reviewed paper

Security and Compliance in Cloud Environments

Anmol Kumar, Christoph Sandbrink

(BA Anmol Kumar, University of Applied Management Studies Mannheim, anmol.kumar@stud.hdwm.org)
(Prof. Dr.rer.pol. Christoph Sandbrink, University of Applied Management Studies Mannheim, christoph.sandbrink@hdwm.org)

1 ABSTRACT

Security and resilience of smart city infrastructures and operations is one of today's most relevant and challenged topics of smart city agendas in times of increasing cyber attacts and ubiquitous digital networks and data driven processes in all aspects of smart city planning and operations. Cloud environments play today and increasingly tomorrow a central role in smart city's IT architectures and infrastructures.

According to the reviewed literature on the subject of cloud and security, the main gap or problem is that while cloud provides a number of advantages and benefits, it also presents risks and challenges for businesses and organizations (Vacca, 2021).

The key challenge is the risk associated with the user privileged accesses. It centers on the problem of inappropriate access control, which can lead to data leakage and unauthorized access of stored information, disruption, and compliance difficulties (Tamunobarafiri, et al., 2019).

Further, it is observed during that one of the biggest challenges to all concepts related to cloud, security and compliance is monitoring and ineffective incident response, which is essential for maintaining security in cloud and hybrid environments (Cybellium Ltd, 2023). It is important that organizations ensure that they establish a clear, well-structured incident response plan and conduct regular security testing internally, or with support from third-party vendors (Bruinsma, 2023).

In addition, the lack of thorough and practical approaches to resource scalability and cost optimization is one of the major research gaps in the field of cloud computing. Companies seek solutions that are capable of handling the whole range of resource scalability and cost optimization challenges, with regard to maintaining security and compliance, as current options are frequently inconsistent and fragmented (Verma, Cherkasova, & Campbell, 2011; Zhang, Cheng, & Boutaba, 2010; Calheiros, Ranjan, Beloglazov, DeRose, & Buyya, 2011).

Finally, raising awareness and educating stakeholders and staff about the security protocols and cloud governance framework is another crucial challenge. Having training sessions, documentations, and establishing clear communication guidelines are important for organizations with the sole aim of reducing the security-related risks (Spair, 2023; Munir, Al-Mutairi, & Mohammed, 2015).

The research objectives of this thesis revolve around some critical issues within the sphere of security and compliance in cloud and hybrid environment. The study aims to comprehensively shed light on the implications of excessive global administrative rights within organizations, investigating the potential risks and vulnerabilities associated with such practices. It also seeks to identify effective approaches for achieving a robust alignment between incident response and monitoring mechanisms, ensuring a proactive and coordinated approach to security threats. Additionally, the research will recommend strategies to enhance stability and optimize costs in context of information security, addressing the challenges that organizations face while maintaining security measures. Lastly, the study will explore the factors that impact the effectiveness of security training programs, providing awareness into how smart city administration and other organizations can better prepare their staff and workforce to mitigate security and compliance risks.

Keywords: smart city, governance, compliance, security, cloud

2 RESEARCH DESIGN

To address the central research question, how risks and challenges for businesses and organizations, could be mitigated and controlled, a set of research objectives as well as related resarrch questions arised.

To address the questions, accomplish the research goals, and fill in the research gaps, a qualitative research design will be used in this study. Because the study's subject matter is delicate and complicated, requiring a high degree of accuracy, dependability, and user satisfaction, the qualitative design approach is the most appropriate choice. By encouraging respondents to elaborate on their responses and better understand their requirements and expectations to close the gaps in the areas linked to security and compliance in cloud and

hybrid environments of a business, a qualitative research analysis will help foster openness. Content analysis will be the analytical technique used. Interviews will be used to gather data, which will then be conceptually analyzed, recorded, and transcribed. Qualitative research designs are typically grounded on people's lived experiences and conducted in natural settings. To finish the paper and comprehend the needs, this strategy is crucial. Nonetheless, the data's ability to be broadly used is limited by the research methodology (Marshall & Roassman, 2016).

Sr. No.	Research Objectives	Research Questions
1	Investigate the implications of excessive global admin privileges	What are the key challenges and benefits of implementing standardized security controls?
2	Identify approaches for achieving a robust alignment of response and monitoring	What are the critical factors in achieving a robust response and monitoring alignment?
3	Propose strategies for efficient resource stability and cost optimization	How can organizations achieve resource scalability and cost optimization while maintaining security and compliance in cloud environments?
4	Explore the factors influencing the effectiveness of security training programs	How can training programs be enhanced to improve employee understanding of security risks and best practices in cloud and hybrid environments?

3 LITERATURE REVIEW

3.1 Identity and Access Management

3.1.1 Challenges of implementing standardized security controls

Establishing standard security controls, protocols and procedures may be a challenging endeavour for companies, which frequently face a slew of obstacles. One key difficulty for numerous companies is a lack of awareness of security hazards. Given their lack of knowledge, companies struggle with the assessment of security measures that are the most significant and corresponding execution. They may not protect themselves adequately from new and developing threats because of an absence of understanding and awareness of the hazards and risks, which could end up in security threats and breaches (Rob S., 2023). The next obstacle is insufficient availability of resources. Setting up and upholding adequate security measures may be laborious and costly. This could pose an important issue for businesses with limited funds, causing it to be hard for them to set up proper safety protocols (Taylor, et al., 2013; Kumar, et al., 2016). Human error leads to basic problems with standardized safety protocols in Cloud systems. Despite advances in technology, humans remain a vital element of safety measures, and human errors can introduce shortcomings (Probst, et al., 2010; Kaspersky daily, 2023). In conclusion, in the modern digital age, everything is becoming more difficult. This amount of detail makes it difficult for business entities to set up and oversee security solutions. With a lot to keep track of, it can be challenging to keep these security measures operating properly. Dealing with and maintaining the health of these complex computer systems requires an enormous amount of effort in order to remain ahead of emerging issues and keep things secure (Weill & Ross, 2004; Amirani, 2020).

3.1.2 Benefits of implementing standardized security controls

Standardized security measures are ever more crucial in the changing world of computing in the cloud for companies wanting to secure sensitive information, meet with regulatory responsibilities, and achieve their business objectives. Standardized security standards offer an extensive and coordinated method for protecting the cloud while reducing the chance of data breaches, unconstitutional access, and other security concerns (Mather, et al., 2009). As a result, by getting data and maintaining compliance with legal and regulatory requirements, uniform security measures render it easier to comply with data protection laws like

the GDPR (Walters & Novak, 2021). Furthermore, consistent security rules reduce the burden of IT employees by simplifying security employment opportunities, tasks, and operations. They can help businesses in lowering the monetary effects of security breaches, thus reducing the impact of incidents of security and operating costs (Boudreaux, et al., 2020). Finally, standardized security control solutions demonstrate an organization's ongoing dedication to data safety, trust, and reputation amongst consumers and business partners (Merkow, 2022).

