"Impact on Existing Security and Compliance when Migrating to Third-Party Hosted Cloud"

TIER4
IT PROCUREMENT REDEFINED

Tino Mantella - President and CEO

Tom Strickland – CISO and Senior Director

Passionate Advisors changing the way IT professionals procure services.

What is Cyber Security?

- Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, training, best practices, and technologies that can be used to protect the cyber environment and organization and user's assets.
- Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment, regardless of on-premises or hosted cloud.

Security Challenges

- **What is Security and how does it impact me?**

Increasing Threats	Service Level Expectations	Demands on Technology Mgt.	Regulation & Compliance
▪ Sophistication ▪ Frequency ▪ Speed ▪ Quantity ▪ Complexity ▪ Impact potential ▪ Interconnected Systems	▪ Trustworthiness ▪ Confidentiality ▪ Integrity ▪ Availability ▪ Privacy ▪ Mobility and Remote Access ▪ Monitoring and Reporting	▪ Integrated Approach to Risk Management ▪ Holistic Approach to Security ▪ Proactive ▪ How to Operationalize	▪ Governance (Policy & Procedures) ▪ CEO, Board-level Accountability ▪ New Laws and Dynamic Regulations ▪ Industry-specific Regulations

Threats and Risks Span Across the Cloud, IT and Corporate Enterprise Infrastructures

Security Environment Common Findings

- Inadequate policies, procedures and culture
- Inadequately designed systems and networks lack defense-in-depth
- Remote access without appropriate access control
- System administration mechanisms and software not adequately scrutinized, monitored or maintained
- Inadequately secured wireless communications
- Non-dedicated communication channels
- Insufficient use of tools to detect and report on suspicious activities
- Unauthorized or inappropriate applications/devices on networks
- Control Systems data not authenticated
- Inadequately managed, designed or implemented critical support infrastructure

Security Industry Trends

- Increasing Threat Environment across all systems and data
- Escalating terrorist and Nation-State (outsider) threat sources
- Advanced cyber attack capabilities leveraging more sophisticated tools
- Cyber attacks leveraging composite information to mount successively higher level targeted attacks
- Increased convergence and dependency of IT and telecommunications
- Increasing needs for remote access, adoption of authentication and encryption techniques
- Increasingly more sophisticated detection and alarm mechanisms
- Increased regulations - DHS moving toward the use of the NIST to meet the various mandates for Enterprise Cyber Security initiatives
- Risk Management Process utilizing the evaluation criteria

Top 20 Areas of Vulnerability 1 of 2

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware/Software on Laptops, Workstations and Servers
4. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
5. Boundary Defense
6. Maintenance, Monitoring, and Analysis of Security Audit Logs
7. Application Software Security
8. Controlled Use of Administrative Privileges
9. Controlled Access Based on Need to Know
10. Continuous Vulnerability Assessment and Remediation

Top 20 Areas of Vulnerability 2 of 2

11. Account Monitoring and Control
12. Malware Defenses
13. Limitation and Control of Network Ports, Protocols, and Services
14. Wireless Device Control
15. Data Loss Prevention
16. Secure Network Engineering
17. Penetration Tests and Red Team Exercises
18. Incident Response Capability
19. Data Recovery Capability
20. Security Skills Assessment and Appropriate Training to Fill Gaps

Working on the Top 20 would form 80% of a security foundation

Considerations when Migrating to Third-Party Hosted Cloud

Types of Cloud Services

- The cloud has opened up new frontier for storage, access, flexibility, productivity and security concerns.
- Cloud computing comes in a variety of forms:
  - **Private clouds**: Generally dedicated to a single organization for private use. Can be built either on-premises or off-site and they deliver virtualized application, communications, and infrastructure services.
  - **Public clouds**: Accessible to the public via a network and usually owned and provided by a third party.
  - **Hybrid clouds**: Offer best of private and public clouds. Enables an organization to retain private, sensitive information in a private cloud, but also provide access to a variety of cloud computing services offered by public clouds.
  - **Community clouds**: Collaborative systems shared by a limited number of organizations, often within the same industry (e.g. healthcare). Costs are split among the users and can be hosted internally, or externally by third parties.

