The Changing Information Systems Landscape Creates New IT Risk

IT audit has been evolving at a fast pace, especially in the past decade. What started as audits of an isolated system in the form of electronic data processing (EDP) has progressed into audits of a wide range of interconnected systems and technologies, sometimes spanning the world. As many enterprises move from traditional brick-and-mortar business to ecommerce and sales through social media, they are compelled to adopt emerging technologies for support. Therefore, audit also needs to evolve to address the technological advances and changes in the information systems landscape.

It is imperative to understand how to integrate new technologies with legacy setups and how to address the widespread risk they introduce.

Enterprises are operating in a competitive world where they aim to outdo others in terms of new product launches, geographical expansion and cost reduction. However, any business strategies devised are incomplete or ineffective without alignment with IT strategies. IT plays a pivotal role in today's business world and can give organizations the right competitive advantage. Technology adoption in business has become so critical that a new role, chief digital officer,[1] has been created to designate a person responsible for adopting digital transformation, including emerging technologies. The objective is to make the business more agile as business needs change. As Bill Gates once said, "Information technology and business are becoming inextricably interwoven. I don't think anybody can talk meaningfully about one without talking about the other."[2]

Though new technologies benefit enterprises, they also create opportunities for cyberbreaches due to a lack of awareness and understanding of the new risk they bring. A small but critical vulnerability in a system can potentially bring an entire network down. It is imperative to understand how to integrate new technologies with legacy setups and how to address the widespread risk they introduce.

Emerging Technologies

Emerging technologies are innovative technical solutions with either development potential or

SRIRAM BALALSUBRAMANIAN | AWS CLOUD PRACTITIONER, CERTIFIED SCRUM MASTER

Is a director with Deloitte's risk advisory practice and has more than 15 years of experience. His focus is on leading large audit engagements across multiple industries that include complex systems and control environments. In addition to audit engagements, he has also led US Sarbanes-Oxley Act of 2002 (SOX) management testing, business process automation, business process redesign, IT internal audits and redesign of clients' risk and controls matrices as per the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework and SAP postimplementation reviews. He can be contacted on LinkedIn at *https://www.linkedin.com/in/srirambalas/*.

The IT landscape becomes increasingly complex when multiple emerging technologies are adopted.

practical applications, or both, that are still largely unrealized. They are emerging into prominence from a background of nonexistence or obscurity. Emerging technologies are often perceived as capable of changing the status quo.[3]

The adoption of emerging technologies has transformed the way traditional IT departments function in many organizations. The rapid digitization of society generates an unfathomable amount of data. In 2020, due to the COVID-19 pandemic, more people worked and studied from home, resulting in a record volume of data. More than 90 percent of the world's data have been produced in the past two years.[4] Global data generation is predicted to increase to approximately 175 zettabytes (i.e., 180 x 1021 bytes) by 2025.[5]

Consider some widely used emerging technologies to understand how they have transformed business:

- **The cloud**—Enterprises are increasingly adopting cloud technology to gain advantages in operational excellence, security, reliability, performance efficiency and cost optimization. Organizations can derive significant cost savings by replacing onsite data centers with pay-as-you-go models, converting capital expenditures or investments to operating expenses. With these models, enterprises do not need to guess on capacity requirements and can scale infrastructure as required. For example, Netflix successfully migrated all its databases to the cloud in 2016. As a result, the streaming giant can now produce more content, onboard more customers and easily handle sharp increases in usage spikes (typically when new episodes of a show are made available). It can also add or reduce storage amounts in real time based on its current viewers.[6]
- **Internet of Things (IoT)**—IoT has become particularly popular with consumer applications such as connected vehicles, wearables (e.g., smart watches) and connected healthcare information services. For example, in the transportation industry, IoT applications can monitor a fleet of vehicles, enable inter- and intra-vehicular communication; manage electronic toll collection systems; and connect sensors that monitor equipment temperature and pressure.
- **Artificial intelligence, machine learning and robotic process automation**—Artificial intelligence (AI) and machine learning (ML) have multiple applications in business. Many enterprises use chatbots as a first line for resolving customer queries and complaints. Other applications in ecommerce include product recommendations, purchase predictions and dynamic price optimization. Bots are also commonly used in image recognition. Robotic process automation (RPA) involves deploying programmed software robots that are closely integrated with multiple applications to read, process data and perform repetitive tasks. This helps automate mundane tasks to optimize the workforce.
- **Blockchain**—A blockchain is a system of recording information in a way that makes it hard to change, hack or cheat the system. The most popular use of blockchain is in cryptocurrency. Many countries are looking into launching their own cryptocurrency called Central Bank Digital Currency (CBDC), which is a legal tender of a particular country in digital form.[7] Banks are deploying blockchain technology to solve issues with processing letters of credit (LCs), goods and services tax invoices and e-way bills (used for tracking of shipments and good movement).[8] Another use of blockchain technology is smart contracts, in which programs stored on blockchain are executed when predetermined conditions are met as agreed upon between the parties. In addition, nonfungible tokens (NFTs) allow digital content such as photos, videos, paintings and digital art and audio to be converted into proprietary assets and traded.
- **Big data**—Big data refers to a massive volume of data that grow exponentially in complexity and size over time. Big data cannot be processed by traditional data management tools. The data are collected from multiple sources, such as business application pools, logs, social media, third parties and IoT devices. Furthermore, data are collated from text, audio, video and images, and missing pieces are completed through data fusion. The retail industry is one of the best use cases of big data. Enterprises build predictive models for new products and services by classifying key attributes

