Cloud Security Auditing:
Challenges and Emerging Approaches

Jungwoo Ryoo, Syed Rizvi, William Aiken, and John Kissell | Pennsylvania State University

IT security audits determine whether an information system and its maintainers meet both the legal expectations of customer data protection and the company's standards of achieving financial success against various security threats. These goals are still relevant in the emerging cloud computing model of business, but they require customization.

Cloud computing, as defined by the National Institute of Standards and Technology (NIST), is "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[1] In essence, cloud computing could be described as the use of computing resources—both hardware and software—provided over a network, requiring minimal interaction between users and providers.

Three service models are commonly implemented in the cloud: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). In each of these service types, security is a significant challenge. Security audits provide a clear and recognizable trail of resource access for various organizations.

Traditional IT audits typically fall into two main categories: *internal* and *external*. Internal audits refer to work done by an organization's own employees, concern very specific organizational processes, and focus primarily on optimization and risk management. External audits give an outside perspective on an organization's ability to meet the requirements of various laws and regulations. Organizations have used traditional IT audits to evaluate issues such as availability to authorized users and integrity and confidentiality in data storage and transmission.

But what happens when an organization's IT resources are moved to the cloud? Because cloud computing allows for multiple users across a large domain, it exposes novel security issues such as cloud-specific confidentiality concerns. These threats pose new challenges for security auditing, but cloud advocates are responding to them. For instance, groups such as Cloud Security Alliance (CSA; www.cloudsecurityalliance.org) are urging standardization of cloud confidentiality, integrity, and availability auditing.

In this article, we highlight the challenges that separate cloud security auditing from traditional IT security auditing practices. These challenges illustrate the importance of special provisions for cloud security auditing in existing or newly emerging security auditing standards. We conducted a series of interviews with experienced cloud security auditors and incorporated their insights and advice into our discussions.

Challenges

A traditional IT security audit is an examination of an IT group's checks, balances, and controls. Auditors enumerate, evaluate, and test an organization's systems, practices, and operations to determine whether the systems safeguard the information assets, maintain data integrity, and operate effectively to achieve the organization's business goals or objectives.[2] To support these objectives, IT security auditors need data from both internal and external sources.

 Copublished by the IEEE Computer and Reliability Societies

Table 1. Cloud-specific auditing challenges.

Challenge	Traditional IT security auditing practice	Cloud-specific challenge	Potential cloud security auditing solution
Transparency	Data and information security management systems are more accessible.	Data and security are managed by a third party.	Service-level agreements should outline CSP policies and assurances while CSPs provide clients with audit results.
Encryption	The data owner has control.	Cloud service providers (CSPs) might be responsible for encryption.	Use a third party and homomorphic encryption.
Colocation	This rarely occurs.	CSPs heavily depend on this.	Standardize and increase oversight.
Scale, scope, and complexity	These are relatively less.	Auditors must be knowledgeable and aware of these differences.	Implement continuing education and new certification programs.

In addition, cloud computing comes with its own set of security challenges. A cloud infrastructure is the result of a constant three-way negotiation among service organizations, cloud service providers (CSPs), and end users to ensure productivity while maintaining a reasonable degree of security. A CSP should keep data safe from security threats and yet give clients access anywhere with Internet service. In addition, the client organization must verify that the cloud computing enterprise contributes to its business goals, objectives, and future needs.

Although both conventional IT security auditing and cloud security auditing share many concerns, a cloud security audit must address unique problems typically not handled in traditional IT security audits. According to our interviews, the most immediate and obvious challenge lies in auditors acquiring sufficient knowledge of cloud computing. Effective cloud security auditors must be familiar with cloud computing terminology and have a working knowledge of a cloud system's constitution and delivery method. This knowledge ensures auditors pay attention to security factors that might be more important in cloud security auditing processes, including transparency; encryption; colocation; and scale, scope, and complexity (see Table 1).

Transparency

Cloud security audits must check whether security-relevant data is transparent to CSP customers. Transparency lets organizations more easily identify potential security risks and threats as well as create and develop the right countermeasures and recommendations for their enterprise.[3] By having access to accurate information, cloud service users (CSUs) can reduce the risk of manifesting threats.