Security Considerations: Cloud versus On-site

- Moving data and applications to the cloud does not remove security requirements.
- What does change, is who takes ownership of the responsibility for maintaining day to day security. This responsibility is now shouldered by the cloud provider.
  - Previously, the business would work proactively to ensure data security in-house by managing infrastructure.
  - On-site technical staff would tackle any potential risks uncovered. It also meant that the actual physical security of the location the infrastructure was housed within, was managed by the company.
  - The shift to the cloud, sees the business lose its ability to manage both digital and physical security itself.
  - Potentially this could lead to a loss of agility should a serious security flaw be uncovered, that needs to be fixed rapidly.

Adapting IT Security Strategy for the Cloud

- Private and public clouds function in the same way, applications are hosted on a server and accessed over the Internet.
- Whether Software as a Service (SaaS) of customer relationship management (CRM) software, creating offsite backups of your company data, or setting up a social media marketing page, you're trusting a third-party company with information about your business and, most likely, your customers
- A cloud migration changes IT security at a fundamental level.

Adapting IT Security Strategy for the Cloud

- The business will need to make some sweeping changes to the strategy it has in place to handle data security once a cloud platform has been implemented.
- Need to move away from a technical, hands on approach to managing data security.
- There will be far less need for technical staff with a skillset to maintain infrastructure security.
- More focus needs to be given to monitoring and management.
- The business becomes responsible for oversight of the cloud host.
- Ensuring that the host is actioning all data security requirements effectively.

Ensuring a Robust Post-Cloud Security Policy

- Migrating critical business systems and data to the cloud, means going back to the drawing board with regards to security policy.
- Draw a clear line between the responsibilities of the business and of the cloud provider.
- The company's IT security policy needs to be most clearly defined.
- Put in place processes for monitoring the security practices of the cloud host.
- Ensure SLA are kept as well as dealing with services deficiencies that breach the SLA on a case by case basis.
- In parallel the company still needs to take care of internal security policies such as maintaining a staff awareness program, and also taking care of desktop security.
- Overall, migrating to the cloud does remove some of the more technical aspects of IT security however, this does not mean that the business can stop being proactive about protecting its valuable data.

Not All Clouds Are Alike

- Each cloud setup or provider brings its unique set of strengths and shortcomings.
- A private cloud, for instance, may offer greater flexibility but less scalability.
- Migrating all apps to the cloud
  - Not all business applications should migrate to the cloud, and enterprises must determine which apps are best suited to a cloud environment.
  - Carefully study how a cloud-based operation might impact their applications' ability to meet stringent compliance, governance, and security issues.
- Not tuning your apps for the cloud
  - When businesses migrate their most essential applications to the cloud, they often fail to check how those apps will perform in their new environment.
  - It's important for enterprises to tweak their apps to run optimally in the cloud.

Not All Clouds Are Alike

- Not doing your due diligence
  - Organizations often fail to thoroughly research a cloud technology or provider before embracing it. It's important to carefully study your IT infrastructure, needs, and usage to best determine which cloud service is right for you.
  - Find out how to leverage the cloud's on-demand processing power to maximize your applications' "bursty" needs.

Not All Clouds Are Alike

- Ignoring cloud geography
  - Enterprise applications may run within a single geographic region from multiple locations, or perhaps across the globe.
  - Consumer-focused apps are often used in multiple geographic regions and sometimes unpredictably.
  - Enterprises may want to block certain apps often for regulatory or security purposes in specific regions. And since multinational companies have offices scattered around the world, they might benefit from distributing apps closer to their points of access.
  - Always explore the geopolitical ramifications of your cloud architecture, and ask potential providers if they're capable of handling your far-flung needs.

Cloud Security Concerns

- Data Breaches
  - Cloud is relatively new, yet data breaches in all forms have existed for years. The question remains: “With sensitive data being stored online rather than on premise, is the cloud inherently less safe?”
  - Overall data breaching are three times more likely to occur for businesses that utilize the cloud than those that don’t. The simple conclusion is that the cloud comes with a unique set of characteristics that make it more vulnerable.

Cloud Security Concerns

- Hijacking of Accounts
  - Attackers have the ability to use login information to remotely access sensitive data stored on the cloud; also, attackers can falsify and manipulate information through hijacked credentials.
  - Other methods of hijacking include scripting bugs and reused passwords, which allow attackers to easily and often without detection steal credentials.
  - Phishing, keylogging, and buffer overflow all present similar threats. However, the most notable new threat – known as the Man In Cloud Attack – involves the theft of user tokens which cloud platforms use to verify individual devices without requiring logins during each update and sync.