of past and current products. With such models, retailers can dig deeper by using data and analytics from focus groups, social media, test markets and early store rollouts to plan, produce and launch new products.[9] With online analytical processing (OLAP), complex queries can be applied to large amounts of historical data aggregated from online transaction processing (OLTP) databases and other sources for data mining, analytics and business intelligence projects.[10]

The IT landscape becomes increasingly complex when multiple emerging technologies are adopted. For instance, an ecommerce enterprise can have multiple home-grown applications (apps) on the cloud and make continuous changes to a mobile app and other business support systems through DevSecOps models. Similarly, a utility enterprise may have hundreds or thousands of smart connected devices that feed data into the cloud, which processes the information and generates relevant alerts. In another example, data lakes in the cloud, organizations use various analytical tools to process the information and derive meaningful insights. Analytical tools are offered by popular cloud service providers and leveraged for this purpose.

New Risk, Threats and Vulnerabilities

As the IT landscape evolves and becomes more complex, IT risk is elevated and new risk and threats are introduced. It is estimated that 60 percent of small- and medium-sized businesses close within six months of a data breach.[11] A data breach can hurt a large enterprise's reputation, as customers may then prefer to conduct business with competing enterprises that they deem safer.[12]

New risk that organizations commonly encounter after adoption of any emerging technology include improper use of data, IoT vulnerability, system failure, attacks and misconfiguration.

Improper Use of Data

Data collection is an essential aspect of both business-to-business (B2B) and business-to-customer (B2C) applications. Developers collect information—such as users' location and social media profile information—for troubleshooting purposes. If the developer is not scrupulous and mindful of the data being collected, this information can easily fall into the wrong hands and have far-reaching implications. Further, organizations can be penalized for not following regulations or for noncompliance with data use regulations.

New risk that organizations commonly encounter after adoption of any emerging technology include improper use of data, IoT vulnerability, system failure, attacks and misconfiguration.

Many enterprises have a bring-your-own-device (BYOD) policy to save on their investment in IT without understanding the threat this practice can pose to network security. Working from home also creates greater risk exposure due to employees accessing content online without the restrictions of firewalls or blacklisted IPs. Furthermore, employees can access email and other business applications through their personal devices, thereby exposing sensitive business information to a possible data breach. Organizations need to understand their existing risk frameworks before considering the feasibility of a BYOD policy.

IoT Vulnerability

Implementation of IoT results in a large number of endpoints, thereby allowing an attacker more ways to find a weak link to infiltrate the network of devices. The attack surface of the network consists of all the possible places where it can be attacked, and it expands with every new Internet-connected device. Even if the chance of one device being accessed by a perpetrator is small, introducing a large number of IoT devices into businesses can create a significant security risk.[13]

The risk due to IoT vulnerability includes access to sensitive data; sabotage, with the hacker either altering or controlling the device's operation; and botnets—huge networks of infected devices cybercriminals use to carry out distributed denial-of-service (DDoS) attacks.

Data breaches via IoT devices can result in business delays and breaches of security and privacy. Regardless of the industry, enterprises collecting data through IoT applications may be subject to data

LOOKING FOR MORE?