A good cloud security audit questions whether a CSP provides a solid balance between security controls and end user access. Employees might need to access the cloud from home or on a business trip. Does the CSP allow for such types of access, and can it prevent others from impersonating legitimate users? More important, is the CSP willingly transparent about its access control mechanisms?

Typically, cloud computing systems are based in a large datacenter, and a third-party subcontractor might manage them. A client has no idea who handles the data or where exactly on the system it's stored. To expose the risks associated with this undesirable situation, a cloud security audit must strive to reveal these details to the client. Transparency of data privacy, data security, anonymity, telecommunications capacity, liability, reliability, and government surveillance ensures strong client data security.[3] For example, a CSP that records personal information such as credit card numbers is an invitation for cybercriminals. As a result, a service-oriented company utilizing a third-party cloud infrastructure or any CSUs should expect to know what kind of information is in the cloud at any given time to adequately respond to breaches.

Even in traditional IT audits, a lack of data transparency can lead to a loss of control over in-house company resources. For instance, an unreported back door to a critical corporate system can result in devastating damage to the organization. Systems administrators shouldn't be the only ones who understand the computing resources and the risks associated with them. A traditional IT security audit gathers and analyzes the data on the organization premises. Without this type of audit, a company has no idea what its assets are, where they're stored, or how to protect them from potential threats.

Transparency is even more critical in cloud security auditing because the security-relevant data is harder to obtain as CSPs, rather than CSUs, control most of the data. A comprehensive understanding of CSP asset data, data location, and data security policies is necessary in cloud security audits as well.

Encryption

It's unsafe to store sensitive plaintext data anywhere, especially outside a home organization's IT

infrastructure. If a cloud is breached, the information in it would be instantly available to hackers. To prevent this, a client could encrypt all its data in-house before sending it to the cloud provider, but this approach introduces the risk of system administrators abusing their privileges. Leaving encryption to the CSP isn't foolproof either: a breach in its storage system might also mean a breach in its encryption and decryption tools.

Traditional IT infrastructures face many encryption concerns as well. Which is more important: encryption of data or access to data? If an entire data pool is encrypted at rest, how can an organization quickly and efficiently query the data without decrypting all of it? Due to its heavy computational requirements, encryption might not always be the most efficient solution. Only in situations in which the sensitive data isn't accessed frequently (for instance, archived payroll information) does encryption at rest become a viable option.

> **Effective cloud security auditors must be familiar with cloud computing terminology and have a working knowledge of a cloud system's constitution and delivery method.**

A cloud infrastructure isn't free from these pitfalls. The same question arises: should data at rest be encrypted? CSPs frequently provide encryption by default—as in the case of Amazon's Simple Storage Service (S3)—which could result in double encryption (once by a CSU and once by a CSP). In contrast, Amazon's Elastic Compute Cloud service doesn't provide encryption by default, leaving it up to customers. Third-party services, such as CipherCloud (www.ciphercloud.com), let clients encrypt the data before sending it to a CSP. Data in transmission is usually encrypted using technologies such as Secure Socket Layer. Assuming a CSU depends solely on the CSP for encryption, it must allow the CSP to control its encryption and decryption mechanisms and have access to all the data it stores (for example, S3).

This isn't a safe practice because if one part of the cloud is compromised, it's possible that all encrypted data will be compromised as well. As a result, it's more desirable for encryption and decryption to take place outside the reach of a CSP. But is encrypting and decrypting cloud storage data worth the extra computational resources outside the cloud? Possibly, but newer innovations in fully homomorphic encryption allow encrypted queries to search encrypted texts without search engine decryption.[4] This type of encryption has the potential to solve the security issue of encrypted data at rest in both traditional IT and cloud infrastructures.

According to the auditors we interviewed, in a traditional IT security audit, both external auditors and an audited organization meet on the audited organization's premises and strive to reach a balance of privacy: auditors want to keep their queries secret, and the audited organization wants to preserve the privacy of all its encrypted data. Auditors are given just enough access to the organization's data to complete their work; they have access but may not copy or remove anything.