3.2 Incident Response and Monitoring

3.2.1 Importance of effective incident management and monitoring

Regarding incident management and monitoring, a cloud-based environment presents a distinctive array of challenges as well as opportunities. As cloud services become increasingly utilized, organizations face a more diversified threat landscape and higher cybersecurity concerns. Furthermore, as to the dispersed nature of cloud infrastructure, an integrated Prompt learning and response to problems is critical for mitigating their impact on company activities. Effective incident management procedures help businesses in swiftly detecting threats, setting priorities, and dealing with problems, reducing disruption length and the potential for widespread harm. According to Gartner (2022), “organizations that implement effective incident management practices can reduce downtime by up to 50% and minimize the financial impact of incidents by up to 80%”. Cloud infrastructures are continually being targeted by cyberattacks, demanding sophisticated incident monitoring and response capabilities. Organizations can swiftly identify and react to security breaches by continuously monitoring cloud systems and applications for deviations and anomalies, protecting vital information, and avoiding financial losses (Lord, 2022).

Moreover, incident monitoring offers businesses with valuable insights into the health and effectiveness of their cloud infrastructure. Organizations can prevent system breakdowns while maintaining top performance by proactively tracking data and identifying possible issues and roadblocks, ensuring perfect business operations (IEEE, 2021). The clients, both internal and external, depend on businesses for protection of their data and offer trustworthy offerings. Effective incident management demonstrates the company's dedication to protection and trustworthiness, which promotes customer trust and loyalty (ISACA, 2021).

Finally, maintaining client satisfaction and efficiency necessitates minimizing interruptions, delays, and outages. Effective incident management systems enable companies to resolve issues promptly and efficiently, lowering disruption time and enhancing uptime (Maayan, 2021).

3.2.2 Critical factors that contribute to robust response and monitoring alignment

Evaluating the success of efforts to establish a successful response and monitoring alignment are both essential for ensuring continuous improvement and the general well-being of the IT environment. Key Performance Indicators (KPIs) provide an invaluable structure for analyzing performance and discovering potential areas of improvement and further refinement. The major key performance indicator (KPI) is the percent of downtime avoided. Downtime occurs when a system or application is not available for use by end users. Monitoring the total amount of downtime avoided shows how successfully the IT system and infrastructure protect against service disruptions. This KPI is determined by dividing total downtime by total available time, and the result is shown as a percentage (Kim, et al., 2018; Snyder, et al., 2010). The next key performance indicator (KPI) is system stability. This KPI effectively gauges the system's ability to maintain consistent performance while preventing unforeseen errors or breakdowns. Measuring system stability assists in identifying possible problems that might cause downtime or poor performance (Beyer, et al., 2016; Johnson, 2014). Performance and reliability are further important performance indicators for assessing the alignment of response and monitoring. The speed and effectiveness with which requests and services are handled and offered determines how well a system functions. The ability to maintain the confidentiality of information and regularity of performance is referred to as reliability. Typical performance and reliability metrics include response times that are defined as the length of time it takes a system to respond to a request. The word "throughput" refers to the rate at which data may be processed by a system. Rates of error are calculated as the frequency with which errors or exception happen, and, data corruption rates, often known as the frequency with which data corruption occurs (Allspaw & Robbins, 2010; Limoncelli, et al., 2014).

Finally, Customer Satisfaction is another key performance indicator (KPI) for handling incidents and monitoring. This KPI primarily pertains to the level of satisfaction that users have with a system's

performance and reliability. The KPI is essential because it reflects end-user perceptions of efficacy and reliability, which have a direct impact on total satisfaction. Customer satisfaction consists of every aspect of the user experience, and most importantly, it includes the fact that they feel supported and get a prompt response in case of complaints or problems (Hayes, 2008). By measuring these KPIs, one may acquire some useful insights into the overall health and performance of IT infrastructure. The collected data may be used to identify areas or room for improvements, prioritize resource allocation, and make qualified and data-based decisions to increase the overall monitoring and incident response capabilities of an organization.

3.3 Resource Scalability and Cost Optimization

3.3.1 Resource Scalability Challenges

Efficient resource management in cloud computing is a crucial problem in many organizations; hence, it is important for organizations to address these challenges in an efficient and effective manner.

The most significant obstacle is financial. Uncontrolled resource scaling can lead to increased expenses, therefore good spending management is vital. Consequently, building a price-control system and using technologies can help with cost management and optimization. Furthermore, handling resources leads to both over- and under-provisioning. Over provisioning contributes to an organization's expenditures, whereas under provisioning causes application latency (Erl & Mahmood, 2013; Goodarzy, et al., 2020; Osypanka & Nawrocki, 2022). Following this, resource scaling could restrict performance, reducing both responsiveness and user experience. In simple terms, while operating big applications to increase the availability of cloud resources, scalability may have an impact on the performance of virtual machines (Atchison, 2016; Leite, et al., 2019). Another difficulty is the fact that many companies do not appropriately manage their resources, resulting in waste of resources and inadequate utilization. Furthermore, expecting the need for resources may be problematic for businesses, resulting in over- or under-provisioning (Travieso-Gonzalez, et al., 2023).

Speaking of obstacles, another problem with growing resources is maintaining compliance with regulations in the sector. Establishing right and correct governance standards and verifying that business activities adhere to regulatory requirements can be tough at times (Buyya, et al., 2013). Last but not least, a lack of expertise is another impediment to resource scaling. It is difficult to adequately involve a subject when everyone on the team is unfamiliar with it. Cloud resources require suitable monitoring, and an absence of knowledge may result in insufficient monitoring settings, leading to additional issues (Brown, 2023).

