QUALITY RESOURCES. EXCEPTIONAL VALUE.

Plans & Policies (Governance)

CKCM Inc. is here to aide in troubleshooting and perfecting your in-place disaster recovery and business continuity plans and policies. Given the current state of technology; these plans are more financially within reach than ever before, and address issues including back-ups as well as compliance with security protocols like PCI, HIPAA, ISO 27001/27002, FISMA and others.

Meeting with your stakeholders we compare your policies and procedures to current industry standards, thus allowing a custom plan to be developed to ensure we fit your budget and specific needs. Our goal is to ensure your operations are not hindered by the integrity or availability of your IT infrastructure no matter the situation.

The goal is for you to have stable practical documents with which to manage your resources and ensure improvement and continued success in our rapidly changing environment.

Monitoring

CKCM Inc. is here to provide continuous intelligence-based monitoring of your network and host data. Using internal and external network and security monitoring as well as live comparison against intelligence feeds with specific intelligence in your areas of operation; we will provide regular reports and urgent alerts to potential threats. Threats like ransomware, worms, data exfill and other major threats can be found in enough time to mitigate damage or losses. Our team consists of people with years of experience in tracking nation state level Advanced Persistent Threats (APTs) and are supported by machine learning.

Consulting

CKCM Inc. is here to provide consulting support to your organization to assist with implementation or utilization of governance as needed with prior contracts in place.

CKCM Inc. Services Lifecycle

CKCM Inc. Intendeds to provide all services in a timely manner that fit your organization's needs. We supply an adjustable lifecycle for all services provided that is based off your regular business days to allow constant communication. This schedule is contingent on your organizations needs and is finalized during the contracting stage to help us better support you and the understanding of process outcomes.

Compliance and Governance Assessments

Day 0: Your organization will send all governance documents and network map as well as key assets that need to be identified (what do you as an organization find the most important).

Day 1: Meet with key leadership to go over initial discrepancies we see and formulate solutions we feel best support you.

Day 2-N: We ensure all your documentation are completed with care and diligence while we stay in constant communication.

Final Day: Your documents are delivered and briefed to you, along with our recommendations.

Post Assessment: We set up a follow-up meeting on the final day to allow you to review our work and provide feedback or request follow up actions.

Consulting

Consulting services are on an hourly basis and are priced based on the work requested.

Services offered

- Compliance and Governance Assessment
  - Governance frameworks to include:
    - ✓ International Organization for Standardization (ISO 27001/27701)
    - ✓ National Institute of Standards and Technology (NIST SP800-53)
    - ✓ Government standards (HIPAA/HITECH, FISMA)
    - ✓ Other (PCI DSS)
- Cybersecurity and Information Assurance Architecture
  - Vulnerability/Attack surface of network
  - Assess control design and implementation
  - Post-implementation reviews
- Program Policies and Procedures Review
  - Acceptable Use Policy
  - Change Management Policy
  - Access Control Policy
  - Information Security Policy
  - Incident Response Policy
  - Remote Access Policy
  - Disaster Recovery Policy
  - Business Continuity Plan

While meeting with your stakeholders, we will compare your policies and requirements to current industry standards; allowing for a custom plan to be developed to ensure we fit in your budget as well as meet your specific needs.

Our goal is to ensure your operations are not hindered by the integrity or availability of your IT infrastructure no matter the situation.

Compliance and Governance Assessment

We develop solutions that enable organizations to align with governance initiatives while supporting their individual business strategy. Providing a complete picture and better understanding of your data; allowing for better asset management and informed decision making. Our experts leverage industry best practices to help you comply with any governance framework, whether it is federal, state, or an industry regulation like PCI, HIPAA, ISO 27001, or FISMA.

PCI DSS (Payment Card Industry Data Security Standard) is a widely accepted set of policies and procedures intended for organization's that handle credit, debit and cash card transactions to ensure the protection of cardholders' personal information. Obtaining a PCI DSS Report on Compliance (ROC) and Attestation of Compliance (AOC) demonstrates your organization's commitment to payment card data security and identifies the level of validation you have achieved.

The Health Insurance Portability and Accountability Act (HIPAA) and subsequent Health Information Technology for Economic and Clinical Health (HITECH) Act defines policies, procedures, and processes that are required to protect electronic protected health information (ePHI). As the regulatory oversight related to HIPAA increases, ensuring compliance becomes more valuable to you and your customers than ever.

ISO 27001 provides an international methodology for the implementation, management and maintenance of information security within a company. Becoming ISO 27001 certified demonstrates conformity of your Information Security Management System (ISMS) with the documented standards and provides your customers with assurance regarding the security of your system. Secure your organization at the top.