The struggle to obtain a balance of privacy also occurs in various cloud computing scenarios. However, in a cloud system, such collaboration between the audited organization and the auditors might not be nearly as efficient, possible, or necessary because all the data resides in a third-party infrastructure (that is, the CSP's datacenters). The CSP might not be willing or able to disclose certain cryptographic information, even under auditing circumstances. To help mitigate this cloud-specific problem, the Payment Card Industry (PCI) Data Security Standard (DSS) Cloud Special Interest Group (SIG) strongly encourages that cryptographic keys and encryption algorithm information "be stored and managed independently from the cloud service."[5]

Colocation

The core benefit of cloud computing is that multiple user organizations can share one service organization's physical systems. Although it's a great cost-reduction method, sharing technology infrastructure leads to equally great security concerns. It's crucial that CSPs keep user systems from gaining administrative access to the physical hardware to prevent abuse of services and access to other clients' data.

IaaS frequently encounters this problem; to address it, CSPs turn to hypervisors that insulate virtual machines (VMs) from physical computing hardware. Examples of hypervisors in use today are Xen (open source), VMWare (proprietary), Microsoft's Virtual Server, the Kernel-Based Virtual Machine (KVM), IBM's PowerVM, and many others that incorporate Intel and AMD architectures. The security auditing problem arises from this situation: there are countless ways to organize or establish a hypervisor in a cloud system, each with its own strengths, weaknesses, and priorities.

A CSP must balance not only a hypervisor's and colocation system's business needs but also the security issues. Despite the apparent need to standardize the structure and security of colocation, no official standard exists. Even PCI DSS doesn't list specialized standards regarding these evolving concerns. However, the PCI

DSS Cloud SIG has developed a few recommendations for multitenancy.[5] It provides three sample cloud segmentation environments: traditional separate servers for each client's cardholder data, virtualized servers dedicated to each client and its cardholder data, and applications running in separate logical partitions and separate database management images with no sharing of resources such as disk storage.

Considering the multitude of cloud–hypervisor combinations and varying degrees of cloud adoption, a PCI DSS–style evaluation of a cloud system must include individual examinations of all CSPs. To assert the importance of proper colocation security, the PCI DSS Cloud SIG issued this statement regarding multitenancy: "Without adequate segmentation, all clients of the shared infrastructure, as well as the CSP, would need to be verified as being PCI-DSS-compliant in order for any one client to be assured of the compliance of the environment."[5]

Scale, Scope, and Complexity

In cloud computing, one physical machine typically hosts many VMs, which drastically increases the number of hosts to be audited. Unless carefully managed, the sheer number of these VMs could overwhelm IT staff and auditors. However, when standardization is in place (for instance, in the form of master VM images verified for security), the auditing process can go smoother and faster despite cloud computing elements' larger scale.

Another factor to consider is the scope of auditing. Whereas the scale problem results from the increased number of IT elements to audit, the scope factor emerges mainly due to the new technology types to audit in cloud computing. For example, examining hypervisor security is much more important when dealing with CSPs owing to the colocation problem. If a hypervisor has a vulnerability that threatens the strict separation among VMs, CSUs will be uncomfortable with their VMs being adjacent to those belonging to other organizations, including their competitors. In addition, many cloud environments have intangible and logical elements to audit, including virtual switches and firewalls. Therefore, auditors must be aware of both subtle and obvious differences in the cloud-specific technologies that could threaten the security of CSUs.

Due to the increase in both scale and scope, the complexity of the systems also increases. Cloud auditors should take this complexity into account, allocating more time and resources than in a traditional IT auditing process.

In addition, cloud computing makes it possible for a CSP to store an organization's data and information at its datacenters located in multiple countries. These countries apply varying laws and regulations, so the client organization's compliance requirements are no longer bound to the CSU's physical location. Therefore, it's crucial that cloud security auditors find out where the CSP stores CSU data and information. Colocation due to multitenancy also contributes to the importance of the physical data and information storage location.

Domains to Consider

Cloud computing offers a large umbrella of services that can be accessed anywhere. However, certain fields of business in different domains will have various needs of their own. Data types can also vary among domains, as can the legal and regulatory requirements mandated for keeping that data safe. Consequently, a one-size-fits-all audit might not satisfy all the needs that a specialized audit should. Domain-tailored audits are an ideal solution.

