COALFIRE

DATASHEET

Cloud security maturity

Adopt Coalfire's cloud security maturity model as a safeguard

Moving to the cloud or thinking about moving to the cloud can be overwhelming and confusing. Coalfire's proven cloud security maturity (CSM) model helps you understand, implement, and scale security as the cloud environment grows.

OUR APPROACH

Leveraging our expertise within cloud environments, we developed our CSM model as an aggregation of industry-leading security practices defined by standards bodies (e.g., FFIEC, Center for Internet Security, NIST 800-53, PCI DSS, HITRUST, and Cloud Security Alliance), as well as recommendations from cloud service providers (CSPs) including AWS, Azure, and Google. Our approach establishes a "high bar" for security implementation that meets these requirements and recommendations.

Our CSM model assesses your environment, and then helps you develop a migration strategy that follows our three pillars of cloud maturity: strategic alignment, capabilities, and efficacy.

WHAT WE ASSESS:

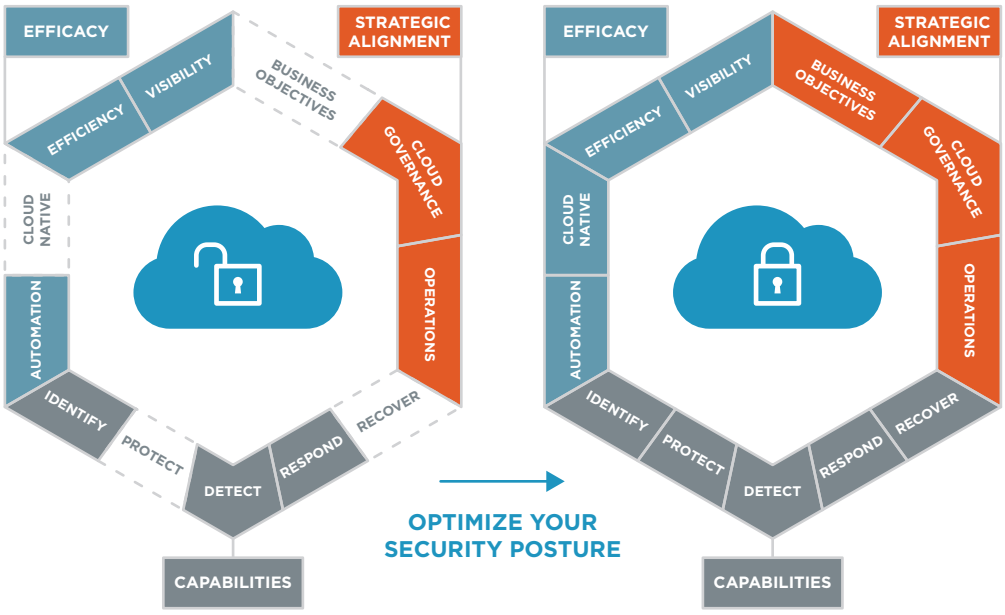
STRATEGIC ALIGNMENT – How your organization's approach to planning and implementing cloud security aligns with enterprise goals, business requirements, and risk appetite

CAPABILITIES – How your organization has designed, implemented, and managed a detailed security controls program

EFFICACY – How your organization visualizes and monitors cloud security, drives efficient cloud usage, and supports DevSecOps

Coalfire's cloud assessment framework helps you identify security gaps in your cloud environment, minimize risk, and align cloud computing strategies to business objectives.

Cloud with confidence knowing you are operating safely and securely in the cloud.



ASSESSMENT PHASES

	Strategic alignment	Capabilities	Efficacy	Vision state	Initiatives and roadmap
INPUTS	Hold workshop to cover: • Business objectives/ requirements • Cloud strategies, initiatives, usage, and migration plans • Governance targets and frameworks	Use previous phase to review: • Security governance, security architecture and services, and security operations controls implementation • Capabilities inspection	Use previous phases to review implementation and future potential for efficacy of security governance, security architecture and services, and security operations	Use previous phases to create a vision state around strategic alignment, capabilities, and efficacy	• Develop and prioritize recommendations • Categorize recommendations into projects • Develop strategic roadmap • Determine milestones, timelines, and dependencies • Identify risks for project completion
OUTPUTS	1. Core business mission and objectives inventory 2. Enterprise vision and policies 3. Risk requirements inventory 4. Identified controls frameworks and requirements 5. Observed maturity of strategic alignment to delivery of identify, protect, detect, respond, and recover objectives 6. Strategic alignment target maturity	1. Inventory of current services, contractors, licensing, etc. 2. Observed maturity of capabilities to delivery of identify, protect, detect, respond, and recover objectives 3. Capabilities target maturity	1. Inventory of existing services and approaches to support proper efficacy 2. Observed maturity of efficacy to delivery of identify, protect, detect, respond, and recover objectives 3. Efficacy target maturity	Vision state strategy alignment, capabilities (governance, architecture, and operations), and efficacy (governance, architecture, and operations)	1. Prioritized recommendations and capability roadmap 2. Identification of projects from a people, process, and technology perspective to reach strategic alignment, capabilities, and efficacy vision states

WHY COALFIRE?

- **Full lifecycle cybersecurity service provider:** Our CSM engineers have access to a full array of resources to help advise on requirements seen in all types of environments.
- **Partnerships across the top CSPs:** Through partnerships with the top-tier CSPs, we gain better insights into the architecture, configuration, and management of your security environment, so we can ensure it adheres to current CSP and industry best practices.
- **Deep technical knowledge:** Our CSM team comprises individuals who have spent years designing, building, and operating cloud environments. Our experience includes builds that meet some of the most complex technical requirements across any CSP.
- **Vast experience:** We have helped government organizations and companies in the financial services, healthcare, higher education, oil and gas, technology, and retail industries with cloud migrations, cloud greenfield builds, cloud deployments, and globally distributed environments.

DS_CSM_050720

SAFEGUARD YOUR MOVE TO THE CLOUD.

Learn more about Coalfire's cloud security maturity model.

Coalfire.com | 877.224.8077

COALFIRE

About Coalfire

Coalfire is the trusted cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for nearly 20 years and has offices throughout the United States and Europe. For more information, visit **Coalfire.com.**