- Read *IT Audit Perspectives on Today's Top Technology Risks. www.isaca.org/it-audit-2022*
- Learn more about, discuss and collaborate on risk management in ISACA's Online Forums *https://engage.isaca.org/onlineforums*

privacy laws such as the EU General Data Protection Regulation (GDPR). There can be hefty fines and legal repercussions if such privacy laws are violated.

System Failures

Not all system crashes are due to cyberattacks. Enterprises are increasingly dependent on multiple interconnected systems, various interfaces, multiple cloud service providers (CSPs) and third-party vendors and sensors that capture and relay real-time information. The complexity of such setups requires meticulous integration testing and appropriate preparation for redundancies in case one elements fails.

> Adoption of emerging technologies while understanding the added risk requires reassessing the standard risk around user access management, change management and even IT operations.

Uber was involved in a fatal crash in Tempe, Arizona, USA, in 2018, which is believed to be the world's first death caused by a self-driving car. The crash was attributed to poor object recognition, emergency planning (for applying emergency brakes), system design, testing methodology and human operation. The object-detection system misclassified the victim when its sensors first detected the victim as "an unknown object, as a vehicle, and then as a bicycle with varying expectations of future travel path." That led the planning software to make poor predictions for the victim's speed and direction and the car's speed and direction.[14]

System failures can impact business operations and result in reputation damage and huge penalties. Another example involves a leading European bank that had a systems failure in 2012 resulting in an inability to account for 600,000 customer payments. Before this incident, the bank was fined UK£56 million for an IT meltdown that caused 6.5 million customers to be locked out of their accounts.[15]

Phishing, Malware and Ransomware Attacks

Phishing is a mechanism used by hackers to trick users into opening harmful emails that look like legitimate emails with business names, logos, links and attachments. The emails prompt users to take action by either logging in through a link or opening an attachment, thereby revealing their credentials and other sensitive information.

Malware is malicious software that can slow devices or disrupt them entirely. It can infiltrate devices when users click on infected links or pop-ups or download files from unknown sources in response to phishing emails. Once malware is active in a system, hackers can gain access to sensitive information such as enterprise passwords, banking data, personal files and credit card information.

Ransomware is a form of malware that encrypts a system, including critical business information, thereby preventing users from accessing their systems or files. Cybercriminals then demand ransom, typically in the form of cryptocurrency, to decrypt the information and restore access. In addition to the ransom, the enterprise may have to pay penalties for exposure of sensitive customer data.

The ransomware attack on Colonial Pipeline in the United States is a well-known example. The attacker targeted the enterprise's billing system and internal business network, leading to widespread gasoline shortages in multiple states. To prevent further disruption, the enterprise paid a ransom of US$4.4 million in Bitcoin.[16]