Medical Domain

Hospitals, doctors' offices, and medical specialists are beginning to use various cloud-based software applications that allow the sharing of patient information with other healthcare professionals. The medical domain holds highly sensitive and confidential information but must allow access by auditors, patients, pharmacies, and other institutions such as hospitals. A sophisticated authentication method is especially essential to the medical cloud, both legally and ethically. Any breach could result in an extreme loss to both the medical organization and their patients.

Legally, the medical domain is held to a very high standard, facing large compensatory as well as punitive costs in the case of a breach. Several legal standards exist to protect patients and regulate healthcare organizations, including the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, the Food and Drug Administration Amendments Act (FDAAA), and the American Recovery and Reinvestment Act (ARRA) of 2009.

Consequently, the medical domain requires a specifically tailored audit approach to comply with these legal standards. A medical-domain cloud security audit must thoroughly evaluate both the medical organization and the cloud containing its information.

CipherCloud describes itself as an organization dedicated to allowing other organizations to reap the benefits of the cloud, which they otherwise wouldn't be able to due to concerns about data security, privacy, residency, and regulatory compliance.[6] CipherCloud announced that Medical Audit & Review Solutions (MARS) had used its encryption infrastructure to create a hybrid MARS PROBE Platform,[6] thus forming a more comprehensive and secure auditing

approach. The MARS PROBE Platform itself is cloud based, and it might prove to have the power to effectively audit medical organizations and satisfy the demands of both HIPAA and HITECH. This example demonstrates the need for cooperation among different organizations to tackle the demands of cloud security auditing in the medical domain. We expect similar hybrids in the near future.

Banking Domain

Banks have a lot of traffic related to users accessing services from various devices around the clock. Banks must not only update information incessantly but must also keep this information secure and available to all clients who want access. Yet, despite the apparently daunting task of constantly updating and securing sensitive data, banking in the cloud holds great potential. Benefits include the sharing of information among banks if a client has multiple accounts as well as cost reduction. TEMENOS Online aims to eliminate large overhead expenses for small banking institutions, which would result in lower interest rates.[7]

Although perfect security is impossible, security systems must be able to resist as well as respond to breaches, especially when billions of dollars and numerous bank accounts are at risk. A big problem relatively large banking clouds face is ensuring that client information can't be stolen or sold. In our opinion, the safeguards need to be twofold. First, data stored in the cloud should be encrypted. Second, access to it should be limited by permissions set by the online banking client.

A traditional IT audit of a bank that stores its data locally (or at the bank's headquarters) usually doesn't need to worry about other banks reaching the data. However, when multiple banking institutions use the same cloud infrastructure, there are additional risks, including the possibility of unintended access to banking data by competitors. In addition, a security breach of one bank might result in the breach of other banks' accounts.

Government Domain

The government is also entering the cloud domain.[8] Maintaining security of and auditing the CSPs is even more important in the government sector due to the sensitive nature of its data and information. To authenticate, authorize, and audit CSPs, government agencies use the Federal Risk and Authorization Management Program (FedRAMP), which performs ongoing assessment of cloud providers.[8]

The three key areas of auditing are *operation visibility*, *change control process*, and *incident response*. Operation visibility requires that CSPs submit automated data feeds to the agencies along with periodic evidence of system performance and annual reports. Change control process restricts CSPs' ability to make policy changes that might affect FedRAMP requirements. Finally, incident response deals with new possible risks or vulnerabilities in the cloud system as well as protects government information against leaks in the event of a breach. For instance, if an attack compromises a government computer and causes military secrets to be exposed, an incident response team should stop the information leakage immediately and prevent any further damage.

Emerging Approaches

To be effective, both cloud computing and traditional IT security audits must conform to some form of standard; we believe this is where cloud computing finds its biggest growth potential. Unlike traditional IT security audits, cloud computing security audits don't have comprehensive certifications to cover their vast number of security concerns. Therefore, cloud security auditors often use a traditional IT security audit standard to make an evaluation.