Cloud Security Concerns

- Insider Threat
  - An attack from inside your organization may seem unlikely, but the insider threat does exist. Employees can use their authorized access to misuse or access information such as customer accounts, financial forms, and other sensitive information.
  - Additionally, these insiders don't even need to have malicious intentions.
  - Insider threat was the misuse of information through malicious intent, accidents or malware.
  - Four best practices companies could follow to implement a secure strategy are business partnerships, prioritizing initiatives, controlling access and implementing technology.

Cloud Security Concerns

- Malware Injection
  - Scripts or code embedded into cloud services that act as “valid instances” and run as SaaS to cloud servers. Malicious code can be injected into cloud services and viewed as part of the software or service that is running within the cloud servers themselves.
  - Once an injection is executed, attackers can eavesdrop, compromise the integrity of sensitive information, and steal data.
  - Threats of malware injections has become a major security concern in cloud computing systems.

Cloud Security Concerns

- Abuse of Cloud Services
  - Cloud-based services has made it possible for both small and enterprise-level organizations to host vast amounts of data easily.
  - The cloud's unprecedented storage capacity has allowed both hackers and authorized users to easily host and spread malware, illegal software, and other digital properties.
  - Privileged users can directly or indirectly increase the security risks and as a result infringe upon the terms of use provided by the service provider.

Cloud Security Concerns

- Hijacked and Insecure APIs
  - Application Programming Interfaces (API) give users the opportunity to customize their cloud experience and can be a threat to cloud security. They give companies the ability to customize features of their cloud services but they also authenticate, provide access, and effect encryption.
  - APIs give programmers the tools to build their programs to integrate their applications with other job-critical software.
  - The vulnerability of an API lies in the communication that takes place between applications. While this can help programmers and businesses, they also leave exploitable security risks.

Cloud Security Concerns

- Denial of Service Attacks (DoS)
  - DoS assaults do not attempt to breach your security perimeter, rather, they attempt to make your website and servers unavailable to legitimate users.
  - DoS is also used as a smokescreen for other malicious activities, and to take down security appliances such as web application firewalls.

Cloud Security Concerns

- Insufficient Due Diligence
  - While not technical in nature, this particular security gap occurs when an organization does not have a clear plan for its goals, resources, and policies for the cloud.
  - In other words, it's the people factor.
  - Additionally, insufficient due diligence can pose a security risk when an organization migrates to the cloud quickly without properly anticipating that the services will not match customer's expectation.
  - This is especially important to companies whose data falls under regulatory laws like PCI, HIPAA, SoX, PII, PCI, PHI, and FERPA or those that handle financial data for customers.

Cloud Security Concerns

- Shared Vulnerabilities
  - Cloud security is a shared responsibility between the provider and the client.
  - This partnership between client and provider requires the client to take preventative actions to protect their data.
  - Major providers may not have standardized procedures to secure their side so fine grain control is up to you, the client.
  - Key security protocols such as the protection of user passwords, access restrictions to both files and devices, and multi-factor authentication is in your hands.
  - The bottom line is that clients and providers have shared responsibilities and omitting yours can result in your data being compromised.

Cloud Security Concerns

- Data Loss
  - Data on cloud services can be lost through a malicious attack, natural disaster, or a data wipe by the service provider. Losing vital information can be devastating to businesses that don't have a recovery plan.
  - Securing your data means carefully reviewing your provider's back up procedures as they relate to physical storage locations, physical access, and physical disasters.

Cloud Security Operational Risks

- Loss or Theft of Intellectual Property
  - Companies increasingly store sensitive data in the cloud.
  - It is reported that that 21% of files uploaded to cloud-based file sharing services contain sensitive data including intellectual property.
  - When a cloud service is breached, cyber criminals can gain access to this sensitive data.
  - Absent a breach, certain services can even pose a risk if their terms and conditions claim ownership of the data uploaded to them.

Cloud Security Operational Risks

- Compliance Violations and Regulatory Actions
  - Most companies operate under ridged compliance frameworks of regulatory control of their information, whether it's HIPAA for private health information, FERPA for confidential student records, or one of many other government and industry regulations.
  - Under these mandates, companies must know where their data is, who is able to access it, and how it is being protected.
  - Bring your own cloud (BYOC) often violates every one of these tenets, putting the organization in a state of non-compliance, which can have serious repercussions.

