Streamlining Vendor IT Security and Risk Assessments:

A PERSPECTIVE ON STANDARDS-BASED ASSURANCE OF CLOUD PROVIDERS

A CLOUD SECURITY ALLIANCE AND NATIONAL TECHNOLOGY SECURITY COALITION WHITEPAPER

CSA cloud security alliance®

NTSC NATIONAL TECHNOLOGY SECURITY COALITION

THANK YOU

The Cloud Security Alliance (CSA) is a not-for-profit, member-driven organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, certification, events and products. CSA's activities, knowledge, and extensive network benefit the entire community impacted by cloud — from providers and customers, to governments, entrepreneurs and the assurance industry — and provide a forum through which diverse parties can work together to create and maintain a trusted cloud ecosystem.

CSA research prides itself on vendor neutrality, agility and integrity of results. I would like to thank our sponsor, the CIO/CISO Interchange, for helping fund the development of this CSA Research Artifact. The CIO/CISO Interchange is a partner organization that supports the findings of the research project but have no added influence on the content development or editing rights of CSA research.

Sincerely,

Luciano (J.R.) Santos
Executive Vice President of Research at CSA Global

https://www.cio-ciso-interchange.org/

ACKNOWLEDGEMENTS

Lead Author
Jim Reavis
Patrick Gaul
Pete Chronis

Contributors
Aaron Guzman

CSA Staff
AnnMarie Ulskey
Frank Guanco
Hillary Baron
John Yeoh
J.R. Santos
Sean Heide

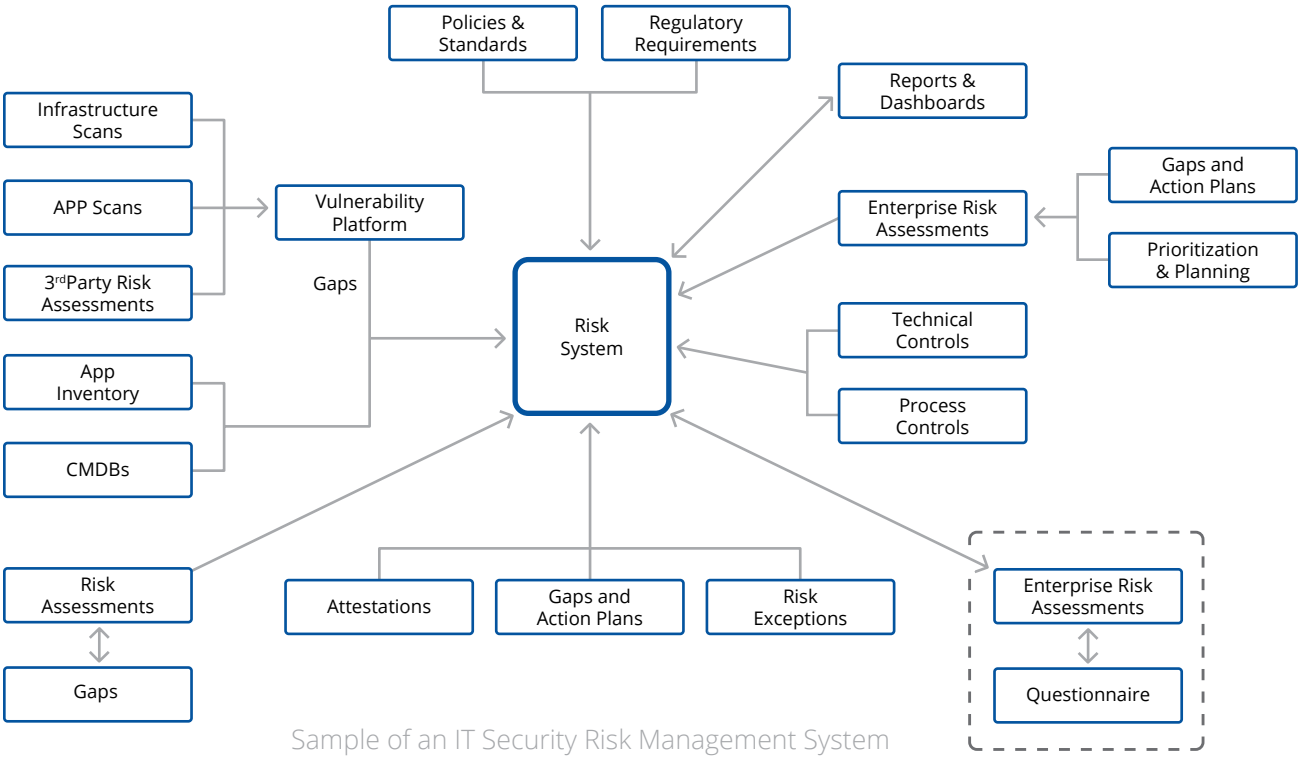
STREAMLINING VENDOR IT SECURITY AND RISK ASSESSMENTS: A PERSPECTIVE ON STANDARDS-BASED ASSURANCE OF CLOUD PROVIDERS

