and the effectiveness of remote auditing practices.
- **Cost-Benefit Analysis:** Conduct a cost-benefit analysis of various cybersecurity tools and practices to identify the most effective and cost-efficient solutions for firms of different sizes. This will inform decision-making on cybersecurity investments.
- **Case Studies and Real-World Applications:** Develop detailed case studies and real-world applications of remote auditing and cybersecurity practices to provide practical insights and lessons learned, bridging the gap between theoretical research and practical implementation.
- **Regulatory and Policy Implications:** Future research should consider the regulatory and policy implications of remote auditing and cybersecurity. Understanding how regulation influences implementation and effectiveness is essential for creating supportive legal frameworks.
- **Impact on Audit Quality and Outcomes:** Research the impact of remote auditing and cybersecurity measures on audit quality and outcomes, including accuracy, reliability, and timeliness.

7 Conclusion

The onset of the pandemic necessitated a shift to remote auditing, posing significant challenges for small audit firms. This literature review reveals a critical need for these firms to adapt their audit practices and incorporate robust cybersecurity measures to safeguard sensitive information while working remotely. Virtual tools and protocols, while enhancing work potential, introduce complexities in managing communication, collaboration, and organizational culture.

Identified cybersecurity challenges—such as VPN access vulnerabilities, unauthorized access risks, and data confidentiality and integrity issues—underscore the need for comprehensive cybersecurity strategies. Small audit firms, constrained by expertise and resources, are especially vulnerable to cyber threats but can benefit significantly from adopting best practices tailored to their needs.

The toolkit guide, including cost-effective tools, a controls checklist, and a cybersecurity awareness presentation, provides small audit firms with practical guidance to manage cyber risks and

deliver high-quality remote auditing services. This transition, while challenging, also offers opportunities for innovation and improvement. Continued adaptation and vigilance regarding evolving cyber threats and maintaining high audit quality standards are essential.

Future research should expand to include studies on larger firms and explore the long-term effects of remote auditing and cybersecurity practices. By identifying effective and customized solutions, researchers can further support small audit firms in their journey toward secure and resilient remote auditing practices.

8 Appendices

8.1 Appendix A:

Approach 1: Unified Solution
Approach 2: Combination/Specialized Solution
Approach 1 is a primary solution to the risks noted and integrates various security features such as firewall, VPN, antivirus, and web filtering.
Approach 2 is multiple cost-effective solutions to the risks noted.

Checklist/Questions	Approach
Size of the organization less than 10 members	2
Having less time for the remote audit	1
Profit of the organization is less than 20% of the capital	2
Have employees who focus more on audit and less on security	1
Keen on cost-cutting even though the size of the organization is more than 10 employees	2

Table 1: Approach Selection Criteria

Example:
For a small business of around 10 employees, using a combination of the above solutions might look like this:

- Firewall: Sophos XG Firewall ($300 initial cost).
- MDM: Scalefusion ($2 x 10 devices x 12 months = $240 annually).
- Endpoint Protection: Bitdefender GravityZone ($29.99 x 10 = $300 annually).
- Patch Management: Automox ($3 x 10 devices x 12 months = $360 annually).

Total estimated annual cost: $1,200 - $1,500 (depending on the specific models and subscriptions chosen).
Note:
Palo Alto's Prisma Access or Next-Gen Firewall solutions can offer all-in-one security, but they are typically more expensive, especially for small businesses. Costs can easily exceed $10,000 annually depending on the configuration and service level. These approaches are better compared to adopting managed security services which might cost $40,000 annually as the minimal cost. The cost outweigh the benefits in these cases and hence, approach 2 is recommended.

S.No	Risks	Mitigation	Recommended Tools	Cost Involved Analysis
1.0	Data Exfiltration	i) Full disk encryption along with an endpoint detection system. ii) Latest critical patches updates. iii) Proper configuration of software. iv) Use Virtual Private Network (VPN). v) Mobile Device Management (MDM) solutions to ensure devices are secure. vi) Secure collaboration tools. vii) Secure Access management. viii) End point security. ix) Secure file sharing cloud drives.	i) Disk Encryption: Microsoft BitLocker for Windows. ii) ManageEngine Patch Manager Plus - Security updates. iii) Windows Defender Antivirus (Microsoft Defender). iv) NordVPN, Surfshark, and Private Internet Access (PIA). v) Miradore, Jamf Now (iOS). vi) Microsoft Teams. vii) Duo Security by Cisco, Auth 0 - Multi-factor authentication. viii) Bitdefender, Crowdstrike - Endpoint protection. ix) OneDrive	i) Disk Encryption software BitLocker and Filevault are included with Windows and macOS, respectively. ii) ManageEngine patch manager - $245 for 50 computers. iii) Antivirus Windows Defender and Malware bytes - $39.99 per year. iv) Subscription cost of $2 to $4 per month for VPN services. v) Miradore - $3 per device per month, Jamf Now - $2 per device per month. vi) Users might have Microsoft packages being used already. vii) MFA- 1-10 Users Duo is free. viii) Bitdefender: 30 dollars per year per device. Crowdstrike: 60 dollars per year per device. ix) It comes with Microsoft 365 Family or $99 per year.
2.0	No Incident Management and Continuous monitoring	Security Incident and event management	LogRhythm NextGen SIEM, ManageEngine Log360	ManageEngine Log 360 up to 25 desktops and 25 servers - $595 per year
3.0	Reduced/No IT and Security Support Staff	Hybrid approach - Troubleshoot on own for basic issues and escalate severe issues.	Refer to YouTube videos or OpenAI tools to troubleshoot basic issues	-

