S|3 SPECIALIZED SECURITY SERVICES

FIVE PILLARS OF CYBERSECURITY COMPLIANCE

FIVE PILLARS OF CYBERSECURITY COMPLIANCE

Foundations for Successful Assessments

There is a myriad of regulatory and compliance frameworks which drive common assessments you encounter. That's old news. But at their core are five components that, if executed well, will position your organization to successfully navigate any assessment you encounter. This whitepaper outlines a set of IT controls that provides a foundation for many common control frameworks, including SOX, PCI, NIST, ISO, HIPAA and FISMA.

1. IT Governance
2. IT Change Management
3. Logical Security
4. Security Administration
5. IT Operations

1. IT GOVERNANCE

A compliance program is an entity's set of internal policies, procedures, processes and internal controls put into place in order to comply with laws, regulations, rules or requirements for the business subject. A compliance program is made up of five components, and the first of these is governance.

Governance provides a framework for scoping, managing compliance activities (including risk assessment), policy development, training, monitoring and reporting. Scoping identifies the laws, regulations, rules or requirements that are included in the compliance program. Scoping can also be applied to the assessments of compliance by determining which areas each specific assessment of compliance is to include. Managing compliance activities includes identifying the initial steps to develop a compliance program (as outlined below), as well as an ongoing plan of action (i.e., road map, remediation plan.) The use of risk assessment in developing the plan of action assists in prioritizing individual actions.

Development of policies, procedures and processes is an initial step in defining how compliance will occur. Once developed, these policies, procedures and processes must be periodically reviewed and maintained. Training of entity personnel on these aspects must occur to ensure everyone knows how to comply. Once training has occurred, monitoring of entity compliance should occur on an ongoing basis. Such monitoring should be viewed with an eye on key performance indicators to provide reporting to the Executive Management of the entity. Reporting should be performed on a regular basis (i.e., monthly) with significant exceptions being reported.

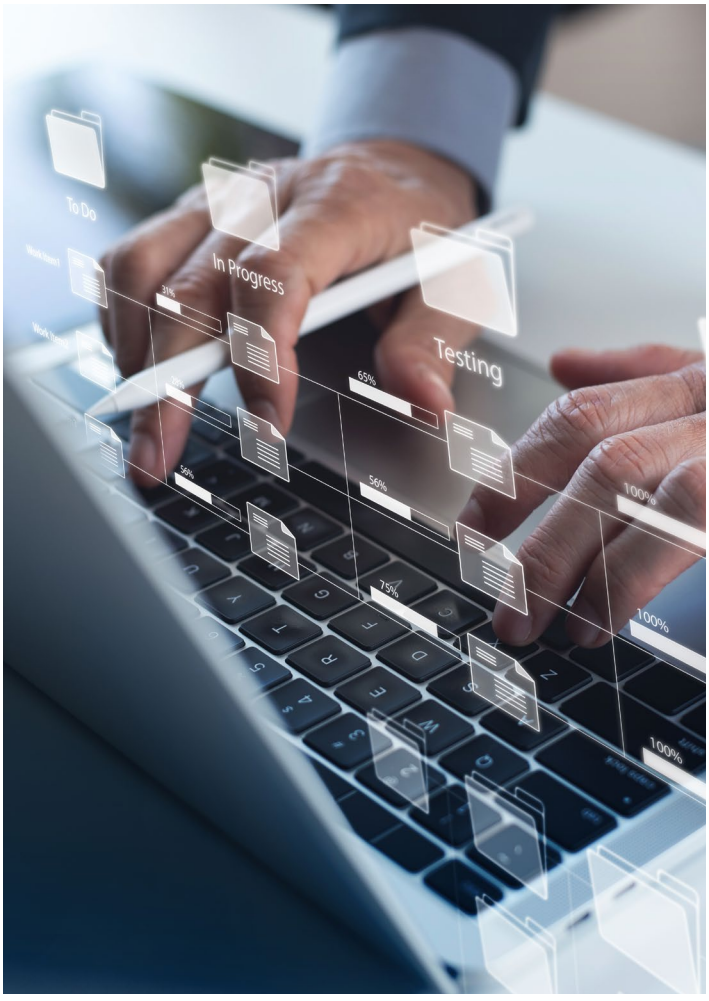
It should go without saying that an underlying governance requirement for any credible compliance program is obtaining entity leadership support. Without appropriate executive leadership behind the compliance program, it will be difficult to obtain needed funding, implementation of policies/procedures and enforce consequences of non-compliance.