3.3.2 Cost Optimization Strategies

“Cost Management or Optimization of cloud governance focuses on establishing budgets, monitoring cost allocation patterns, and implementing controls to improve cloud spending behaviours across the IT portfolio” (Azure, 2023). As per a report by Deloitte, on an average, organizations save 14% just by moving to Cloud (Deloitte Business Consulting, S.A, 2021). This statistic shows us the importance of cost optimization and why it is of high advantage for companies to implement successful best practices and strategies. Focusing on efficient use of Cloud not only brings security advantages, but also tangible financial benefits. Organizations need to be prepared to profit from this opportunity. Cloud computing cost management is a difficult task. Gartner Research made a framework accessible that explained how to help enterprises. According to this guiding framework, companies must learn how to create budget expectations and forecast or anticipate. They must then have continual access to information about how much clients spend on each program, project, and application. Following this, tracking is set up, businesses must search for methods to reduce their expenses. Expenses can be reduced by using the enhanced capacity to spot deviations and drive remedial efforts. Organizations can gain scalability by automation of their methods for making decisions. To plan, manage, and maximize the use of cloud computing, organizations must develop an assortment of competencies based on this guideline framework. The framework highlights standards of excellence in each of the included components and is relevant regardless of the organization's cloud deployment status. Figure 11 illustrates a number of substitutes for cloud cost management and optimization. It is split into five major sections: Plan, Track, Reduce, Optimize, and Evolve (Gartner Research, 2020; Annis, 2023; Khan, 2020).

3.4 Employee Training and Security Awareness

3.4.1 Significance of security training programs

Security in an organization is not exclusively an IT matter to be handled independently by the IT team. It encompasses everyone with the organization, irrespective of the roles and positions, and employees play a crucial part. Awareness and Training programs for the employees are essential in order to ensure employee engagement, behaviour change, compliance, incident prevention and response, reputation protection, and trust building (Cybellium Ltd, 2023). Employee involvement is boosted by safety awareness activities, which develop an awareness of responsibility and involvement in solid security procedures (Neal & Griffin, 2006). In addition, by addressing psychological concerns and building a culture of high security understanding, it is necessary to make sure that outstanding security training plays a crucial role in encouraging appealing behavioural changes among employees (Ajzen, 1991). Training programs are indispensable for ensuring compliance as they educate employees on regulation and legal requirements, as well as the significance of keeping up to established security standards (Sherif & Sherif, 1964). Plus, security training provides employees with the information and skills required to evaluate and respond to emerging security hazards, which plays a significant role in both incident prevention and successful response (Anderson & Bushman, 2002). The training programs serve protect an organization's image by lowering the likelihood of security breaches and handling the associated negative press (Fombrun, 1996). Finally, security training and awareness fosters faith among stakeholders by demonstrating the company's commitment to protecting both employee and customer or client data, thereby enhancing trust in internal processes (Mayer, et al., 1995). Furthermore, according to a survey conducted by IBM Security, 46% of organizations consider employee training and security awareness as the most common and significant investment (IBM Security, 2023).

3.4.2 Roadblocks to implementing security trainings and raising awareness

In accordance with a survey carried out by Verizon, organizations state that the biggest obstacles in implementing security training and increasing employee awareness include lack of budget (28%), lack of time (35%), lack of management support (17%), lack of employee buy-in (11%) and lack of training resources (11%) (Verizon, 2023). Moreover, these findings are consistent with the findings of, yet another survey conducted by PwC in collaboration with ISACA (Information Systems Audit and Control Association, 2022).

3.4.3 Cultivating a security-aware culture

Although adopting security training and awareness programs provides hurdles and constraints, companies may use some effective methods to get around these obstacles and develop a security-conscious organizational culture in the IT and cloud environments. The first and most critical stage in creating a security-aware culture is to obtain the approval and participation of the organization's management; without their support, the laws and regulations will remain unread and ineffectual. If upper management considers security and security awareness as a serious topic, it will naturally propagate across the organization and contribute to the development of an improved security awareness culture (Gardner & Thomas, 2014; MacKay, 2023). Another way to enhance security awareness is to commence from the beginning. It is needed that the idea of security and related issues be introduced from the very beginning of an employee's life cycle, namely during the period of onboarding. This will not only assist in contributing to the organization’s security, but it will also emphasize how pertinent the subject is to the new employee and, eventually, the entire organization (Executech, 2022; Winkler, 2022). Besides, given today's fast changing cybersecurity and cloud landscapes, organizations need to go beyond typical yearly or biannual security training courses to successfully tackle new vulnerabilities. A more frequent training tempo is necessary, and quarterly seminars or sessions or monthly micro-trainings have shown to be successful solutions for many organizations (Executech, 2022; Harkut & Kasat, 2023). Finally, effective exchange of information is critical for ensuring organizational security. Transparent and open communication channels enable the swift sharing of information with regard to dangers, weaknesses, and incidents, which is key to preventing and responding to security breaches (Spellman, 2018; Cavusoglu, Cavusoglu, & Goldman, 2014).

3.4.4 Measuring training and awareness effectiveness

"Key Performance Indicator (KPI) is a business metric that measures the performance and progress of a business against its key objective. The purpose of using KPIs is to help businesses evaluate success at reaching specific targets." (Oberlo, 2023)

The primary key performance indicator (KPI) for evaluating the achievement of organizational security training programs is the successful completion rate of security awareness training. This indicator represents the percentage of employees who have successfully completed security awareness training. A high rate of completion acts as evidence of active employee participation in the learning process, implying a possibility that they will proactively shield themselves and the business from potential risks (Majewski, 2022).

A further significant KPI is the result of phishing simulations, which defines the percentage of employees who click on phishing links or attachments in simulated IT phishing emails. In this kind of situation, a lower click rate is appealing since it corresponds with achieving the KPI and demonstrates a high level of resilience to phishing attacks (Jampen, et al., 2020). Additionally, the level of security incident reporting rate is a key performance indicator (KPI) that measures the amount of security issues reported to the organization's IT or security teams. A bigger reporting rate indicates that employees are aware of what is going on and appreciate the need of swiftly reporting such instances (Arctic Wolf, 2023). Lastly, simply implementing a training program is not enough; so, a KPI in the form of a security knowledge evaluation score is sought. This score is the median score on a security knowledge evaluation, having an elevated average indicating that employees possess an in-depth understanding and grasp of security best practices (Chapple, et al., 2021).

4 RESEARCH METHODOLOGY

A qualitative research design will be used to respond to the questions, achieve the study's objectives, and fill research gaps. The qualitative design technique is an ideal fit for the study's sensitive and difficult topic, requiring high level of precision, dependability, and user satisfaction. A qualitative research study will create openness through enabling respondents to elaborate on what they have to say and better understand what they want and need in order to overcome gaps in areas related to security and compliance in a business's cloud and hybrid settings. The evaluation of content will be the analytical method applied. Interviews will be conducted to collect data, which will then be thematically examined, recorded, and transcribed. Qualitative research designs typically depend on actual experiences of individuals and done in natural settings (Marshall & Roassman, 2016). The secondary data of the research comes from journal papers, books, websites, and other online sources, while the primary information is obtained through interviews. Qualitative research is analytical in nature and is most effective when a particular issue or gap has not yet been addressed by a specific group of people, or if the subject matter is just emerging (Morse, 1991 in Creswell, 2002). The qualitative analysis will be performed with purposive sample. The material in the sources is structured in a systematic way according to the topics of the sub-sections. Furthermore, semi-structured interviews will be conducted based on the literature review, giving an elevated level of comparison (Creswell, 2002). Appendix 1 comprises of interview guide intended for the purpose of this paper. The interviews were recorded with prior permission of the interviewees for the purpose of transcription compliant with GDPR. This is also essential and advantageous when conducting a more in-depth review of the interviews (Collis & Husset, 2013; Bryman & Bell, 2015).