Continued on next page

S.No	Risks	Mitigation	Recommended Tools	Cost Involved Analysis
4.0	Spike in hacking attempts: Emails containing infected documents with malware. - Impersonation and trick IT staff to gain network access. - Offer codes to proliferate the spread of malware. - Phishing attacks to exfiltrate key information.	Awareness campaign	Several Security Awareness YouTube videos are available and the main points focussing on the Auditor's responsibilities is outlined in Appendix C	-

Table 2:Cost effective tools

8.2 Appendix B:

Dimension	Domain	Focus Areas	Controls	Yes	No
Security Governance	Strategic Planning	Digitalisation	Invest in Cost effective Cybersecurity solutions as per the toolkit.		
		Scaling up	Partner with vendors offering flexible and scalable Cybersecurity services.		
			Implement secure and efficient remote auditing tools.		

Security Governance	Strategic Planning	Resiliency	Implement Second remote access system for administrators to access critical internal systems in the event that the primary remote access systems are taken offline.		
	Access Management	Identity and Access Management	Assign Admin/Approval authority to approve access to company system/application/database.		
			Create individual user access ID to login to application/database.		
			Assign a user to monitor only authorized users have access to company data and remove any user no longer require access.		
			Perform access log reviews in a monthly or quarterly basis.		
			Enforce two factor or multi factor authentication for access.		
		Privilege User Access Management	Utilize password vaults or other techniques to guarantee that administrative accounts can be employed securely.		
			Examine super users/privileged users for limitations and sufficient backups.		
	Asset Management	Asset Reviews/Updates	Assign a user or admin to collect the company issued devices from user's leaving the organisation and have a track of assets with its ID, model, data.		
	Security Operations	Secure Remote Audit Guidelines	Publish a guide to all users to conduct remote audits securely.		
		Security Operations Centers (SOCs)	Assign a user to ensure timely detection and response to security incidents.		
		Security Policy Reviews	Perform regular assessments and updates of security policies.		
		Risk assessment/Privacy impact assessment	Conduct regular risk assessments and data privacy assessments.		
			Document assessment findings and action plans.		
		Security Culture framework	Provide a checklist to users to prepare for secure remote audit.		
		Revisiting risks / Continuous monitoring	Assign a user to perform continuous monitoring to revisit the risks identified in a regular basis (Ex: half yearly).		
	Data backup & recovery	DR Testing and Support	Develop and maintain a comprehensive Disaster recovery plan.		

Security Governance	Incident response plan	Incident Response and Management	Develop and maintain a comprehensive incident response plan.		
Technology & Infrastructure	Endpoint Security	Secure channel	Install a high secure VPN		
			Ensure VPN Software and firmware up to date		
			Implement Twofactor or multifactor authentication for VPN access		
		Endpoint protection software	Install and maintain up-to-date antivirus and antimalware software		
			Schedule regular scans and ensure real-time protection is enabled		
		Cloud Solutions	Implement strict access controls and MFA for cloud services		
			Encrypt data at rest and in transit		
		Patching	Assign an admin or user to enable automatic updates for operating systems and applications		
			If automatic updates not available, train users to check for and apply critical patches at least monthly		
		Configuration	Assign an approval authority to approve the changes to avoid misconfiguration.		
			Admin/user to follow basic hardening guides for their systems (e.g., disable unnecessary services)		
		Encryption	Use full disk encryption on laptops and mobile devices.		
		Firewalls & Antivirus	Set both firewall and antivirus software to update automatically.		
			Check firewall is properly configured to block unauthorized access.		
		Regular software update	Enable automatic updates for all software		
			Manually check for updates for critical applications monthly.		
		Secure Email communication	Use email services that offer end-to-end encryption.		
			Implement multi-factor authentication for email accounts.		
			Enable advanced spam and phishing filters		
		Mobile device management	Use MDM software to manage and secure mobile devices		
			Enable remote wipe capabilities for lost or stolen devices.		