2.IT CHANGE MANAGEMENT

In Information Technology, general computing controls for change management are vital to ensure the integrity and security of systems and data. Change management governs the process of implementing alterations to IT systems, including updates, patches and configuration changes. Robust controls involve effective procedures to authorize, document, manage and monitor these changes. This encompasses ensuring change requests undergo appropriate review and approval processes, changes are implemented by authorized personnel, and that adequate documentation is maintained throughout the process. Additionally, mechanisms should be implemented for tracking changes, assessing their impact and mitigating associated risks, such as potential disruptions to service or security vulnerabilities.

Change management functions should also include evaluating the segregation of duties to prevent conflicts of interest and unauthorized alterations. This involves making sure there are clear distinctions between roles and responsibilities for requesting, authorizing, implementing and reviewing changes. Effective segregation of duties helps prevent unauthorized or inappropriate modifications to IT systems, and reduces the risk of errors, fraud and security breaches.

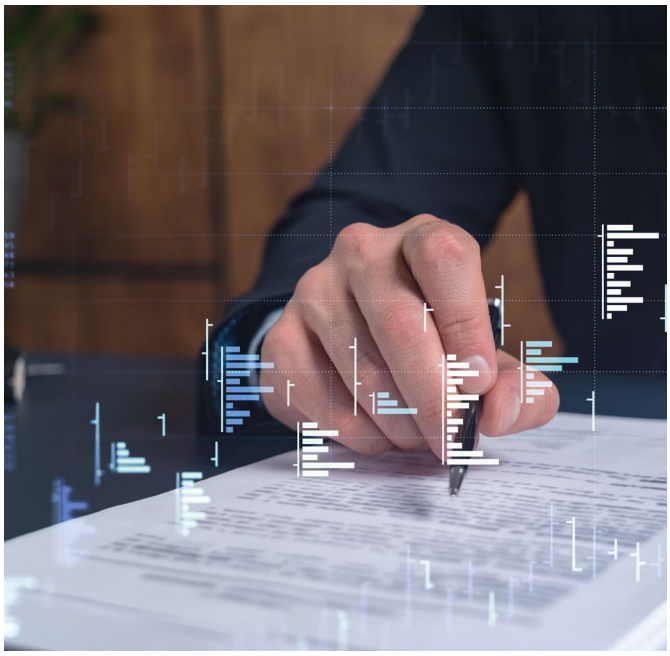
The change management process should provide adequate coverage for emergency changes, ensuring there are mechanisms in place to address critical issues promptly, while still adhering to proper authorization and documentation procedures. By implementing effective change management functions, organizations can enhance their ability to manage IT changes efficiently while maintaining the integrity, availability and confidentiality of their systems and data.



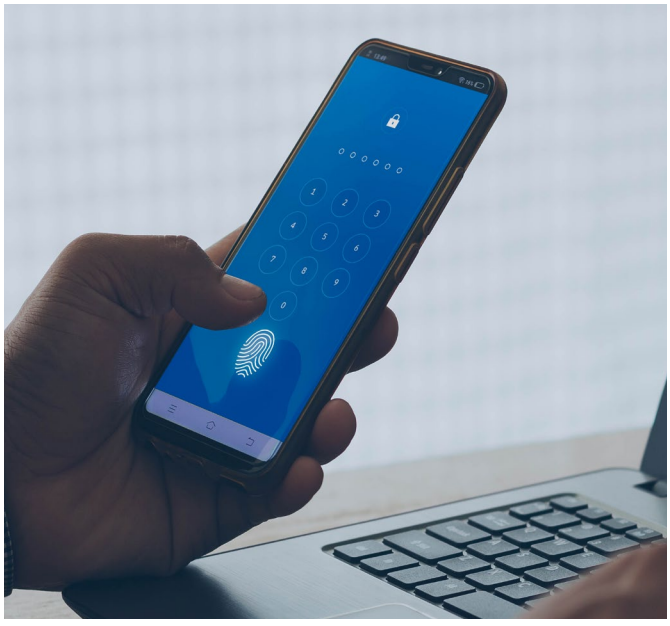
3. LOGICAL SECURITY

Logical access controls also protect the integrity, availability and confidentiality of data and assets by establishing processes to limit access within a system (both logical and physical) to appropriate personnel and manage the means by which users authenticate to said assets.