Cloud Security Operational Risks

- Contractual Breaches with Customers or Business Partners
  - Contracts among business parties often restrict how data is used and who is authorized to access it.
  - When employees move restricted data into the cloud without authorization, the business contracts may be violated and legal action could ensue.
  - An example would be a cloud service that maintains the right to share all data uploaded to the service with third parties in its terms and conditions, thereby breaching a confidentiality agreement the company made with a business partner.

Cloud Security Operational Risks

- Increased Customer Churn
  - The company needs to decide a suitable strategy in marketing and sales material.
  - If customers even suspect that their data is not fully protected by enterprise-grade security controls, they may take their business elsewhere to a company they can trust.
  - A growing chorus of critics are instructing consumers to avoid cloud companies who do not protect customer privacy.

Cloud Security Operational Risks

- Data Breach Requiring Disclosure and Notification to Victims
  - If sensitive or regulated data is put in the cloud and a breach occurs, the company may be required to disclose the breach and send notifications to potential victims.
  - Certain regulations such as HIPAA and HITECH in the healthcare industry and the EU Data Protection Directive require these disclosures.
  - Following legally-mandated breach disclosures, regulators can levy fines against a company and it's not uncommon for consumers whose data was compromised to file lawsuits.

Cloud Security Operational Risks

- Data Location and at Rest
  - Often companies can't confirm if their employees are using their own cloud in the workplace.
  - In order to reduce the risks of unmanaged cloud usage, companies first need visibility into the cloud services in use by their employees.
  - Need to understand what data is being uploaded to which cloud services and by whom.
  - IT teams can begin to enforce corporate data security, compliance, and governance policies to protect corporate data in the cloud.
  - Companies must balance the risks of cloud services with the clear benefits they bring.

Going Forward when Migrating to Third-Party Hosted Cloud

Going Forward - Identify and Confirm

- Secure Data Transfer
  - All traffic travelling between your network and whatever service you're accessing in the cloud must traverse the Internet.
  - Make sure your data is always travelling on a secure channel; only connect your browser to the provider via a URL that begins with "https."
  - Data should always be encrypted and authenticated using industry standard protocols, such as IPsec (Internet Protocol Security), that have been developed specifically for protecting Internet traffic.

Going Forward - Identify and Confirm

- Secure Software Interfaces
  - Be aware of the software interfaces, or APIs, that are used to interact with cloud services.
  - Reliance on a weak set of interfaces and APIs exposes organizations to a variety of security issues related to confidentiality, integrity, availability, and accountability
  - Learn how any cloud provider you're considering integrates security throughout its service, from authentication and access control techniques to activity monitoring policies.

Going Forward - Identify and Confirm

- Secure Stored Data
  - Data should be securely encrypted when it's on the provider's servers and while it's in use by the cloud service.
  - It has been reported that few cloud providers assure protection for data being used within the application or for disposing of your data.
  - Ensure how potential cloud providers secure your data not only when it's in transit but also when it's on their servers and accessed by the cloud-based applications.
  - Confirm if the providers securely dispose of your data, for example, by deleting the encryption key.

Going Forward - Identify and Confirm

- User Access Control
  - Data stored on a cloud provider's server can potentially be accessed by an employee of that company, and you have none of the usual personnel controls over those people.
  - Consider carefully the sensitivity of the data you're allowing out into the cloud.
  - Receive specifics from the provider about the people who manage your data and the level of access they have to it.
  - Ensure these processes do not violate your policies and agreements.

Going Forward - Identify and Confirm

- Data Separation
  - Identify how cloud-based service shares resources.
  - Hypervisor software is used to create virtual containers on the provider's hardware for each of its customers so investigate the compartmentalization techniques, such as data encryption.
  - Confirm there is a defense-in-depth strategy, including multifactor authentication on all hosts, host-based and network-based intrusion detection systems, applying the concept of least privilege, network segmentation, and patching shared resources.
  - You should address these security issues with the cloud provider before you entrust your data to its servers and applications, they shouldn't be a deal breaker. Cloud computing offers small businesses too many benefits to dismiss out of hand. After all, you already met many of these security challenges the first time you connected your network to the Internet.