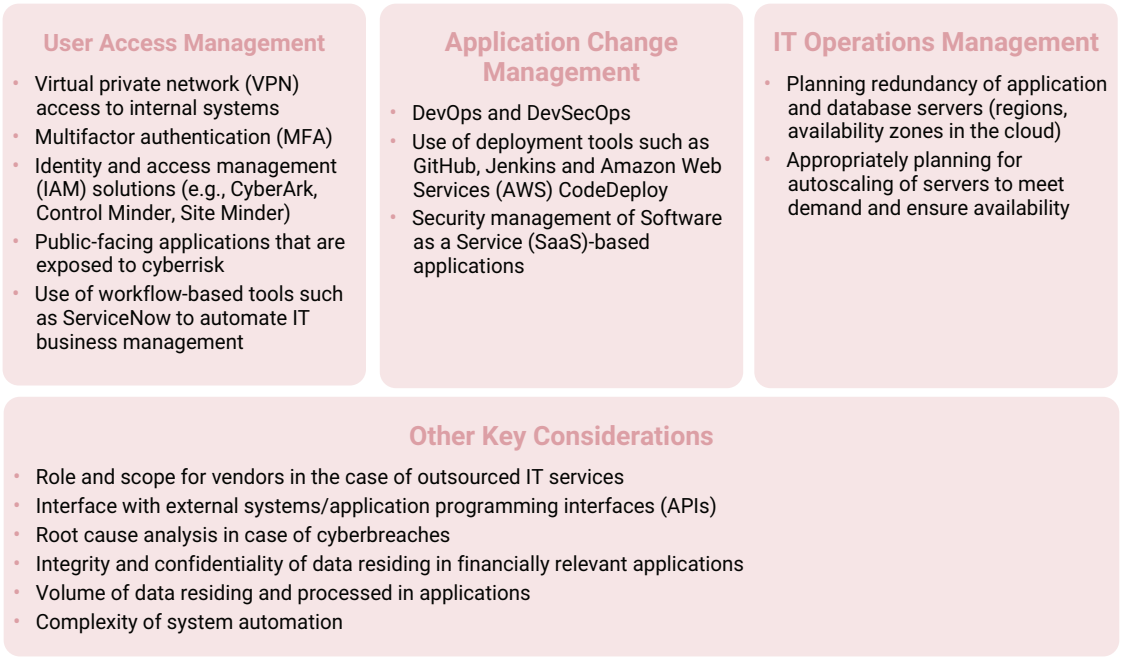
Misconfigurations

Security misconfigurations result when security controls are inaccurately configured or left unsecured, putting systems and data at risk. Any poorly documented configuration changes, default settings, or technical issues across any component in the endpoints can lead to a misconfiguration.[17]

Security misconfigurations have become common due to constant changes to complex network infrastructures to support businesses. Organizations can easily overlook crucial settings, including network devices that might retain default configurations. For example, Accenture was impacted by an Amazon S3 misconfiguration attack in September 2017 when authentication information that included certificates, plaintext passwords, keys and sensitive customer information was leaked.[18]

FIGURE 1

Factors for Mitigating Emerging Technology Risk



Mitigating the Risk

Adoption of emerging technologies while understanding the added risk requires reassessing the standard risk around user access management, change management and even IT operations. Some factors to consider are highlighted in **figure 1**.

Stronger Safeguards and Controls

New risk factors due to emerging technologies require a fresh look at the organization's risk and controls framework. Risk management requires balancing the tradeoffs between security, operational requirements and cost.

IT governance plays a significant role in adopting emerging technologies and integrating them into the business. This process requires representation from various IT stakeholders—such as the security and infrastructure team, application development, application support and C-suite—and specific inputs from third-party vendors.

The board and C-suite should review the approach to emerging technology risk in crucial areas including:

- **Validating the current risk framework**—The adoption of any emerging technology needs to align with the overall risk appetite of the enterprise. The organization should also assess how such technology will impact the current systems landscape and support rendered by existing IT service providers. This requires an understanding of the new IT risk and the controls it might necessitate.
- **Assessing the team's competency in emerging technologies**—The IT team should not just oversee implementation of the new technologies and solutions; but should also be watchful from a risk and vulnerability perspective. IT team members should be experienced professionals who, in addition to being technically strong and adept with new technologies, can view things from a compliance perspective, understanding the relevance of IT controls and impact of vulnerabilities.
- **Assessing risk exposure from third-party service providers**—In most cases, enterprises depend on third parties when implementing emerging technologies. However, many organizations do not consider third-party risk before engaging with a vendor for implementation and support. This creates risk because such implementations are expensive and may have serious repercussions on business continuity and reputation.
- **Creating or strengthening cybersecurity policy**—An organization's cybersecurity policy