Fundamentally, the first step in effectively implementing logical security controls is to document and publish an Information Security Policy (ISP) that aligns with the IT Strategic Plan and direction of the business. Your ISP should determine the standards for how people, processes and technologies will be stood up and maintained, including roles and responsibilities; use of super user and administrative accounts; group and account naming standards; password standards; account creation and termination; access review requirements; and expectations for the monitoring and resolution of security violations.



Various information systems provide the abilities to grant system access in many different ways. As such, it's critical to establish standards for user, system and privileged accounts, define how access will be provisioned, and outline how system and privileged accounts are to be used. System users should be assigned unique user IDs to enable accountability and traceability of user activity. User accounts should be restricted to only viewing, editing or deleting data which is necessary for that user's job function. Accounts tagged with privileged access should be subject to



defined approvals and user access reviews, as well as segregation of duties reviews.

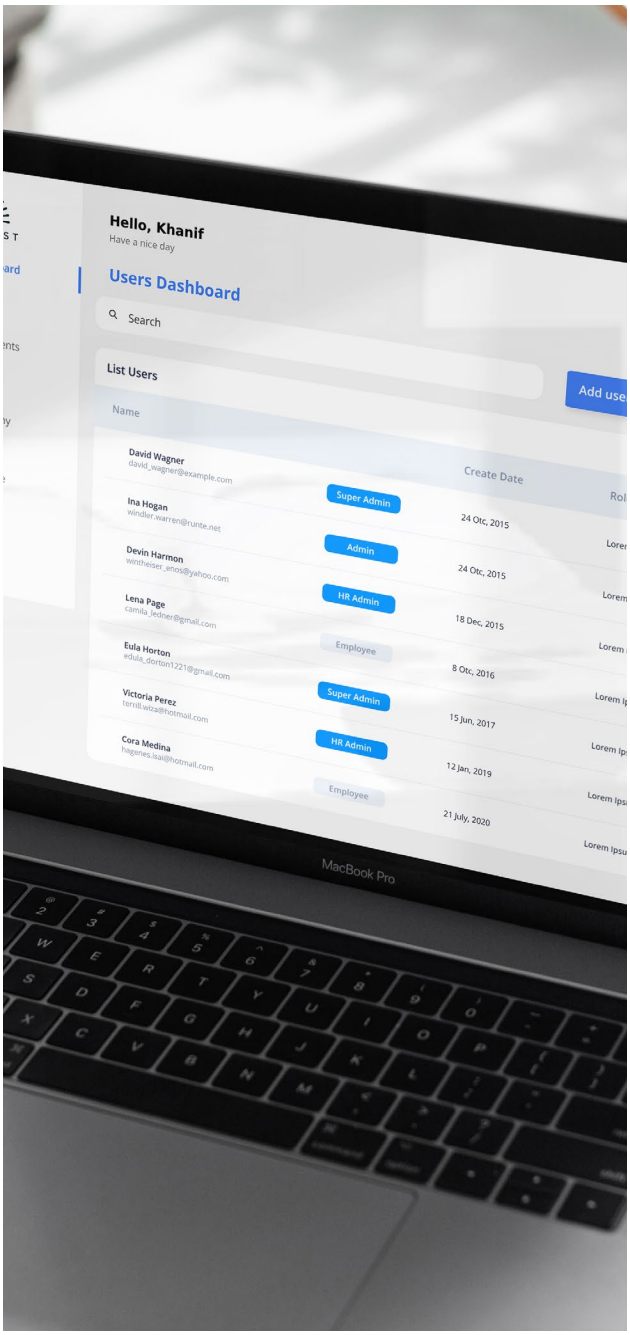
Strong authentication and access mechanisms (password rules, MFA, tokens, etc.) should be implemented on all user, system and administrative accounts to effectively ensure authorized use and the integrity of data.

Finally, effective logical security controls include monitoring processes to identify and respond to security events. Generally, this will involve implementing logging and monitoring tools, specifically to record information related to key transactions within a system. Perhaps most critically, implementing log on to a system is of no use unless monitoring processes are established for identifying inappropriate activity (including who performed it and when) and responding timely to such events.