5 DISCUSSION BETWEEN FINDINGS AND LITERATURE REVIEW

The dissertation's literature review outlines the primary problems that organizations face when implementing standardized security controls (Rob S., 2023; Taylor et al., 2013; Kumar et al., 2016; Probst et al., 2010; Kaspersky Daily, 2023; Weill & Ross, 2004; Amirani, 2020). The participants in the interviews validated these challenges, highlighting: firstly, a lack of awareness regarding security risks (R1; R2; R3); secondly, resource constraints (R1; R2; R4; R6; R7; R9); thirdly, human errors (R3; R4; R5; R7; R8; R9); and finally, the complexity of modern IT systems (R2; R3; R5; R6; R7; R9; R10). Furthermore, the interviews revealed new findings about challenges that were not covered in the literature review, such as the importance of top management and stakeholder support and collaboration (R6; R10), raising employee awareness (R7; R10), and proper planning (R3; R8).

Furthermore, the goal was to understand the primary benefits of applying traditional security procedures. According to the literature review, the results include better security posture, optimal data privacy and

compliance, higher efficiency and cost reduction, and improved trust and reputation (Mather et al., 2009; Walters & Novak, 2021; Boudreaux et al., 2020; Merkow, 2022). These findings are consistent with the viewpoints of the respondents. At the outset, 100% of respondents agreed that implementing standardized security measures greatly improve the company's security posture (R1; R2; R3; R4; R5; R6; R7; R8; R9; R10). Furthermore, 8 out of 10 respondents agree that trust and reputation can be improved (R1, R2, R3, R4, R7, R8, R9, and R10). The empirical evidence backs up the notion that higher efficiency and cost savings are beneficial, as respondents concur (R1; R2; R3; R5; R8; R9). Finally, 30% of respondents agreed on improving data privacy and compliance (R5; R6; R8). Among the key performance indicators for successful response and monitoring alignment highlighted in the literature review (Kim, et al., 2018; Snyder, et al., 2010; Beyer, et al., 2016; Johnson, 2014; Allspaw & Robbins, 2010; Limoncelli, et al., 2014; Hayes, 2008), the respondents aligned with only two: firstly, the percentage of downtime avoided (R1; R2; R3; R4; R6; R7; R9; R10), and secondly, the system stability (R1; R2; R4; R5; R10). In particular, some important conclusions from the literature review that were not represented in the interviews are linked to performance, reliability, and customer satisfaction. In contrast, several empirical results that were lacking from the literature review included incidence rate (R1; R3; R5; R7; R8), reaction time (R5; R6; R7; R10), and successful closure of internal and external audits. Important scalability challenges in a cloud environment, according to the results of the literature review, include cost management, performance challenges, inadequate resource provisioning, compliance and governance, and a lack of expertise (Erl & Mahmood, 2013; Goodarzy, et al., 2020; Osypanka & Nawrocki, 2022; Atchison, 2016; Leite, et al., 2019; Travieso-Gonzalez, et al., 2023; Buyya, et al., 2013; Brown, 2023). The aforementioned challenges are consistent with the perspectives of interviewees in the actual world (R1; R2; R3; R4; R5; R6; R7; R8; R9; R10). The interview findings also highlight other problems associated with resource scalability, especially forecasting (R3). In the midst of a difficulty, effective remedies are required. The literature review proposes a framework for controlling and improving cloud expenses that includes practical tactics such as Plan, Track, Reduce, Optimize, and Evolve (Azure, 2023; Deloitte Business Consulting, S.A, 2021; Gartner Research, 2020; Annis, 2023; Khan, 2020). Undoubtedly, all respondents agree with this structure and have helped define particular procedures or approaches for each component (R1; R2; R3; R4; R5; R6; R7; R8; R9; R10).

Finally, the literature review examines security training programs, outlining the problems, solutions, and critical aspects found while implementing staff training efforts.

Beginning with all of the obstacles outlined in the literature review (Information Systems Audit and Control Association, 2022), the majority have been substantiated by the respondents: firstly, a lack of time (R1; R2; R4; R8); secondly, insufficient budget (R2; R5; R6; R8; R9); thirdly, inadequate management support (R3; R4; R5; R6; R7; R9; R10); fourthly, lack of employee buy-in (R1; R2; R3; R4; R5; R6; R7; R9; R10); and finally, lack of resources (R2; R7; R8). A fresh discovery about challenges, which was not expressly discussed in the literature review, is lack of understanding (R10). In addition, tackling the solutions, the vast majority of challenges established in the literature review (Gardner & Thomas, 2014; MacKay, 2023; Executech, 2022; Winkler, 2022; Executech, 2022; Harkut & Kasat, 2023; Spellman, 2018; Cavusoglu, Cavusoglu, & Goldman, 2014) have been clearly stated by the respondents: involving management (R2; R4; R5; R8; R9; R10), advocating for best practices (R9), integrating security from day one (R3; R4; R7), conducting regular trainings. Respondents did not expressly address the inclusion of various concepts to promote awareness. Furthermore, the interview findings stress on change management (R3), which is not expressly addressed in the literature review.

Ultimately, in the discussion of key performance indicators (KPIs), the literature review highlights four core criteria, the majority of which were also stated by interviewees. These include the completion rate of security awareness training (R4; R6; R8; R10), the outcomes of phishing simulation (R1; R2; R3; R5; R6; R7; R8; R9; R10), the rate of security incident reporting (R3; R4; R6; R9), and the security knowledge evaluation score. The respondents also mention click rate (R1; R2; R7; R8; R10) and time spent on training (R9) as additional KPIs to consider while assessing the success of security training in a business.