Contemplating the numerous threats to a company's technology assets quickly becomes overwhelming. To respond, technology and business leaders try to enumerate and manage risk. However, developing a comprehensive IT risk management program often eludes and remains beyond the reach of many organizations. Pressures to more quickly release products to market along with navigating the complexities of conducting assessments and remediation work makes comprehensive risk management difficult.

Despite this common challenge across companies, few alternatives exist to help those companies manage cybersecurity, intellectual property, regulatory compliance, and privacy risk. Most IT security risk management methodologies include several core principles. Using NIST 800-39 as an example, those principles include:

- **Framing:** Risk framing sets the rules for a company's program including scope, roles, responsibilities, setting enterprise risk tolerances, etc.
- **Assessing:** Assessing involves developing and executing plans to assess risk. These plans include remediation options that accountable parties can evaluate.
- **Responding / Accepting:** This principle generally involves taking action to remediate enterprise risk, including accepting the risk "as is" or accepting it after some remediation activities. Because of some action or actions taken to reduce risk, remediation may result in residual risks.
- **Monitoring / Reviewing:** Continuous risk monitoring and review by key stakeholders or third parties is a key component of any risk management program.

Despite the rigor of such an overall program, it's not complete unless the program also includes third-party technology vendors and service providers that form part of a company's technology ecosystem. However, vendor security assessments generally consume a lot of time and cost while resulting in a limited understanding of a vendor's risk profile. These inefficient assessments have trouble keeping up with the growing ecosystem of technology vendors—and especially the increased reliance on cloud security vendors. In such an ecosystem, technology leaders must redouble their efforts to improve vendor security oversight, risk assessment, and risk management activities.



Sample of an IT Security Risk Management System

Cloud computing has rapidly gained traction as a significant and even default IT system for many different organizations. For some, cloud has become the foundation for digital transformation, leading to a rapid acceleration in the use of this technology and highly dynamic, software-defined configurations. In such a dynamic environment, cybersecurity is paramount—especially with third parties that provide cloud or cloud-based services to companies. This new era of technology dependence on cloud has placed enormous strain on how IT is governed, regulated, and secured.

In this paper, the Cloud Security Alliance (CSA) and the National Technology Security Coalition (NTSC) are advocating for a new approach to how organizations manage risks, achieve assurance, and enable trust in the cloud. To achieve this end, we believe it is imperative that all stakeholders in this ecosystem increase their level of collaboration while utilizing existing standards and open tools.

As a critical step toward securing the digital foundation of our economy, we recommend that businesses reduce their reliance on proprietary, in-house security assessment programs related to cloud computing. Instead, we recommend leveraging the CSA's Security, Trust & Assurance Registry (STAR) program and its associated assurance tools as core components of vetting and procuring cloud providers and services. We believe this emphasis on consistent, uniform cloud security standards will increase the security baseline for all participants in our economy.

We encourage CISOs, governments seeking to regulate information technology, and other stakeholders to review this paper and provide us with your feedback.

CLOUD AND THE FUTURE OF DIGITAL TRANSFORMATION

Cloud computing is a global compute utility replacing the notion of purchasing, installing, and managing physical computers and data centers with pay-per-use, on-demand usage of publicly available compute resources. Any individual or organization with a new idea and a credit card can immediately gain access to the world's largest data centers.

Cloud originally ascended to prominence as a new business model with relatively mature technology: virtualization and internet access. As cloud has grown, innovators have developed many new technologies and architectures that are significantly changing cloud such as:

- **Containers and Microservices** – These are complementary technologies that provide lightweight abstractions of operating systems, greatly simplifying management and application development in the cloud.
- **Software-Defined Networking** – This makes cloud-based transport networks completely virtual and programmable.
- **Microsegmentation** – This involves implementing fine-grained security controls to isolate workloads in the cloud. A version known as Software Defined Perimeter shows the potential to create highly secure Virtual Private Clouds.
- **DevOps** – DevOps is a merging of software development and operations which, when combined with the above technologies and cloud-specific tools, changes how organizations develop, deploy, and secure business applications.