4. SECURITY ADMINISTRATION

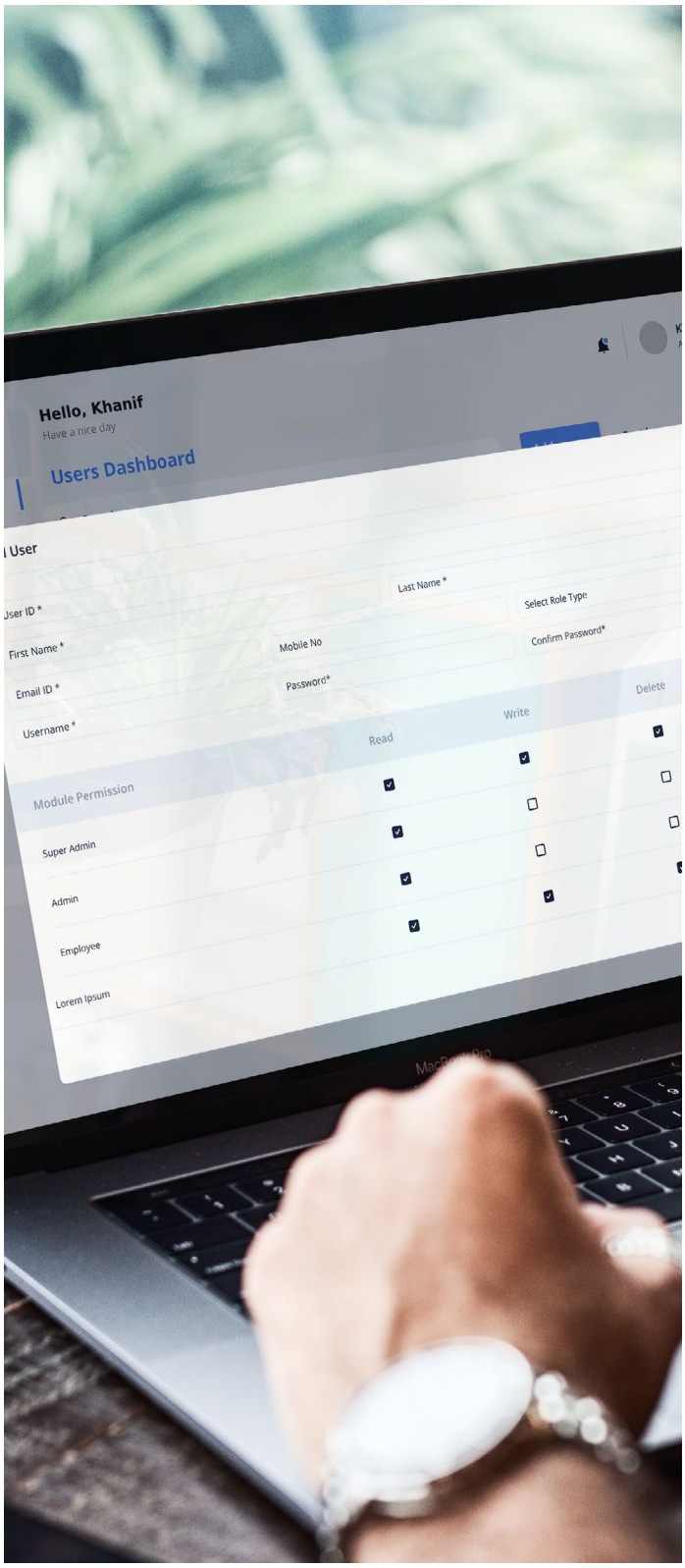
Another important component of compliance is Security Administration – which is comprised of three main activities: 1) Access Provisioning, 2) Access Revocation, and 3) Access Review.

The access provisioning process is also comprised of three basic activities: Access Request, Approval/Denial and Implementation. The key phrase for access provisioning is least privilege. In other words, users only receive permissions essential to perform their job tasks. Access requests should include the name of the individual, specific access/privileges being requested, their position or job title, and the date access is to be available.



Access requests are typically initiated by HR or the individual's supervisor/manager. The decisioning step – Approval/Denial – is the responsibility of someone who has been authorized to perform that task. Approvers are responsible for ensuring the access requested aligns with the responsibilities of the position held by the individual receiving access.

Implementation, if approved, results in account creation and assignment of access privileges. Implementation is the responsibility of an administrator whose elevated privileges allow them to create accounts and assign access privileges. On the surface, Access Revocation is generally the opposite action of access provisioning. But there are nuances in the process which can create some challenges. The key word for access revocation is timeliness. Timely disablement of access



and timely removal of accounts are the goals for this process. There are also three steps to access revocation: Removal Request, Approval and Implementation.