Technology & Infrastructure	Endpoint Security	Secure collaboration tools	Use multi-factor authentication for access to collaboration tools.		
		Intrusion Detection system (IDS)	Implement an IDS solution and assign a user/admin to regularly review IDS alerts		
		Intrusion Prevention system (IPS)	Implement an IPS solution and assign a user/admin to regularly review IPS alerts		
		Security logs monitoring	Set a schedule to review logs weekly and configure alerts for critical events.		
		Penetration testing	Assign a user to perform basic pen testing to identify vulnerabilities.		
		Data integrity solutions	Implement checksums or hashes to verify data integrity.		
			Regularly back up audit data.		
			Implement strict access controls.		
Security Awareness	Security Awareness	User Awareness	Conduct user awareness training session as provided in the toolkit and maintain the log of completion.		

Table 3: Controls Checklist

8.3 Appendix C:

Auditor's Responsibilities

- Perform basic security checks as it's your role too.
- Keep strong passwords and do not share your passwords with anyone.
- Implement another authentication method like a one-time password in addition to your password.
- Manually check for critical software updates including firewalls and antivirus.
- Avoid sharing client data in messaging tools or on your personal device.
- Using internet resources, for basic issues, troubleshoot on your own.
- Do not bypass any security controls.
- Daily or weekly back up your work in the centralized cloud solution.
- Conduct virtual walkthroughs and inspections to improve audit quality evidence.
- Be aware of phishing emails and do not click on baits.

Let's rely on trusted sources and do not open mail links or attachments from unknown sources. Virus or malware downloaded can lead to unauthorized access and data breaches.

- Handling your asset: While handling your company-issued device, ensure to:
  - Keep it safe from theft.

  - Lock the system when not at work.
  - Connect to only secure Wi-Fi.
  - Do not insert USB or external hard drives – use cloud solutions and secure channels for data transfer.

- If using your approved personal device (Bring Your Own Device - BYOD) for work, please follow all the mentioned endpoint controls for your personal device as well.

References

[1] R. Florea and R. Florea, "Implications of covid-19 crisis on risk management, audit and controls activities," 2021, george Bacovia University, Bacau, ROMANIA. [Online]. Available: https://www.proquest.com/openview/acd9ee0016b873e6d7314322a56c079a/1?pq-origsite=gscholar&cbl=266695

[2] N. Farcane, O. C. Bunget, R. Blidisel, A. C. Dumitrescu, D. Deliu, O. Bogdan, and V. Burca, "Auditors' perceptions on work adaptability in remote audit: a covid-19 perspective:," 2022. [Online]. Available: https://doi.org/10.1080/1331677X.2022.2077789

[3] N. A. Rakha, "Ensuring cyber-security in remote workforce: Legal implications and international best practices," 2023. [Online]. Available: https://pdfs.semanticscholar.org/793e/d8585d083690f159bda79181622afdd99a0a.pdf

[4] pwc, "Embracing the new normal," 2020. [Online]. Available: https://www.pwc.com/jg/en/issues/covid-19/cyber-security-challenges-during-the-covid-19.pdf

[5] A. Cartwright, E. Cartwright, and E. S. Edun, "Cascading information on best practice: Cyber security risk management in uk micro and small businesses and the role of it companies," 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404823001980

[6] M. Bispham, S. Creese, W. H. Dutton, P. Esteve-Gonzalez, and M. Goldsmith, "Cybersecurity in working from home: An exploratory study," 2020. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3897380

[7] K. Nazarova, M. Nezhyva, T. Metil, V. Hordopolov, L. Prystupa, and O. Moyseyenko, "Digital information security: Corona-crisis impact on the accountants, business analysts and auditors training," 2021. [Online]. Available: https://doi.org/10.21744/lingcure.v5nS4.1854

[8] A. Georgiadou, S. Mouzakitis, and D. Askounis, "Designing a cyber-security culture assessment survey targeting critical infrastructures during covid-19 crisis," 2021. [Online]. Available: https://www.researchgate.net/publication/349107129_Designing_a_Cyber-security_Culture_Assessment_Survey_Targeting_Critical_Infrastructures_During_Covid-19_Crisis

[9] EY, "Cyber security resilience and response throughout covid 19 pandemic," 2020. [Online]. Available: https://assets.ey.com/content/dam/ey-sites/ey-com/en_ie/topics/cybersecurity/ey-covid-19-cyber-impact-assessment.pdf

[10] pwc, "Managing the impact of covid-19 on cyber security," March 2020. [Online]. Available: https://www.pwc.com/jg/en/issues/covid-19/managing-impact-of-covid-19-on-cyber-security.pdf

[11] D. Koerniawati, "The remote and agile auditing: A fraud prevention effort to navigate the audit process in the covid-19 pandemic," 2021. [Online]. Available: https://www.researchgate.net/publication/356636873_THE_REMOTE_AND_AGILE_AUDITING_A_FRAUD_PREVENTION_EFFORT_TO_NAVIGATE_THE_AUDIT_PROCESS_IN_THE_COVID-19_PANDEMIC

[12] O. Almatari, S. Mazen, I. M. Helal, and S. Elhennawy, "Cybersecurity tools for is auditing," 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8588282