In addition, several other important technology trends are becoming mainstream that relate closely to cloud:

- **Internet of Things (IoT)** – This is a trend toward compute-enabling virtually any physical item. IoT scales exponentially with cloud architecture and management.
- **Artificial Intelligence/Machine Learning** – Long standing computing theories are gaining much traction and implementation due to the increase in compute made available by the cloud and the need to manage an exponential growth in information.
- **Blockchain** – This transaction logging technology underlying cryptocurrencies is finding several new applications as an immutable distributed ledger system.

Many businesses adopt cloud technologies and solutions as part of their digital transformation, leading to a fundamental rethinking of the structure and processes making up the modern enterprise. This digitally transformed enterprise is highly dynamic, software-defined, and automated to a far greater extent than most organizations today. In this context, cybersecurity best practices need to significantly change to protect the digitally transformed enterprise.

SECURITY EVOLUTION AND PRIVACY

Historically, information security evolved in organizations as an outgrowth of corporate physical security. Taking a completely organizational-centric view of protecting its mission and assets, information security, like physical security, worked similar to the history of fire brigades where a private fire department would protect a building under contract while letting the building next door burn to the ground. In the same way, businesses prioritized information security within a company in isolation.

Two milestones changed this worldview:

- **The commercialization of the Internet.** As the Internet connected organizations' computers together, businesses felt the impact of another organization's poor computer security hygiene. As businesses became more IT-driven, they began extending security requirements into their supply chains to create a consistent security standard across interdependent organizations.
- **Critical infrastructure protection (CIP).** In 1998, Presidential Directive (PDD) 63 designated several industries as critical to the survival of the nation. This was a recognition that a business in a critical infrastructure industry has a responsibility to be resilient even if its customers are not mandating security within their vendor procurement processes. In the 20 years since the enactment of PDD-63, an increasing amount of enumerated risks to critical infrastructure have been related to cybersecurity. The White House through its National Cyber Strategy released in September 2018, the Department of Defense's updated version of its cyber strategy (the first since 2015), and DHS's new National Risk Management Center are just a few of the latest steps the federal government has taken to more rigorously promote and support critical infrastructure protection in the wake of such increased threats.

As cloud computing moves to the forefront of an enterprise, it amplifies a few key trends that are driving important shifts with information security best practices:

- **Shared responsibility.** As the cloud represents "someone else's computers", security becomes a shared responsibility between the customer and cloud provider. The responsibility demarcation is often explicitly stated in contracts or service level agreements (SLAs). There's a very important implication of the shared responsibility model that often goes unmentioned - namely that there are important security control implementation and operational responsibilities that the customer has to execute, both before using the service (i.e. during service implementation) and ongoingly thereafter.
- **The leveraging of indirect security assurance tools.** Lacking direct physical control over cloud computers and data centers, risk management in the cloud requires greater utilization of indirect measurement methods such as carefully examining contracts, audits, certifications, and compliance statements made available by the cloud provider.
- **Continuous compliance.** Cloud software is highly dynamic and may be updated several times a day, making it important that customers have nearly real-time monitoring of security and compliance between continuous assessments, point-in-time audits, and certifications.
- **Inherited compliance.** The cloud's rapid development and reliance upon APIs means that any cloud service may be a "mashup" of several different cloud applications and providers. Customers need ways to ascertain that a cloud service inherits the optimal security controls of each disparate cloud provider, and that the service and applications work in an integrated

fashion to avoid gaps or misalignment of controls.

- **Country-specific data sovereignty and compliance.** Recently, China enacted its version of a Cybersecurity Law that identifies 'critical infrastructure' specific to state directives and strategic plans. Multi-nationals with shared infrastructure clouds must be cognizant of these data sovereignty laws and consider limitations on the export, use, and analytics on data protected by certain country regulations. Additionally, cybersecurity teams should consider segmentations due to certain legal requirements to maintain state required mandates to ensure the security of protected information through tools, processes and restrictions on public and private cloud services.

Moreover, a growing reliance on "multicloud" makes assessing vendor risk even more difficult. In early 2018, a survey showed that 87 percent of organizations were in a multicloud environment. This trend, along with the rapid evolution of information security technologies, tools, and best practices, means that companies may look to regulations as a way to help make sense of what standards they need to follow. However, depending on regulations may not be the best bet.