FIGURE 2

IT Risk and Best Practices for Emerging Technologies

UNDERLYING TECHNOLOGY	IT DOMAIN	RISK	ADDRESSING RISK
RPA	Logical Access	RPA bots sit on top of multiple interconnected systems. Compromise of privileged credentials in a bot can put all interconnected systems at risk.	Restrict use of privileged access to bot user accounts. Ensure bots are sufficiently secured to prevent unauthorized access.
Cloud	Change Management, DevOps	Multiple applications (both internal and external) rely on APIs for seamless integration and information exchange. Unauthorized changes to APIs can impact the quality and completeness of data transferred.	Changes to APIs are as critical as any other application changes. Ensure that changes are properly tracked and tested with appropriate use cases.
Cloud	Logical Access, Change Management, Network Security	It is a myth that all risk is transferred to the CSP once the application is hosted on the cloud. The shared responsibility model indicates that the responsibilities are divided between the enterprise and the CSP.	Application/server security, encryption and backup can be the enterprise's responsibility depending on the type of cloud setup. Validate the responsibilities with the CSP's system and organization control (SOC1) report to ensure that the enterprise is taking ownership of areas not covered.
Cloud, Cybersecurity	Network Security	With interconnected systems and a hybrid cloud, a web application firewall (WAF) alone may not offer sufficient protection. A cyberbreach in the network can put the web application server at risk as well. Other sophisticated tools for DDoS protection and real-time monitoring are required. Lack of attention to cybersecurity can result in cyberbreaches that have irreversible implications, including loss/leak of sensitive data, costs and reputational damage.	Cybersecurity controls should include network architecture, network monitoring, WAF, intrusion detection solutions (IDSs), vulnerability assessment and penetration testing (VAPT) and timely addressing of network vulnerabilities. Use sophisticated network tools to carry out network monitoring. Consider onboarding a vendor for a security operations center (SOC) due to the critical applications and their sensitivity/impact. If applications are integrated with active directory (AD), then validate if AD administrators have access to the application and database.
IoT	Logical Access	IoT devices can be hacked to infiltrate the corporate network, thereby putting other financially critical applications at risk.	All IoT devices should be authenticated when connecting to the corporate network. Further, such devices should operate on the principle of least privilege by allowing users access to only what is necessary for them to do their job. Factory-installed passwords should be updated, and MFA should be enabled wherever possible. All IoT devices connecting to a corporate network should have regular patches and updates.
Big Data	Security and Privacy	One common pitfall with big data is the tendency to collect all data and think about analyzing it later. This not only increases storage costs but also increases compliance risk. Having vast amounts of unsecured data can lead to regulatory noncompliance (e.g., with the GDPR), which can not only result in huge penalties but also impact an organization's reputation.	It is prudent to only gather data that are relevant to reduce the extent of impact during a data breach. Organizations can consider segmenting the data that are collated from various sources and accordingly encrypt sensitive data.
Blockchain	Security and Privacy	Hackers can exploit loopholes in enterprise blockchain software to access smart contract deployments and manipulate the logic. This can impact the sanctity of an active contract thereby resulting in higher payments, regulatory noncompliance and penalties.	Enterprise blockchain software should be kept up to date with the latest security fixes. Security vulnerability databases should be monitored for blockchain and smart contract entries. Code security should be reviewed and new secret keys should be generated prior to deployments.

should be a living document that is constantly updated as attacks evolve. The fundamental policy should include guidelines on protecting network devices (including operating system patches, firewall, antivirus and encryption), multifactor authentication (MFA), and solutions on data leakage prevention and data protection (e.g., BYOD policy, mobile data management and handling personally identifiable information [PII]).

Best Practices

Once the risk and vulnerabilities of implementing emerging technologies and the focus areas to appropriately tackle them are understood, organizations can implement best practices (**figure 2**).

Formal Frameworks

The Cloud Security Alliance (CSA) has developed a cybersecurity control framework for cloud computing called the CSA Cloud Controls Matrix (CCM). It is composed of 197 control objectives across 17 domains covering all key aspects of cloud technology. The controls are mapped across industry-accepted security standards and regulations, such as International Organization for Standardization (ISO) standard ISO 27001, COBIT®, US National Institute of Standards and Technology (NIST) standards and the Payment Card Industry Data Security Standard (PCI DSS).[19]

Considering the widespread impact of IT risk on business, it is imperative that business owners participate equally in this initiative and work collectively with first and second lines of defense.

The shared responsibility model provides guidance on division of responsibilities between the organization and the CSP. The CSP is responsible for security of the cloud, whereas the customer is responsible for security in the cloud.[20]

The Internet Society's IoT Trust Framework covers a set of strategic principles necessary to help secure IoT devices and their data when shipped and throughout their entire life cycle. The framework is comprised of four key areas:

1. Security principles
2. User access and credentials
3. Privacy, disclosures and transparency
4. Notifications and related best practices[21]

Conclusion

Adopting emerging technologies can create competitive advantages, but the benefits are naturally accompanied by risk. Process owners can take a proactive approach to identifying IT risk by engaging with internal audit or enterprise risk management. Considering the widespread impact of IT risk on business, it is imperative that business owners participate equally in this initiative and work collectively with first and second lines of defense.

Initiating discussions about risk and controls early in the technology's implementation helps in identifying unaddressed issues and process improvements and ensures that emerging technologies are successfully integrated into the business. Organizations need to be conscious of emerging IT risk and adopt the leading industry practices to strengthen their existing IT policies and procedures. This requires assessing teams' competency and evaluating the risk from third-party service providers.