ISO 27701 is the first publication to address international data privacy. ISO 27701 is designed to help organizations protect and control the personally identifiable information (PII) that controllers and processors handle. Companies will benefit from the ISO 27701 certification as it will streamline compliance obligations for ISO 27001 and the GDPR by integrating privacy into an organization's information security management system.

The Federal Information Security Management Act (FISMA) establishes security guidelines that federal agencies or entities that interact with federal data or information systems, must adhere to. For companies pursuing federal contracts, or that are currently working with a federal agency, compliance with FISMA is essential to properly safeguard the systems and maintain contractual compliance.

Cybersecurity and Information Assurance Architecture

As threats perpetually change and adapt to new defensive postures; our job is to ensure your impact from such attacks are as minimal as possible. Our phased approach allows for an assessment and then security of any vulnerabilities your architecture encounters.

Phase 1: Security Assessment –Testing your existing systems and compare them to cyber security standards.

Phase 2: Security Roadmap Development – Comparing where you are today with where you want to go and create a plan to bridge the gap.

Phase 3: Security Plan Implementation – Taking our best practices and implementing those to get your organization's security posture to the desired level.

Phase 4: Monitor and Continually Reassess – Your organization, your IT systems, and the threats that you face are constantly evolving. We provide security with continuous monitoring and adaptation of your systems to always stay on top of protection for you and your company.

PHASE 1: Security Assessment

We specialize in four different assessments:

1. Automated Penetration Testing - Automated penetration testing provides an organization with an offensive assessment at a fraction of the cost.
2. Social Engineering Services – Our penetration testers use social engineering to test an organization's employees' understanding of information security and report on areas of weaknesses.
3. Vulnerability Services – This service removes false positives in the scan results and helps prioritize the identified vulnerabilities.
4. Penetration Testing – More information to come

PHASE 2: Security Roadmap Development

With the assessment complete we can then pair a full solution to align your business strategy to your cybersecurity and information assurance posture. We will provide a detailed report that outlines the validated vulnerabilities present within your organization, as well as risk rankings and recommendations for remediation of listed vulnerabilities.

PHASE 3: Security Plan Implementation

After the roadmap has been set, with the correct milestones and timing in place, we start rolling out the correct security architecture and fixing in holes within your appliances, ensuring data integrity and availability is almost at the front of our concern.

PHASE 4: Monitor and Continually Reassess

Security isn't a one-time fix. Continuous monitoring and vulnerability assessments are key to protecting your organization's most viable assets and staying up to date with threats.

- 24/7 Monitoring services by the security operating center analysts for your environments
- Advanced threat protection and incident reporting reinforcement
- Capable of ingesting all real time events while eliminating false positives to prioritize real threats

Program Policies and Procedures Review

We help organizations build and manage policies and procedures that grow over time. Our experts help establish the foundation for overarching policies to manage a client's risk through auditable work processes and documented policies and procedures.

- **Acceptable Use Policy (AUP)** – An AUP establishes the organizational IT constraints and practices that an employee must agree to in order to access the corporate network or the internet.
- **Change Management Policy** – Our experts help clients develop a formal process and change management program to ensure that all changes are conducted methodically to minimize and adverse impact on services.
- **Access Control Policy (ACP)** – The ACP outlines the access available to employees of an organization's data and information systems. CKCM's experts help clients set the policy for access control standards such as NIST's Access Control and Implementation Guides outlining how unattended workstations should be secured; and how access is removed when an employee leaves the organization.
- **Information Security Policy** – CKCM's experts help establish the primary information security policy of an organization to ensure that all employees who use information technology assets within the organization, or its networks, comply with its stated rules and guidelines.
- **Incident Response (IR)** – The incident response policy is an organized and methodical process establishing how the organization will manage an incident and remediate its impact on operations as well as reduce recovery time and control costs.
- **Remote Access Policy** – The remote access policy outlines and defines acceptable methods and processes to remotely connect to an organization's internal networks. This policy is required for organizations that allow employees to operate from insecure network locations.
- **Electronic Communication Policy** – An organization's electronic communication policy is a document that formally outlines how employees can use the organization's chosen electronic communication medium. It provides guidelines to employees on what is considered the acceptable and unacceptable use of any corporate communication technology such as email, blogs, social media and chat technologies.
- **Disaster Recovery Policy** – Together with the IT and cybersecurity team, CKCM's experts help develop and implement an organization's disaster recovery plan. The plan extends into a larger business continuity plan that's managed using the incident response policy.
- **Business Continuity Plan (BCP)** – CKCM's experts help organizations develop and test the BCP together with the disaster recovery plan that coordinates efforts across the organization to restore hardware, applications and data deemed essential for business continuity.