The NTSC noted in an August 2018 blog post that "As a rapidly evolving area of cloud computing that businesses are quickly embracing, multicloud also creates implications for cybersecurity laws, policies, and regulations that may affect this technological adoption. While multicloud may mitigate business risks and offer more agility for organizations, many cybersecurity questions emerge around the use of multiple cloud vendors, an organization's security posture, and governance. [...] [Organizations] try to 'contain complexity' with multicloud when workloads are managed per environment, visibility and control stops at the boundaries between the cloud environments, and operations are domain- or vendor-centric".

STATE OF IT REGULATORY ENVIRONMENTS RELATED TO CLOUD COMPUTING

Although the growth of cloud computing may be displacing traditional information technology systems, it is certainly not causing a net reduction in information security-related IT regulations. At a federal level, Congress and agencies have updated existing regulations with guidance specific to cloud and introduced many new cloud-related regulations. While the rationale of any new and existing IT regulations may be sound, the quality of each regulation varies. Highly prescriptive rules may be quickly superseded by the cloud's dynamic technology changes, forcing organizations to choose between state-of-the art security or compliance. Less prescriptive regulations that focus upon compliance with currently available best practices and standards tend to have greater longevity.

In addition, concerns about privacy conflict with the ease of using cloud. The ripple effects of the EU's General Data Protection Regulation (GDPR) on the US, along with a possible wave of privacy regulations inspired by the California Consumer Privacy Act of 2018, may negatively impact companies and cloud providers that do not have clear standards or best practices in place to assess risk. Legislation and regulations around data breach notification also introduce issues to companies and cloud providers. For example, attribution is challenging with multicloud because of the complexity of the cloud infrastructure. In an interview with the NTSC in June 2018, Bikash Koley, CTO of Juniper Networks, said, "The cloud can't be viewed as a single entity any longer—because it's not. Cloud is no longer one organization, provider, or even an appliance. It's a fluid infrastructure. If lawmakers and policymakers understand what multicloud enables enterprises to do, then that knowledge will help policymakers craft sensible policies."

In the meantime, cloud providers complain that various compliance requirements duplicate security control requirements but are highly disparate in the documentation requirements. Because they have far fewer compliance resources than global cloud providers, smaller providers struggle to achieve balance between compliance and delivering improved security for their organization.

As an example of how these issues could be solved, the Federal Risk and Authorization Management Program (FedRAMP) is the US federal government's program for assuring the security of cloud providers used by various government agencies. While complaining about FedRAMP is its own cottage industry, its structure contains important components that represent an advancement in regulatory approaches to cloud computing:

- **Transparent, repeatable processes and artifacts for Shared Responsibility Model Execution.** FedRAMP CSPs produce comprehensive security control documentation (a FedRAMP System Security Plan) that is securely shared with customers that identifies which controls customers have full or shared responsibility for and describes what the customers responsibilities are. Control responsibility allocations are summarized in the FedRAMP Control Implementation Summary and customer control implementation responsibilities are compiled concisely in the FedRAMP Customer Responsibility Matrix. This comprehensive information facilitates comparisons between different CSPs and customer implementation of their security responsibilities with their selected CSP.
- **Authorization to Operate (ATO).** This is reciprocity between federal agencies. If a cloud service is authorized once under FedRAMP, it can be used by any number of federal agencies.

Comply once, use many.

- **Continuous Monitoring.** FedRAMP requires validation every 30 days that the security controls are maintained with the cloud service.
- **Low/Medium/High Assurance.** FedRAMP has requirements for differing levels of security assurance, allowing cloud providers and federal customers with a negotiated approach to the scope of compliance activities related to the business risk requirements.

Similarly, the NTSC and CSA are arguing for less prescriptive, flexible, and standards-based regulations that are consistent at both the federal and state level and encourage cloud providers to improve security while avoiding the pitfalls of highly prescriptive legislative or regulatory compliance requirements that do not effectively solve the root problem or promote trust.

ORGANIZATIONAL PROCUREMENT AND THE SECURITY VETTING OF CLOUD

Large organizations tend to have mature information security programs perhaps started two decades ago or longer that evolved with changes in technology, society, and regulatory requirements. Cloud computing represents a significant challenge to many of these programs, bringing into question whether this continued evolution will be sufficient or if existing approaches must be rethought completely.