Endnotes

1 Tucci, L.; "Chief Digital Officer (CDO)," *TechTarget*, *https://www.techtarget.com/searchcio/definition/Chief-Digital-Officer-CDO#:~:text=A%20chief%20digital%20officer%20is,to%20a%20digital%20business%20model*
2 Stephens, T.; "Information Technology and Business are Becoming Inextricably Interwoven," 28 July 2013, *https://trevorstephens.com/ramblings/it-and-business/*
3 Wachemo University (Ethiopia) E-Learning Platform, "Introduction to Emerging Technologies," *https://wachemo-elearning.net/courses/introduction-to-emerging-technologies/#tab-course-section__overview*
4 Marr, B.; "How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read," *Forbes*, 21 May 2018, *https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/?sh=3103aac360ba*

5 Patrizio, A.; "IDC: Expect 175 Zettabytes of Data Worldwide by 2025," *Network World,* 3 December 2018, *https://www.networkworld.com/article/3325397/idc-expect-175-zettabytes-of-data-worldwide-by-2025.html*

6 Daley, S.; "Twenty-Six Cloud Computing Examples That Keep the World at Our Fingertips," Builtin, 14 March 2022, *https://builtin.com/cloud-computing/cloud-computing-examples*

7 Central Bank Digital Currency (CBDC) Tracker, "Today's Central Bank Digital Currencies Status," *https://cbdctracker.org/*

8 *The Economic Times Banking, Financial Services and Insurance (ETBFSI),* "How Indian Banks are Leveraging Blockchain Technology," 2 December 2021, *https://bfsi.economictimes.indiatimes.com/news/banking/how-indian-banks-are-leveraging-blockchain-technology/88027231*

9 Oracle, "The Top Use Cases for Big Data Analytics," *https://www.oracle.com/in/big-data/what-is-big-data/the-top-use-cases-for-big-data-analytics/*

10 Stitch, "OLTP and OLAP: A Practical Comparison," *https://www.stitchdata.com/resources/oltp-vs-olap*

11 Galvin, J.; "Sixty Percent of Small Businesses Fold Within Six Months of a Cyber Attack," *Inc.*, *https://www.inc.com/joe-galvin/60-percent-of-small-businesses-fold-within-6-months-of-a-cyber-attack-heres-how-to-protect-yourself.html*

12 Poremba, S.; "Six Potential Long-Term Impacts of a Data Breach," *Security Intelligence,* 5 November 2021, *https://securityintelligence.com/articles/long-term-impacts-security-breach/*

13 Avast, "What Risks Do IoT Security Issues Pose to Businesses?" 12 February 2019, *https://blog.avast.com/iot-security-business-risk*

14 Madrigal, A. C.; "Uber's Self-Driving Car Didn't Malfunction, It Was Just Bad," *The Atlantic,* 24 May 2018, *https://www.theatlantic.com/technology/archive/2018/05/ubers-self-driving-car-didnt-malfunction-it-was-just-bad/561185/*

15 Farrell, S.; C. Fishwick; "RBS Could Take Until Weekend to Make 600,000 Missing Payments After Glitch," *The Guardian,* 17 June 2015, *https://www.theguardian.com/business/2015/jun/17/rbs-fails-to-make-600000-payments-customers-it-technology-failure-bank*

16 Touro College Illinois (Skokie, Illinois, USA), "The 10 Biggest Ransomware Attacks of 2021," 12 November 2021, *https://illinois.touro.edu/news/the-10-biggest-ransomware-attacks-of-2021.php*

17 Manage Engine, "Security Misconfiguration," *https://www.manageengine.com/vulnerability-management/misconfiguration/*

18 Dizdar, A.; "Misconfiguration Attacks: Five Real-Life Attacks and Lessons Learned," Bright, 4 October 2021, *https://brightsec.com/blog/misconfiguration-attacks#amazon-s3*

19 Cloud Security Alliance (CSA), Cloud Controls Matrix (CCM), *https://cloudsecurityalliance.org/research/cloud-controls-matrix*

20 Cloud Security Alliance (CSA), "Shared Responsibility Model Explained," 26 August 2020, *https://cloudsecurityalliance.org/blog/2020/08/26/shared-responsibility-model-explained/*

21 Internet Society, "OTA IoT Trust Framework," *https://www.internetsociety.org/iot/trust-framework/*