6 SUMMARY OF PRESENTATION OF FINDINGS

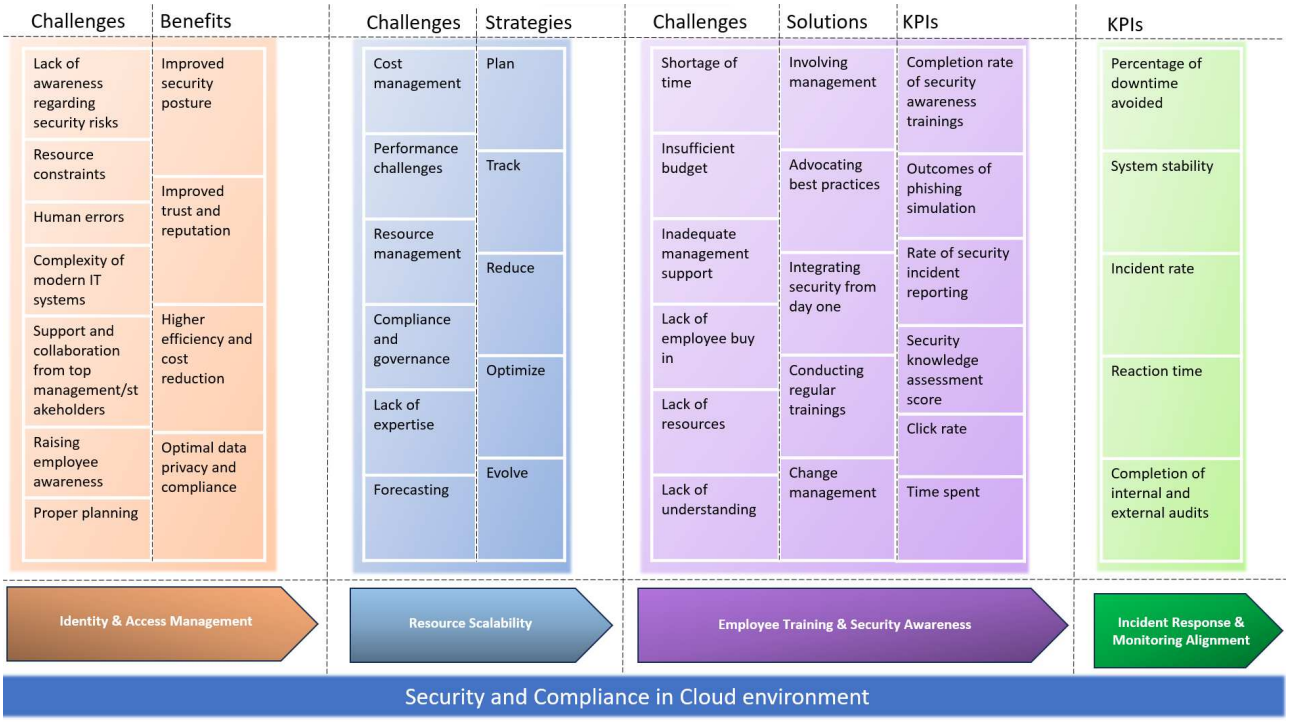
Although the cloud has enormous potential, its implementation requires negotiating a difficult security and compliance landscape. The methodology explained in this chapter is based on interviews with professionals and aims to prepare businesses to better understand the areas.

The focus kicks off with Identity and Access Management, where the key is to strike a balance between granular access limits, user ease, and successfully maintaining privileges using role-based accesses. Implementing this provides organizations with benefits such as great data protection, compliance, and reduced breach risk. The framework aims to provide the possible challenges and benefits in cloud.

Next, we talk about resource scalability. The issue is to maintain strong security despite unforeseeable resource variations while assuring consistent configurations across different scenarios. The section of the framework is aimed at explaining the challenges and practical strategies to successfully scale up or scale down resources in an organization.

Furthermore, the framework covers employee education and security awareness. The goal is to keep employees informed about emerging hazards, foster an awareness culture, and evaluate training performance. Overcoming these hurdles results in lower phishing danger, improved data cleanliness, and proactive reporting of suspicious activities. Ongoing training, simulating phishing attacks, and promoting secure behaviour are critical implementation components.

Lastly, it is equally important to develop a clear incident response strategy. Constant cloud monitoring of resources and computerized security incident management are critical for swift identification and reaction, resulting in less damage, faster resolution times, and a stronger overall security posture. In this regard, the framework explains the main critical factors which are stepping stones for an organization to succeed in the area. The below figure is a visual roadmap that guides businesses through possible risks, mitigation techniques and critical factors for building a strong cloud security and compliance architecture. Security and compliance are ongoing journeys. Embracing this framework as a flexible foundation may evolve as your cloud environment expands.



7 CONCLUSION

As a conclusion a right balance model between compliance and governance at the one hand and openness and degrees of freedom at the other hand, to secure the security and fluent delivery of smart city processes and infrastrcture operations in modern cloud environments.

The constantly changing characteristics of cloud computing demands an attentive approach to security and compliance. The characteristics of cloud computing systems must have a strategy that tackles multiple elements, as mentioned in the introduction of this paper. This encompasses identity and access management, incident response and monitoring, resource scalability, cost optimization, and efficient employee security training. Identity and Access Management (IAM) is essential for enhancing security and compliance in the cloud while establishing the groundwork for managing access to sensitive data. The challenging task of

embracing compatible safety measures in IAM has associated advantages, such as lowered unauthorized access risks and enhanced adherence, which emphasize the need of overcoming the hurdles discussed in the paper. Successful incident response and tracking strengthen the cloud's security posture, pointing out the necessity of proactive oversight in mitigating potential threats. Resource scalability and cost optimization are crucial variables, requiring an accurate compromise between satisfying altering workload requirements while retaining ideal resource allocation. Employee training and awareness programs handle the role of the human aspect of security, and this is imperative for fostering a security-focused mindset.

Combating obstacles to implementation needs to be a team effort to implement security standards into actual actionable processes and procedures. Assessing the efficacy of these initiatives exposes significant details about an organization's security as well as opportunities for advancement. In short, an integrated and comprehensive approach to IAM, incident response, resource management, and knowledge among employees must be implemented for organizations to navigate the complex environment of the cloud securely and successfully.

Following extensive research and 10 interviews with professionals, it emerged that security and compliance in an organization should be of the utmost importance, not just for the long-term advantages it provides, but also for building confidence and reputation in the minds of employees and other internal and external stakeholders. Additionally, it is strongly recommended to start using actual solutions and tools, such as organizing administrator rights on a global level or central level and allocating them to the right people. Furthermore, linking business objectives with real-time threat identification and lightning-fast response times is critical. Also, provided the value of resource scalability and cost optimization, systems such as Hydra, Nerdio Manager for AVD, ControlUp Workspace, among others can be implemented to tackle scalability issues and meet the demands of increasing workloads. Finally, no accomplishment can be achieved without the active participation of employees; thus, employee education and awareness of security related topics are fundamental.