Currently, vetting the security of outside IT vendors often occurs during the procurement process. However, cloud computing introduces unique challenges to vendor management. Whereas traditional IT procurement involves capital investments and centralized processes, cloud computing procurement can be highly distributed, purchased immediately, and expensed later. In some cases, the vetting may be less rigorous than traditional IT procurement and not helped by proprietary, in-house IT security checklists and assessment questionnaires.

Many of these proprietary documents originated in outsourcing and supply chain security, and use cases tend to fit legacy outsourcing situations. They involved years of work and many iterations, resulting in generally excellent work products that refer to well-known, high quality industry standards. Proprietary security vetting programs represent extensive knowledge of an organization's needs and risk appetite, and many organizations leverage this knowledge by mapping their needs to standard security documentation used by providers. However, these standards may satisfy only 80-90% of an organization's requirements—with resultant gaps addressed more efficiently when provider security documentation is unclear or inadequate.

The reality is that a cloud provider's compliance experts find it more efficient to relate their existing security compliance documentation to an organization's unique needs. This restructuring often results in no security compromise but it changes the instruments of communication and negotiation of security requirements, placing the organization at the mercy of the cloud provider rather than the other way around.

While organizations are often loath to discontinue the usage of these internally developed assessments, it is no longer realistic or even beneficial to use proprietary security assessment questionnaires as part of a cloud provider procurement negotiation. Traditional outsourcing does not operate at the same radical level of scale as cloud. For cloud providers to scale and remain efficient, they must leverage resources over an exponentially large number of customers and operate with opaqueness and anonymity. In a cloud environment, it is extremely difficult for a provider to expend mindshare around a single customer's proprietary security assessment methodologies.

To address these issues, the NTSC and CSA are jointly issuing a call to all stakeholders, and particularly to CISOs, to embrace the CSA's Security, Trust & Assurance Registry (STAR) program to create consistency and greater accountability and security within the cloud ecosystem. CSA STAR is the world's leading program for cloud provider assurance. Initiated in 2011, CSA STAR has been adopted by many in the industry and provides multiple tools that create the foundation of an industry standard for vetting the security of cloud providers.

Cloud Controls Matrix (CCM)

As a controls framework tailored to cloud computing, the CSA CCM provides both cloud providers and customers with needed structure, detail, and clarity relating to information security. The CCM provides fundamental cloud control objectives around three key areas: cloud architecture, cloud governance, and cloud operations. It also includes context around cloud provider versus customer control responsibilities as well as mappings to popular standards such as PCI/DSS, ISO/IEC 27001, COBIT, NIST 800-53, and many more. Used by enterprises as the controls framework baseline for their transition to cloud computing, the CCM is typically mapped against the internal information security management system (ISMS). Remaining gaps important to the enterprise can then be specifically addressed.

The Consensus Assessments Initiative Questionnaire (CAIQ)

Based upon the CCM, the CAIQ provides a set of Yes/No/NA questions that a cloud consumer and cloud auditor may wish to ask of a cloud provider to ascertain compliance to the CCM and CSA best practices. Nearly all cloud providers have experience with the CAIQ and can often provide a completed copy relatively quickly (although in some cases an NDA is necessary).

The STAR Registry

The STAR Registry is a publicly accessible website where cloud providers post both self-assessments and third-party audits based upon CSA cloud security standards. By insisting upon cloud provider transparency, CSA's STAR entries deliver a level of detail around security practices previously only available under a non-disclosure agreement (NDA). These entries provide valuable information that enterprises can compare to customer requirements. All major cloud providers and hundreds of others have adopted the STAR program. Enterprises can query the STAR Registry to search for cloud providers they wish to evaluate or procure. If a cloud provider does not appear in the STAR Registry, customers can send the CAIQ to the provider.

We understand that large organizations may have security requirements not articulated within CSA STAR. However, the usage of CSA STAR will allow the consumer to radically narrow down the scope of their inquiry to specific gaps. Based on feedback to the CSA, the STAR program on average satisfies a minimum of 80% of an organization's cloud security requirements and lifts a tremendous burden from vendor management vetting processes. The process for updating and improving CSA STAR is transparent and open to all organizations that wish to help.