In our interviews with professional cloud security auditors, we found three primary schools of thought regarding cloud security auditing standardization. One is a belief that we don't need a new standard at all. Because most traditional IT auditing standards are technology neutral by design, existing standards are still relevant. Auditors are responsible for developing their expertise in cloud computing on their own and gaining insights by simply doing it. Another school of thought is to keep the technology-neutral nature of the well-known IT security auditing standards but supplement them with cloud-specific information, for example, what to look for or avoid when conducting a typical cloud security audit. Finally, some interviewees wanted to develop an entirely new standard dedicated to cloud security auditing. In our opinion, the supplement approach is a great compromise.

One of the most widely used IT security auditing standards is the ISO 27000 series. The ISO 27001 and ISO 27002 auditing standards have a long history; ISO 27002 is based on a document published by the English government in 1995.[9] The ISO 27000 official website lists current audit standards whose coverage varies from internal audits to management responsibility, from security policy to physical security, and from access controls to compliance. For a traditional IT security audit, these kinds of controls fit well as all these concerns exist inside the organization itself.

However, for organizations using the cloud, ISO 27001 and ISO 27002 can provide only limited support. As we discussed earlier, in this case an audit's quality depends heavily on the auditor's cloud computing experience and knowledge, which could be problematic. For example, ISO 27000 series' encryption

Table 2. Standards applicable to cloud security auditing.

Standard	Type	Strength	Sponsoring organization
Service Organization Control (SOC) 2	Audit for outsourced services	Technology neutral	American Institute of CPAs
ISO 27001 and 27002	Traditional security audit	Technology neutral	ISO
NIST 800-53 rev. 4	Federal government audit	Technology neutral	National Institute of Standards and Technology
Cloud Security Alliance (CSA)	Cloud-specific audit	Dedicated to cloud security auditing	CSA
Payment Card Industry (PCI) Data Security Standard (DSS)	PCI Qualified Security Assessor cloud supplement	Cloud specific and provides guidance	PCI DSS

section simply states that "a policy on the use of cryptographic controls for protection of information shall be developed and implemented" and that "key management shall be in place to support the organization's use of cryptographic techniques."[10] There's no mention of the different encryption scenarios cloud auditors must understand to do their job effectively. The same is true for other critical factors of cloud security auditing, such as transparency, colocation, scale, scope, and complexity, because many of these problems arose after the drafting of ISO 27001 and ISO 27002. As of this writing, ISO is developing a new cloud-specific security standard—ISO/International Electrotechnical Commission (IEC) 27017—to address this problem.

Unlike the technology-neutral approach, PCI DSS has the Qualified Security Assessor cloud supplement to guide auditors handling PCI DSS certifications in the cloud computing domain.[5] In terms of organizations preparing to directly tackle the issues associated with cloud security auditing, the Cloud Security Alliance is using best practices to educate practitioners and help secure the many forms of cloud computing. Because CSA is a nonprofit, independent organization, it can contribute to various cloud security groups and has come to encompass other smaller cloud interest groups. One such group is CloudAudit, which lists its goals as automated audit, assertion, assessment, and assurance of the cloud system while being "simple, lightweight, and easy to implement" and supported entirely by volunteer efforts.[11] CSA and its member groups aren't tied to a specific organization or standard, meaning they're free to cover all aspects of cloud computing in the forms of SaaS, PaaS, IaaS, and many more services. Moreover, this system based on volunteer efforts is reminiscent of the origins of the Internet Engineering Task Force (www.ietf.org), one of the most important protocol-creating organizations in the realm of computer networking.

Table 2 summarizes a wide spectrum of standards and their coverage of cloud security auditing. Although not specifically mentioned in this article, Service Organization Control (SOC) 2[12,13] and NIST 800-53 revision 4[14] are similar to the current ISO 27000 series in that they don't have built-in cloud-specific provisions in their standards. Unlike NIST 800-53 revision 4, NIST 800-144 offers specific guidelines on security and privacy in public cloud computing.[15]

Our future research will focus on improving the existing cloud security auditing approaches discussed in this article. Another goal is to identify more challenges that clearly differentiate cloud security auditing from traditional IT security auditing by conducting a formal survey of various stakeholders in the cloud security auditing community. The more comprehensive the list of the cloud security auditing challenges, the more educated cloud security auditors will be and the more thorough and reliable the audit results will be. ■

Acknowledgments

We consulted many cloud security auditing practitioners while working on this article. In particular, we acknowledge the help and advice provided by Douglas Barbin, principal (shareholder) at BrightLine CPAs & Associates, and Robert Sweeney, internal IT auditor at the Hershey Company. Their insights were indispensable in completing this article.