In essence of this paper, an in-depth strategy to cloud security and compliance involves technological advances controls, proactive incident management, cautious spending, and a cyber-conscious mentality. To stay ahead of the curve, organizations have to handle barriers, adopt best practices, and change their strategy on a regular basis. Businesses are able to fully capitalize on the benefits of the cloud as long as they undertake an entire and seamless approach that protects their data, infrastructure, and reputation.

8 REFERENCES

Ajzen, I., 1991. The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), pp. 179-211.

Allspaw, J. & Robbins, J., 2010. Web Operations: Keeping the Data On Time. s.l.:O'Reilly Media, Inc.

Amazon Web Services, Inc., 2023. Cost Optimization with AWS. [Online] Available at: https://aws.amazon.com/aws-cost-management/cost-optimization/ [Accessed 27 December 2023].

American Psychological Associaton, 2017. Ethical Principles of Psychologists and Code of Conduct. [Online] Available at: https://www.apa.org/ethics/code [Accessed 28 November 2023].

Anderson, C. A. & Bushman, B. J., 2002. HUMAN AGGRESSION. Annual review of psychology, pp. 27-51.

Annis, P., 2023. 4 cloud cost optimization strategies with Microsoft Azure. [Online]

Available at: https://azure.microsoft.com/en-us/blog/4-cloud-cost-optimization-strategies-with-microsoft-azure/ [Accessed 05 December 2023].

Antonopoulos, N. & Gillam, L., 2010. Cloud Computing ("The Cloud"). Cloud Computing: Principles, Systems and Applications, pp. 271-272.

Arctic Wolf, 2023. The Value of Security Awareness Training For Your Organization. [Online]

Available at: https://arcticwolf.com/resources/blog/calculating-roi-for-security-awareness-training/ [Accessed 26 November 2023].

Atchison, L., 2016. Architecting for Scale: High Availability for Your Growing Applications. s.l.:O'Reilly UK Ltd..

Atlassian, 2023. Incident management for high-velocity teams. [Online] Available at: https://www.atlassian.com/incident-management/incident-response [Accessed 05 December 2023].

AVI Networks, 2023. Hybrid Cloud. [Online] Available at: https://avinetworks.com/glossary/hybrid-cloud/

Azure, 2023. Get started: Manage cloud costs. [Online] Available at: https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/get-started/manage-costs [Accessed 05 December 2023].

Beyer, B., Jones, C., Petoff, J. & Murphy, N. R., 2016. Site Reliability Engineering: How Google Runs Production Systems. s.l.:O'Reilly Media.

Bhowmik, S., 2017. Cloud Computing. India: Cambridge University Press.

Blackstone, A., 2012. Methods, Principles of Sociological Inquiry: Qualitative and Quantitative. Orono: s.n.

Boudreaux, B. et al., 2020. Data Privacy During Pandemics: A Scorecard Approach for Evaluating the Privacy Implications of COVID-19 Mobile Phone Surveillance Programs. United States: RAND Corporation.

Brand, D., 2018. Why are research questions important? What makes them important?. Twin Cities: University of Minnesota.

British Educational Research Association, 2012. Ethics and Educational Research. [Online] Available at: https://www.bera.ac.uk/publication/ethics-and-educational-research [Accessed 28 November 2023].
Brown, S., 2023. What is Cloud Scalability? Examples, Benefits, and More. [Online] Available at: https://www.strongdm.com/blog/cloud-scalability [Accessed 04 December 2023].
Bruinsma, R., 2023. Azure Cloud Adoption Framework: A Practical Guide for Real-World Implementation. Friesland: Ronald Bruinsma.
Bryman, A. & Bell, E., 2015. Business research methods. s.l.:Oxford University Press.
Buecker, A. et al., 2011. IBM Security Solutions Architecture for Network, Server and Endpoint. United States: IBM Redbooks.
Buyya, R., Vecchoila, C. & Selvi, S. T., 2013. Mastering Cloud Computing: Foundations and Applications Programming. MA: Elsevier Inc..
Calheiros, R. N. et al., 2011. CloudSim: A toolkit for modeling and simulation of cloud computing infrastructures and services. s.l., IEEE, pp. 1-10.
Castagna, R., 2021. information technology (IT). [Online] Available at: https://www.techtarget.com/searchdatacenter/definition/IT
Cavusoglu, H., Cavusoglu, M. & Goldman, A., 2014. An analysis of organizational information security management practices. Journal of Computer Information Systems,, pp. 285-304.
Chapple, M., Stewart, J. M. & Gibson, D., 2021. (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide (Sybex Study Guide). 9th ed. s.l.:Sybex.
Collis, J. & Husset, R., 2013. Business research. 4th ed. Hampshire: Palgrave Macmillan.
Comer, D., 2021. The Cloud Computing Book: The Future of Computing Explained. In: United States: CRC Press, pp. 5-6.
Creswell, J. W., 2002. Match between Problem and Approach. Qualitative, Quantitative, and mixed methods approaches, pp. 23-24.
Crossman, A., 2020. Understanding Purposive Sampling.. [Online] Available at: https://www.thoughtco.com/purposive-sampling-3026727 [Accessed 28 November 2023].
Cybellium Ltd, 2023. Cyber security training for employees. s.l.:Cybellium Ltd.
Cybellium Ltd, 2023. Mastering Cloud Auditing: A Comprehensive Guide to Learn Cloud Auditing. DE: Cybellium Ltd..
Deloitte Business Consulting, S.A, 2021. Cloud Cost Optimization: Unlimited efficiency and flexibility, London: Deloitte Business Consulting, S.A.
Drnevich, P. & Croson, D., 2013. Information Technology and Business-Level Strategy: Toward an Integrated Theoretical Perspective. MIS Quarterly, pp. 483-509.
Erl, T. & Mahmood, Z., 2013. Cloud Computing: Concepts, Technology & Architecture. s.l.:ServiceTech Press.
Executech , 2022. How to Promote Cybersecurity Awareness Month at Your Organization. [Online] Available at: https://www.executech.com/insights/how-to-promote-cybersecurity-awareness-month/
Fombrun, C. J., 1996. Reputation: Realizing value from the corporate image. Harvard: Harvard Business School Press.
Gardner, B. & Thomas, V., 2014. Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats. Netherlands: Elsevier Science.
Gartner Research, 2020. How to Manage and Optimize Costs of Public Cloud IaaS and PaaS. s.l.:Gartner Research.
Gartner, 2022. How to Build an Effective IT Incident Management Process, s.l.: Gartner.
Goodarzy, S. et al., 2020. Resource Management in Cloud Computing Using Machine Learning: A Survey. 19th IEEE International Conference on Machine Learning and Applications (ICMLA), pp. 811-816.
Google Cloud, 2023. What is a Hybrid Cloud?. [Online] Available at: https://cloud.google.com/learn/what-is-hybrid-cloud#section-2
Gupta, D., 2024. The Cloud Computing Journey: Design and Deploy Resilient and Secure Multi-cloud Systems with Practical Guidance. s.l.:Packt Publishing.
Hall, A., 2018. Why are research questions important? What makes them important?. s.l.:s.n.
Hamirani, E., 2020. THE CHALLENGES FOR CYBER SECURITY IN E-COMMERCE. Mumbai, R.K. University.
Harkut, D. G. & Kasat, K. N., 2023. Security Policy & Governance: Forging Resilence. s.l.:Dr. Dinesh G. Harkut.
Hayes, B. E., 2008. Measuring Customer Satisfaction and Loyalty: Survey Design, Use, and Statistical Analysis Methods. Wisconsin: Asq Pr.
Hernández, J. A., Hasayen, A. & Aguado, J., 2019. Cloud Migration Handbook Vol. 1: A Practical Guide to Successful Cloud Adoption and Migration. s.l.:Lulu Publishing Services.
Hurwitz, J. S., Bloor, R., Kaufman, M. & Halper, F., 2010. Cloud Computing For Dummies. Ukraine: Wiley.
IBM Security, 2023. Cost of a Data Breach Report, Michigan: IBM Security.
IBM Security, 2023. Cost of a Data Breach Report 2023, New York: IBM Security.
IBM, 2023. IBM. [Online] Available at: https://www.ibm.com/topics/incident-response [Accessed 05 December 2023].
IEEE, 2021. The Impact of Incident Management on Cloud Infrastructure Security. IEEE.
Information Resources Management Association, 2020. Research Anthology on Artificial Intelligence Applications in Security. United States: IGI Global.
Information Systems Audit and Control Association, 2022. Internal Audit Transformation: A Global Perspective, s.l.: PwC in collaboration with ISACA.
ISACA, 2021. ISACA's CISM Domain 4: Information Security Incident Management. ISACA.
Jampen, D., Gür, G., Sutter, T. & Tellenbach, B., 2020. Don't click: towards an effective anti-phishing training. A comparative literature review. Human-centric Computing and Information Sciences, 10(1).
Jobs.net, 2023. The Three Major IT Functions. The IT Department: What They Do Vs. What Everyone Thinks They Do.
Johnson, L., 2014. Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response. 1st ed. Netherlands: Elsevier Science.
kaspersky daily, 2023. The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within. [Online] Available at: https://www.kaspersky.com/blog/the-human-factor-in-it-security/ [Accessed 28 November 2023].
Khan, O., 2020. Defining roles and responsibilities for cloud cost optimization. [Online] Available at: https://azure.microsoft.com/de-de/blog/defining-roles-and-responsibilities-for-cloud-cost-optimization/ [Accessed 05 December 2023].
Kim, F., 2020. Cybersecurity in the Age of the Cloud. 1st ed. California: SANS Institute.
Kim, G., Behr, K. & Spafford, G., 2018. The Phoenix Project: A Novel About IT, DevOps, and Helping Your Business Win. United States: IT Revolution Press.