The request for removal of access should include the name of the individual, their job title/role, their potential access, and the date access is to be removed. Approval for access revocation is a little simpler than an access request. Approvers should validate timing of removal to ensure timeliness, as well as the access list included in the request to assess completeness. Like provisioning, implementation is the responsibility of an administrator with elevated privileges which allow them to disable accounts and either remove access privileges or delete the account.

Account removal can be a multi-step process, making it difficult to balance needs of the business and strict adherence to policy. For example, work transitions may require access that spans multiple jobs rather than a single job requirement. Conversely, a separation may require a span of time to review documentation/ information before access can be fully removed to avoid losing original/critical content, IP, etc. Accounts are disabled or rendered unable to accept an interactive login immediately and then, after a defined period of time, the accounts are deleted. But some systems do not allow removal of accounts for various reasons.

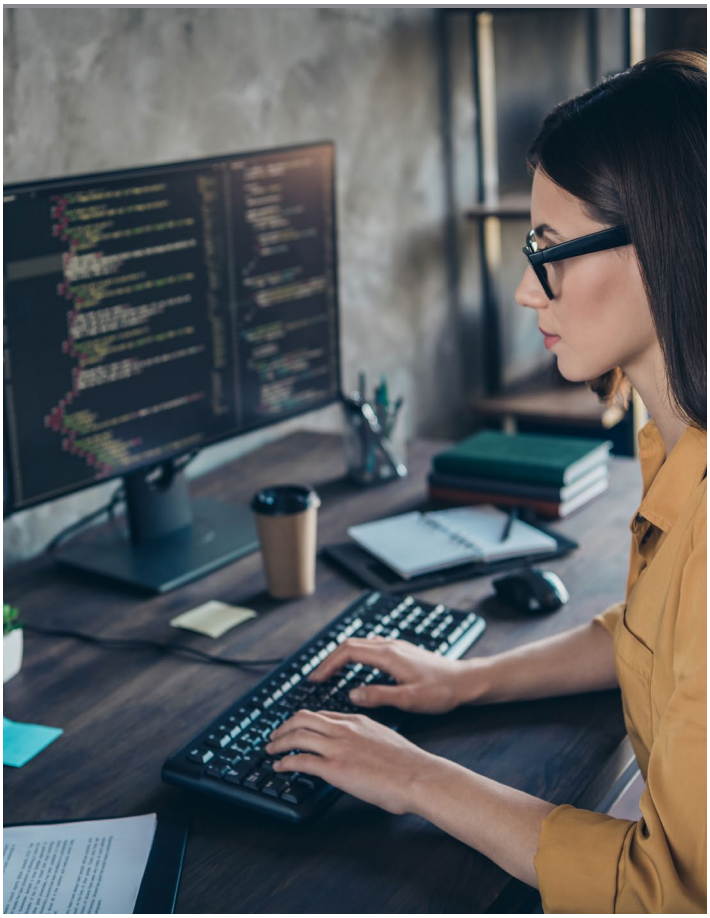
The third step in security administration – Access Review – involves documenting the reconciliation of accounts and the privileges/access of individuals. Activities include the collection of access/privileges, identification of individuals with access, evaluation of appropriateness, recommendations of changes, and implementation of changes.