CLOUD PROVIDER VETTING BEST PRACTICES

As organizations grapple with improving cloud security provider vetting, we recommend that you include a variety of key practices in your company's IT vendor security assessments. These practices include:

- **Treating third party technical services as an asset in your organization.** These third-party technical services include cloud providers. If not seen as assets, your organization may neglect to assess the risk of third-party technical services and open yourself up to liability. Assigning threat profiles to assets can help you evaluate the risk of those assets to the organization.
- **Establish a risk-based approach to third-party assessments.** Companies may rely on thousands of third-party technical solutions, which can be difficult to track and manage. Knowing which third-party technical solutions introduce the most relative risk helps if prioritization becomes necessary.
- **Develop third-party assessments based on input from key stakeholders across the organization.** CISOs should not develop these assessments alone. Solicit input from IT, security, privacy, business leaders, operations personnel, and others to create a comprehensive assessment program.
- **Ensure business owner engagement.** Business owners need to be engaged in the assessment process and understand their vendor management responsibilities. This helps later with a successful implementation and continuous use of the cloud provider assessment program.
- **Periodically review the highest risk vendors.** On a regular basis, perform reviews of the highest risk vendors to ensure that risk continues at acceptable levels or is accepted by the business. This review lessens "surprises".
- **Consider requiring the use of pre-approved vendors across the organization.** This kind of policy will especially help ensure regulatory compliance such as with credit card processing vendors.
- **Encourage or mandate the use of compliant suppliers.** Encouraging or mandating the use of compliant suppliers shows you mean business. Require that cloud suppliers demonstrate compliance with a known and accepted technical standard (such as ISO 27001) or provide transparency into best practices (such as SSAE16 SOC2 or CSA STAR).

TIPS FOR ROLLING OUT CLOUD PROVIDER VETTING PROGRAMS AND IMPROVING EXISTING PROGRAMS

When rolling out the STAR program within your organization, these tips will help encourage its success and help the program take root.

1. **Educate yourself about all aspects of the CCM.** By taking the time to learn about the CCM, you are also educating yourself and confirming industry best practices concerning what a cloud provider must do to ensure a secure cloud infrastructure.
2. **See where you already overlap with the CCM, and where you don't.** It's highly likely you will overlap heavily with the CCM simply by following existing standards. By comparing your internal program with the CCM, you can focus more on gaps and assessing how to cover those gaps. During this comparison process, don't forget industry-specific (such as HIPAA) and international security requirements (such as GDPR).
3. **Train your staff.** Make sure your employees are trained and up-to-date on any changes, requirements, and updates related to the CCM—especially training those who will help vet cloud providers, manage those relationships, and interact with the technology.
4. **Educate your suppliers.** As you roll out this program, your suppliers may resist or show surprise at this change. Many cloud providers should already follow most of these standards, but your shift in the way you vet and assess cloud providers will require some education and communication as you answer their questions and address concerns.

Even after the rollout, you want to continuously improve your program and keep it vital. The following tips may help.

1. **Stay up-to-date on any CCM changes.** Keep connected to the CSA as it updates and discusses the CCM through its working groups.
2. **Address issues proactively.** Don't let your program lapse or die out from weak enforcement, taking shortcuts, or allowing speed-to-market to once again dominate your security strategy. As issues arise with cloud provider security and risk, address them as soon as possible.
3. **Adapt your standards as your business and industry changes.** While the CCM serves as a foundational cloud provider vetting tool, it will not on its own account for specific changes within your business or industry. Maybe you're entering international markets for the first time. Or maybe your industry is grappling with a new or changed regulation. Your program needs to reflect these changes and you need to communicate those changes to cloud providers.
4. **Constantly communicate and educate.** Don't assume that because you've told cloud providers and business stakeholders about your program once that they completely understand it. Continual communication and education is necessary to remind stakeholders and cloud providers why the program exists, what it does, and what they must do to become more secure.

ADVANCED PROGRAM TOOLS AND INSIGHTS

Once your program is up and running, CSA offers some advanced tools that can help you get more out of your cloud provider vetting and assessments.