Kral, P., 2021. Incident Handler's Handbook. SANS Whitepaper, pp. 1-10.
Kumar, R., Khan, S. & Khan, P. R., 2016. Modern Security Challenges. International Journal of Innovation & Advancement in Computer Science, 5(4), pp. 1-6.
Kumar, R., Raj, H. & Jelciana, 2017. Introduction. Exploring Data Security Issues and Solutions in Cloud Computing, pp. 691-692.
Leite, D. M. et al., 2019. A cloud computing price model based on virtual machine performance degradation. International Journal of Computational Science and Engineering, 18(4), pp. 451-463.
Limoncelli, T. A., Chalup, S. R. & Hogan, C. J., 2014. Practice of Cloud System Administration, The: Designing and Operating Large Distributed Systems, Volume 2: DevOps and SRE Practices for Web Services. Canada: Pearson.
Lord, N., 2022. What is Security Incident Management? The Cybersecurity Incident Management Process, Examples, Best Practices, and More. s.l.:s.n.
Lucas, J. & Moeller, B., 2004. The Effective Incident Response Team. Switzerland: Addison-Wesley.
Maayan, G. D., 2021. Best Practices for Cloud Incident Response. RSA Conference 2024.
MacKay, J., 2023. 10 Ways To Improve Staff Cyber Security Awareness. [Online] Available at: https://www.metacompliance.com/blog/cyber-security-awareness/10-ways-to-improve-staff-cyber-security-awareness
Majewski, M., 2022. Security Awareness Program Builder: Practical guidelines for building your Information Security Awareness Program & prep guide for the Security Awareness and Culture Professional. s.l.:s.n.
Malhotra, M. & Aljawarneh, S., 2017. Critical Research on Scalability and Security Issues in Virtual Cloud Environments. United States: IGI Global.
Manager, I., 2023. Resource Scalability and Cost Optimization [Interview] (20 November 2023).
Marshall, C. & Roassman, G. B., 2016. Designing Qualitative Research. 6th ed. California: SAGE Publications, Inc..
Mather, T., Kumaraswamy, S. & Latif, S., 2009. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. United Kingdom: O'Reilly Media.
Mayer, R. C., Davis, J. H. & Schoorman, D. F., 1995. An integrative model of organizational trust. The Academy of Management Review, pp. 709-234.
Melvin B Greer, J. & Jackson, K. L., 2016. Practical Cloud Security: A Cross-Industry View. United States: CRC Press.
Merkow, M. S., 2022. Practical Security for Agile and DevOps. United States: CRC Press.
Mezzio, S., Stein, M. & Campitelli, V., 2022. Cloud Governance: Basics and Practice. Germany: De Gruyter.
michaels, ross & cole, ltd. (mrc), 2023. Scalability, Reliability, and Cost Savings: The Benefits of Cloud Computing for Software Development. [Online] Available at: https://www.mrc-productivity.com/blog/ [Accessed 27 December 2023].
Microsoft Security, 2023. What is identity and access management (IAM)?. [Online] Available at: https://www.microsoft.com/en-us/security/business/security-101/what-is-identity-access-management-iam
Mishra, A., 2023. Cloud Security Handbook for Architects: Practical Strategies and Solutions for Architecting Enterprise Cloud Security Using SECaaS and DevSecOps. India: Orange Education Pvt Limited.
Munir, K., Al-Mutairi, M. S. & Mohammed, A. A., 2015. Handbook for Research on Security Considerations in Cloud Computing. s.l.:IGI Global.
Natwick, D. & Cuff, S., 2022. Microsoft Security, Compliance, and Identity Fundamentals Exam Ref SC-900: Familiarize Yourself with Security, Identity, and Compliance in Microsoft 365 and Azure. United Kingdom: Packt Publishing.
Neal, A. C. & Griffin, M., 2006. A study of the lagged relationships among safety climate, safety motivation, safety behavior, and accidents at the individual and group levels. Journal of Applied Psychology, pp. 946-953.
Nickel, J., 2016. Mastering Identity and Access Management with Microsoft Azure. United Kingdom: Packt Publishing.
Niranjanamurthy, M., Samuel, R. D. J., Kumar, T. A. & Samuel, T. S. A., 2022. Privacy and Security Challenges in Cloud Computing: A Holistic Approach. United States: CRC Press.
Nord Security, 2023. Nord Security. [Online] Available at: https://nordlayer.com/identity-access-management/?gclid=CjwKCAiAmZGrBhAnEiwAo9qHiYzh5BoV6k-uChoo7rbO1JrcvQF0gYjIVtL1tNw1SxjxsfQibNp90hoCDjYQAvD_BwE [Accessed 27 November 2023].
Oberlo, 2023. KEY PERFORMANCE INDICATOR (KPI). [Online] Available at: https://www.oberlo.com/ecommerce-wiki/key-performance-indicator-kpi [Accessed 26 November 2023].
Osypanka, P. & Nawrocki, P., 2022. Resource Usage Cost Optimization in Cloud Computing Using Machine Learning. IEEE Transactions on Cloud Computing, 10(3), pp. 2079-2089.
Ozer, M. M. et al., 2020. Cloud Incident Response: Challenges and Opportunities. 2020 International Conference on Computational Science and Computational Intelligence (CSCI), pp. 49-54.
Pearson, S. & Yee, G., 2013. Privacy and Security for Cloud Computing. Netherlands: Springer London.
Probst, C. W., Gollmann, D., Hunker, J. & Bishop, M., 2010. Insider Threats in Cyber Security. Germany: Springer US.
Ravuri, A., Lingamallu, R. K., S Arvind, P. S. R. & Ammisetty, V., 2023. Evaluation of Cloud-Based Cyber Security System. International Journal on Recent and Innovation Trends in Computing and Communication, 11(10), pp. 1723-1730.
Rob S., 2023. New whitepaper: A Guide to Cybersecurity Certifications in the UK 2023 edition. CyberSmart.
Salkind, N. J., 2012. 100 Questions (and Answers) About Research Methods. s.l.:SAGE Publications.
Senior Manager, T. L. I., 2023. Employee Training and Security Awareness [Interview] (20 November 2023).
Sherif, M. & Sherif, C. W., 1964. Reference Groups; Exploration Into Conformity and Deviation of Adolescents. California: Harper and Row.
Skaria, R., 2023. Optimizing Microsoft Azure Workloads: Leverage the Well-Architected Framework to Boost Performance, Scalability, and Cost Efficiency. United Kingdom: Packt Publishing.
Snyder, E. P., Christner, R. W. & Lionetti, T. M., 2010. A Practical Guide to Building Professional Competencies in School Psychology. United Kingdom: Springer US.
Solar, R. G. d., 2016. Why are research questions important? What makes them important?. Barcelona: University of Barcelona.
Spair, R., 2023. The ultimate guide to unlockng the full potential of cloud services: Tips, Recommendations, and Strategies for Success. s.l.:Rick Spair.
Spellman, F. R., 2018. Communications Sector Protection and Homeland Security. United States: Bernan Press.
Srivastav, N. & Saxena, S., 2023. SECURITY AND COMPLIANCE: A MUST-HAVE VISUAL GUIDE FOR EVERYONE!. s.l.:CyberEdx.