References

1. P. Mell and T. Grance, "The NIST Definition of Cloud Computing," NIST special publication 800-145, 2011; http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.
2. D. Cannon, *Certified Information Systems Auditor Study Guide*, 3rd ed., Wiley, 2011.
3. W.A. Pauley, "Cloud Provider Transparency: An Empirical Evaluation," *IEEE Security & Privacy*, vol. 8, no. 6, 2010, pp. 32–39.
4. C. Gentry, "A Fully Homomorphic Encryption Scheme," PhD dissertation, Dept. Computer Science, Stanford

Univ., Sept. 2009; http://crypto.stanford.edu/craig/craig-thesis.pdf.
5. "Information Supplement: PCI DSS Cloud Computing Guidelines," Cloud Special Interest Group PCI Security Standards Council 2013; https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf.
6. "CipherCloud Enables Healthcare Pioneer to Deliver a Medical Audit Solution," CipherCloud, 16 May 2012; www.ciphercloud.com/company/about-ciphercloud/press-releases/ciphercloud-enables-healthcare-pioneer-deliver-medical-audit-solution.
7. "Banking in the Cloud," TEMENOS, 2011; www.temenos.com/temenos-online/banking-in-the-cloud.
8. "FedRAMP: Ensuring Secure Cloud Computing for the Federal Government," US General Services Administration, 20 Nov. 2012; www.gsa.gov/portal/category/102371.
9. "An Introduction to ISO 27001, ISO 27002 ... ISO 27008," The ISO 27000 Directory, 2009; www.27000.org.
10. ISO/IEC 27001:2005, A. 12.3.2, International Organization for Standardization, 2005.
11. "CloudAudit: Automated Audit, Assertion, Assessment, and Assurance," CloudAudit, 12 Feb. 2010; http://cloudaudit.org/CloudAudit/About.html.
12. "Reporting on Controls at Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2)—AICPA Guide. January 2012," American Institute of CPAs, 2012.
13. "Service Organization Control (SOC) Reports," American Institute of CPAs, 2013; www.aicpa.org/interestareas/frc/assuranceadvisoryservices/pages/sorhome.aspx.
14. "Recommended Security Controls for Federal Information Systems and Organizations. NIST Special Publication 800-53 Revision 4," Nat'l Inst. Standards and Technology, 2009; http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.
15. W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing," Nat'l Inst. Standards and Technology, Dec. 2011; http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf.

Jungwoo Ryoo is an associate professor of information sciences and technology at the Pennsylvania State University–Altoona. His research interests include information assurance and security, software engineering, and computer networking. Ryoo received a PhD in computer science from the University of Kansas. He's a member of IEEE and the ACM and a technical editor of *IEEE Communications Magazine*. Contact him at jryoo@psu.edu.

Syed Rizvi is an assistant professor of information sciences and technology at the Pennsylvania State University–Altoona. His research interests lie at the intersection of computer networking, network security, and modeling and simulation. Rizvi received a PhD in modeling and simulation from the University of Bridgeport. He's a member of the IEEE Communications Society and the ACM. Contact him at srizvi@psu.edu.

William Aiken is a student at the Pennsylvania State University–Altoona, majoring in security and risk analysis. His primary research interest is information security management systems auditing, particularly in cloud computing. Contact him at wva5029@psu.edu.

John Kissell is a student at the Pennsylvania State University–University Park, majoring in security and risk analysis. His primary research interests include cloud computing, with a special emphasis on security and issues with legal and regulatory compliance. Contact him at jzk5354@psu.edu.

Letters for the editor? Please email your comments or feedback to editor Brian Kirk (bkirk@computer.org). All letters will be edited for brevity, clarity, and language.