Going Forward - Identify and Confirm

- Evaluate Terms and Conditions and Read the Fine Print
  - Know what you are signing up to. Pay attention to service level agreements and data storage provisions. Use a Request for Proposals (RFP) or some kind of evaluation tool to compare different alternatives.
  - Often cloud contracts are spread over a host of different terms and conditions documents and acceptable use policies. Know where they all are and not just look at one and ignore the hyperlinks to the other documents.
  - The service provider may be able to suspend your right to use the service or terminate the agreement of any reason or for no reason within 60 days notice
  - In the event of a suspension of service, ensure the service provider won't intentionally ease your data and will preserve it.
  - The service provider usually can change the terms of service at any time without notice
  - Access to services may be suspended without notice. The service provider may have no liability for the downtime.
  - The customer bears sole responsibility for adequate security and back-up of data, even though it had been hosted by the service provider.

Going Forward - Identify and Confirm

- Geographical Differences in Privacy and Compliance
  - The virtual nature of the cloud means cloud service providers can host customers' data anywhere.
  - The downside for businesses is that they need to be aware of the differences between data privacy regulations in different parts of the world.
  - In the USA there is no overarching data protection legislation, but there are separate regulations for sectors such as health and finance.
  - In the US, data laws can also vary from state to state. Most states now have data breach notifications, which require companies to notify customers if data is lost or compromised.
  - It is important for organizations to know where their data is stored, if they are going to keep within the law.
  - The US Patriot Act is one consideration for any organization hosting personal data in the US. It gives the US government the right to subpoena data held by US companies.

Going Forward - Identify and Confirm

- Getting Data Out of the Cloud
  - Choosing what data to put into the cloud is one thing, but making sure you can get the data back out again is crucial.
  - One solution is to duplicate the data in more than one cloud service.
  - The savings that some public sector organizations are so great through cloud, that this is a feasible option.
  - Insisted in the contract that suppliers must provide and detail the cost of getting into the service, how to exit the service and the cost of exiting the service.
  - Confirm how to get the data back, in what format it comes back in and where the data is held.
- Phased Roll-Outs
  - When it comes to rolling out a cloud project it is crucial to work in phases rather than in a big bang.
  - It should be possible for to end the project after each phase and still add value to the organization.

What We Are Seeing - Summary

- Cyber security is a serious and increasing challenge for all industries and cloud systems infrastructure.
- Cyber threats can impact national security, public safety, the national economy and your bottom line.
- While governments are responsible for national security, the private sector owns and operates most of the cloud services, assets and infrastructure.
- This means securing IT systems is a shared responsibility across many technologies, corporate departments, cloud and system partners.
- Whether on-premise or cloud based, all systems will require a minimum set of controls with more critical systems requiring higher levels of protection and automation.

Overall Security Risks Across On-Premise and Hosted Cloud Environments

Security Threat Models to the Cloud

- Administrative
- Crypto
- Download
- Identification & Authentication
- Information System
- Initialization
- Insider
- Key Management
- Terrorist Act
- Malicious Code
- Network
- Operational Denial of Service
- Operational Disclosure
- Physical
- Social Engineering
- Trust

So ask yourself…..

- Where do I look **first**?
- What do I **focus** on?
- What **should** I do?
- What **can** I do?

Threat Remediation – What Is Being Done

- Avert Threats - Design, deploy, and operate jointly with partners.
- Develop and maintain effective security programs, including insider threat protections.
- Pursue Operational, Architectural, and Technical Innovations
- Develop proactive approaches to improving security and managing cyber risk.
- Deploy Security Measures Based on Proven Effectiveness
- Distribute information regarding proven strategies.
- Identify and Harden Critical Information Infrastructure
- Lead enterprise-wide efforts to secure all systems, including: continuous monitoring, sharing of best practices, assessing the security of all departments, advocating for the importance of effective technology management, helping to achieve cost savings for cyber security-related procurements, and developing enterprise-wide operational architectures and guidance.
- Leverage the Enterprise in Taking Priority Actions

Threat Remediation – What Is Being Done

- Prepare for Contingencies
- Work with stakeholders to prioritize cyber recovery efforts.
- Ensure a unified and coordinated response to significant cyber incidents.
- Enable the rapid transition of effective technologies from development to application.
- Fuse Information - Design, deploy, and operate jointly with partners.
- Provide stakeholders with a common operating picture.
- Distribute Information Effectively and Only as Appropriate
- Work to establish, refine, and maintain a trusted information sharing environment with increasing numbers of stakeholders.
- Provide Specialized and Continuing Security Training to the Cyber Workforce
- Provide information and services, in collaboration with other trading partners and federal agencies, to enable the cyber security workforce to meet standards of competence.
- Focus on the Return on Investment
- Increase System Fault Tolerance