- **Self-service tools:** CSA offers self-assessments that cloud providers can fill out covering both standard CCM requirements (CSA STAR Self-Assessment) as well as GDPR requirements (CSA GDPR Code of Conduct Self-Assessment) if companies do business in the EU.
- **Independent third-party assessments:** CSA provides a STAR Attestation based on type 1 or type 2 SOC attestations supplemented by the criteria in the CCM. This attestation provides flexibility for organizations to update the criteria as technology and market requirements change while also allowing for robust reporting on the service provider's description of its system and controls. There is also a CSA STAR Certification that provides a rigorous third-party independent assessment of a cloud service provider's security. This technology-neutral certification leverages the requirements of the ISO/IEC 27001 management system standard together with the CCM. (CSA also provides a STAR Attestation for the Greater China market that harmonizes CSA best practices with Chinese national standards.)
- **Continuous, automated assessments:** CSA STAR Continuous will enable the automation of cloud providers' current security practices. It utilizes the CCM, the CloudTrust Protocol (CTP) (the mechanism by which cloud service consumers can ask for and receive information about the elements of transparency as applied to cloud service providers), and the CloudAudit (a common interface and namespace that allows enterprises and cloud computing providers interested in streamlining audit processes to automate the Audit).

VENDOR ASSESSMENT SHOWCASE: THE TRUSTED PARTNER NETWORK

The Trusted Partner Network (TPN) serves as a great example of how a program like CSA's STAR program can help CISOs. The TPN is a joint venture between two major industry associations—the Motion Picture Association of America (MPAA) and the Content Delivery & Security Association (CDSA)—that provide third-party entertainment industry assessments.

A few years ago, the entertainment industry had a major problem with vendor assessments and audits for movie and television productions spiraling out of control. Content was created more and more by a growing ecosystem of third-party vendors, each with varying degrees of security. This reliance on third-party content providers escalated the security threat to the entertainment industry's most prized and valuable asset—its content.

As an industry-wide film and television content protection initiative, the TPN established a single benchmark of minimum-security preparedness for all vendors and their teams wherever they work and whatever their specialty. The TPN mapped its technical security standards to the CCM. Vendors serving companies that have joined the TPN fill out one CCM questionnaire and upload it into the TPN database. Then, any TPN member can access it. Because audit results are uploaded and shared across the TPN community, the costs to studios and partners are reduced.

"There is no doubt this program will help reduce vendor assessment security costs and help raise the overall security in the industry," said CDSA President Guy Finley. "Vendor transparency will help improve security, not just for these vendors, but the entire industry."

It's clear that something similar can work for CISOs across all industries.

CONCLUSION:

By using an agreed upon standard of cloud assurance tools that can be extended with an organization's unique requirements, CSA STAR provides the best of all worlds:

- Enterprises can immediately get answers to the most common security concerns from cloud providers and address the small number of residual risks using proprietary tools. They can also speak with a unified and amplified voice to cloud providers and more easily have their priorities addressed by the market.
- Cloud providers can more rapidly comply with popular standards and provide customers with comprehensive assurance information.
- Regulatory bodies can reference state of the art best practices within their guidance and prevent regulations from quickly becoming obsolete.
- The entire industry itself raises its security baseline as all consumers benefit from the efforts of providers to comply with STAR.

We believe that the future of cybersecurity, the future of cloud computing, and the resilience of our economy is largely in the hands of the consumers of cloud services. If organizations each take their own path toward performing security vetting of cloud providers, their voices will be diluted and have less of an impact on the industry. However, by collaborating (even with competitors), organizations adopting cloud can send the message to cloud providers and regulatory bodies that agreed upon, robust, industry-standard best practices for security in the cloud are a mandate for all.

The NTSC also urges that federal lawmakers, regulators, and policymakers align with CISOs and the CSA framework when creating or updating laws and regulations that impact cloud. Using the CSA framework as a standard will increase the quality, longevity, and adaptability of laws and regulations, ensure that compliance is less prescriptive and fits the needs of businesses dealing with dynamically changing cloud technology, and ultimately protect consumer privacy with stronger national cybersecurity standards.

About Cloud Security Alliance

The Cloud Security Alliance (CSA) is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, certification, events and products. CSA's activities, knowledge and extensive network benefit the entire community impacted by cloud — from providers and customers, to governments, entrepreneurs and the assurance industry — and provide a forum through which diverse parties can work together to create and maintain a trusted cloud ecosystem. For further information, visit us at www.cloudsecurityalliance.org, and follow us on Twitter @ cloudsa.

About the National Technology Security Coalition (NTSC)

The National Technology Security Coalition (NTSC) is a non-profit, non-partisan organization that serves as the preeminent advocacy voice for Chief Information Security Officers (CISOs) across the nation. Through dialogue, education, and government relations, we unite both public and private sector stakeholders around policies that improve national cybersecurity standards and awareness.

Twitter @NTSC_CISO