Taiwo, A. A. .., Lawal, F. A. & Agwu, E., 2016. Vision and Mission in Organization: Myth or Heuristic Device?. The International Journal Of Business & Management, 4(3), p. 127.
Tamunobarafiri, A., Aghili, S. & Butakov, S., 2019. Data Security and Privacy Assurance Considerations in Cloud Computing for Heath Insurance Providers. In: I. R. M. Association, ed. Cloud Security: Concepts, Methodologies, Tools and Applications. Edmonton: IGI Global, pp. 973-977.
Taylor, A., Alexander, D., Finch, A. & Sutton, D., 2013. Information Security Management Principles Updated Edition. 2nd ed. Swindon: BCS Learning and Development Ltd..
Travieso-Gonzalez, C. M. et al., 2023. Sustainable Computing: Transforming Industry 4.0 to Society 5.0. Switzerland: Springer International Publishing.
Turban, E., Pollard, C. & Wood, G., 2021. Information Technology for Management: Driving Digital Transformation to Increase Local and Global Performance, Growth and Sustainability. United Kingdom: Wiley.
UK Data Service, 2023. Research data management. [Online] Available at: https://ukdataservice.ac.uk/learning-hub/research-data-management/#data-protection [Accessed 28 November 2023].
Vacca, J. R., 2021. Cloud Computing Security: Foundations and Challenges. 2nd ed. FL: CRC Press.
Verizon, 2023. 2023 Data Breach Investigations Report, s.l.: Verizon.
Verma, A., Cherkasova, L. & Campbell, R. H., 2011. Resource scalability and cost optimization in cloud computing. s.l., IEEE, pp. 235-242.
vmware, 2023. What is Cloud Security?. [Online] Available at: https://www.vmware.com/topics/glossary/content/cloud-security.html
Walters, R. & Novak, M., 2021. Cyber Security, Artificial Intelligence, Data Protection & the Law. Singapore: Springer Nature Singapore.
Weill, P. & Ross, J. W., 2004. IT Governance: How Top Performers Manage IT Decision Rights for Superior Results. s.l.:Harvard Business Review Press.
Winkler, I., 2022. Security Awareness For Dummies. United States: Wiley.
World Medical Association, 2023 . WMA DECLARATION OF HELSINKI – ETHICAL PRINCIPLES FOR MEDICAL RESEARCH INVOLVING HUMAN SUBJECTS. [Online]
Available at: https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/ [Accessed 28 November 2023].
ZAHRA, A. B., 2022. Building Cloud Data Platforms Solutions; An End-to-End Guide for Designing, Implementing, and Managing Robust Data Solutions in the Cloud. s.l.:Anouar BEN ZAHRA.
Zhang, Q., Cheng, L. & Boutaba, R., 2010. Cloud computing: State-of-the-art and research challenges. Journal of Internet Services and Applications, pp. 7-18.