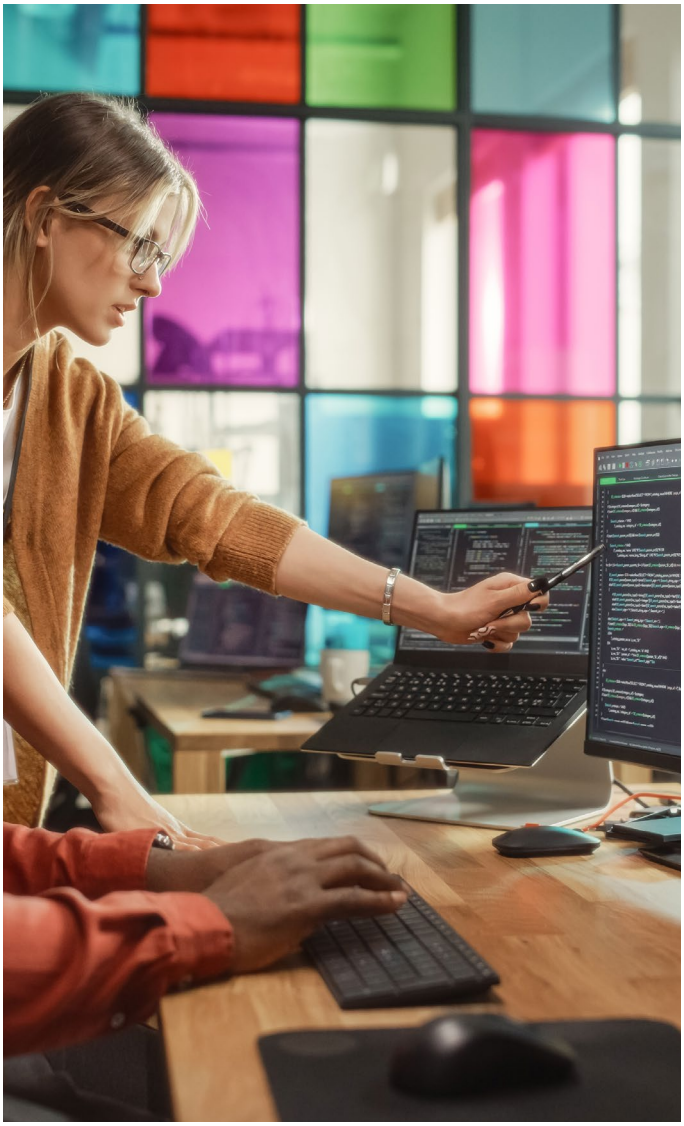
The goal of access review is to ensure the individuals with access are appropriate and that the privileges assigned to them align with the responsibilities of their job. In order to meet that goal, the person charged with performing the review needs to acquire three things: 1) A list of access/privileges for the target system, 2) A list of individuals and their job titles, and 3) Knowledge of job responsibilities and/or access required to perform a job. Understanding job requirements and access required to perform them is critical to the success of the review. Shared accounts, service accounts and default accounts can all create challenges during the review process and require additional documentation to connect them with a named individual.

5. IT OPERATIONS

Overall, IT Operations controls refer to the policies, procedures and mechanisms implemented within an organization to ensure the effective and secure management of its IT infrastructure and systems. These controls are essential for maintaining the availability, reliability and integrity of IT services, as well as for managing risks and supporting the organization's overall strategic objectives. A few key areas include Monitoring & Alerting functions, Back-up & Recovery, and Documentation.

Monitoring and alerting are critical components of IT general controls (ITGCs) that help ensure the security, availability and integrity of IT systems and data. Monitoring and alerting should cover critical IT infrastructure such as servers, databases, network devices and applications. Establishing appropriate thresholds and performance baselines is critical to avoid alert fatigue (too many false positives), while defined escalation procedures ensure alerts are addressed according to their severity and impact. Increased automation adoption and the use of third-party services can be effective options here, helping reduce response times and improve overall effectiveness. But it is still critical to avoid sole reliance on these services and retain subject matter expertise along with regular reviews and testing.





Operational backup and recovery policies – including procedures for data backups, storage and recovery processes – are back in the spotlight. With today's landscape of cyberattacks (ransomware, etc.), the effective segmentation of backups, retention standards and access controls helps ensure backup integrity is available to address worst-case scenarios when mitigating business risks. Besides adherence to regulatory requirements and industry standards, regular testing of these functions is critical to ensure backup integrity is available to facilitate any business continuity effort.

Lastly, foundationally strong documentation policies and procedures are critical to establishing a baseline that provides clarity, completeness and relevance to the organization's operations. Once established, maintenance through regular reviews and updates helps documentation remain current and reflect any changes in IT systems or organizational processes.

CONCLUSION

In summary, organizations that demonstrate proficiency with these five components are in a strong position to successfully navigate many common assessments. More importantly, they've established a foundation for securing and protecting their information, processing data securely and reliably, efficiently managing change and effectively governing their IT environment.

Of course, many of these organizations have one more thing in common: They have S3 Security standing behind them. For 25 years, our team has specialized in assessing the potential impact of new regulations, crafting tailored solutions that address the unique aspects of your business, and providing continuous support that ensures successful strategies. When you partner with S3 Security, you gain access to a wealth of proven expertise, relevant experience and practical resources that help you mitigate risk, enhance your cybersecurity posture and achieve compliance with confidence.

LEARN MORE ABOUT CYBERSECURITY ASSESSMENTS

S3SECURITY.COM | 972-378-5554