Threat Remediation – What Is Being Done

- Develop the Cyber Workforce across All Departments
- Implement processes to raise awareness of risks among the enterprise, help develop the workforce structure, and recruit and train the next generation of the cyber security workforce.
- Build a Base for Distributed Security
- Support other awareness campaigns by providing toolkits and additional information.
- Reduce Vulnerabilities
- Coordinate the development of software assurance standards and benchmarking measures through public/private partnerships.
- Improve Usability
- Encourage development of usability requirements and their incorporation into trusted technology.
- Automate Security Processes
- Support the development and piloting of automated security processes and frameworks.

Threat Remediation – What Is Being Done

- Appropriately Validate Identities
- Deploy multi-factor authentication to validate identities of personnel.
- Mandate development of processes, technologies, and policies for managing online identities and how those identities can be used to access information resources.
- Increase Technical and Policy Interoperability Across Devices
- Allocate resources to support the development and deployment of interoperable technologies, architectures, policies, and standards.
- Encourage the development of standardized dictionaries for security automation and measurement to facilitate information sharing and interoperability.
- Build trust among stakeholders.
- Identify the Root Causes and Extent of Adverse Events
- Enhance and promote methods for appropriately sharing information about the causes, extent and impact of hazards.
- Conduct vulnerability assessments of critical information infrastructure.

What to Expect in the Future

- Focus on sustainability, increased regulatory compliance, resources limitations, and increased external threats.
- Increasing needs to protect all aspects of systems and data
- Significant challenges of supporting profitability while not compromising availability, quality and client satisfaction.
- Highly dependent on integrated systems to manage complex resources.
- Increased convergence and dependency of IT and telecommunications.
- Increased use of distributed intelligent devices and controls.
- Increasing needs for remote access, adoption of authentication and encryption techniques.
- Increasingly more sophisticated detection and alarm mechanisms.

Key Lessons Learned

- Executive sponsorship is essential
- Build a culture of security, not compliance
- Plan first, then implement
  - Understand your business and technology maturity level
  - Define solid business requirements to align with evolving standards
- Technology is not a silver bullet solution, overuse of technology can be just as bad as under use
- Develop a enterprise-wide program for security management and implement
- Establish awareness with vendor relationships

Going Forward

Are You Being Asked?

> To satisfy an ISO27001, HIPAA, HITRUST, PCI, PII, SOC2, FISMA, NIST 800:53 audit or certification?

> If your network, production systems, endpoints are vulnerable to hacking, bots, ransomware or cyber security breaches?

> To find a CISO partner to get started and/or maintain your certified state but don't want to hire full-time?

WHAT WE DELIVER

- Detailed findings and gap analysis reports
- Risk Assessment & Remediation Plans
- Training Development & Delivery
- Process Documentation for internal adoption

#TIER4 #ITSecurityServices

OUR OFFERINGS

- Security Assessments – scheduled and on-demand
- Preventative Maintenance – annual agreements performed on-demand or per schedule

TIER4 CISO-as-a-Service

ON DEMAND

- ✓ Security Program Structure and Process Planning
- ✓ Security Technology Solutions
- ✓ Strategic & Organizational Consulting
- ✓ Security Program Support and Management
- ✓ Cyber & Physical Security Design and Implementation
- ✓ Governance Charter and Design Facilitation
- ✓ Organizational and Functional Integration
- ✓ As Needed CISO Support and Guidance – Fractional Time

ASSESSMENT

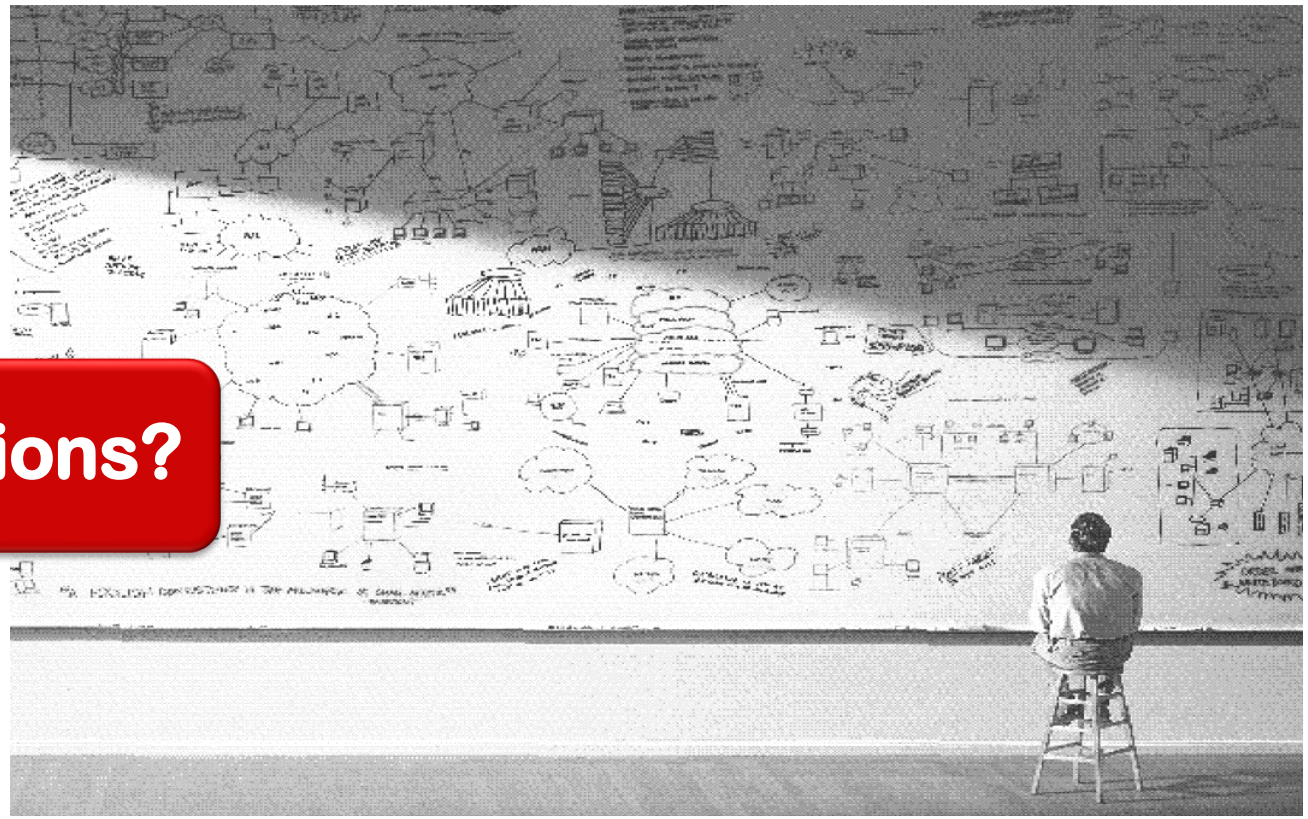
- ✓ Risk Based Methodology Assessment Review & Creation
- ✓ Pre/Post Audit, Assessments & Audit Preparedness
- ✓ Vulnerability & Penetration Testing
- ✓ Risk Assessment and Management Services (HIPAA, PCI, NIST, GDPR, NERC-CIP, ISO, COBIT)
- ✓ Compliance and Best Practice Design
- ✓ Architectural and Infrastructure Reviews
- ✓ Compliance and Gap Analysis Support
- ✓ Mitigation and Remediation Project Planning and Support

STRATEGIC

- ✓ Trusted Strategic Advisor
- ✓ Cybersecurity Design & Deployment
- ✓ Compliance Infrastructure Design
- ✓ System Product Lifecycle Management
- ✓ Enterprise Security Convergence Strategy
- ✓ Disaster Recovery Plan Development and Support Services
- ✓ Business Continuity Planning
- ✓ Incident Response
- ✓ Enterprise Security Awareness Training
- ✓ Compliance, Regulatory and Industry Convergence
- ✓ Independent Risk and Threat Analysis
- ✓ Data Center, Network Operation Centers (NOC) and Security Operations Centers (SOC)

Q&A

Any Questions?



Visit us online: **www.tier4advisors.com**
Connect on LinkedIn: Tier 4 Advisors
Follow: www.twitter.com/tier4advisors