Cyber Security Architecture Management (CSAM)

ADMG
Advanced Design Management Group

After years of hardening Security Programs, it has become clear that Effective Enterprise Security Management requires a Robust Enterprise Architecture Partnership. Understanding the Connected and Evolving Enterprise Operating Model is critical for Protection, Detection, Response, and Recovery through the Creation of a Cyber Security Architecture Blueprint. The CSAM Ecosystem supports planning and decision-making by bringing together information from various functions including Program/Project Portfolio Management, Provisioning, Risk and Compliance Management, Operational Security & Performance Monitoring, eDiscovery, IT Service Management, Disaster Recovery, Enterprise Security Management, and IT Asset Management. Benefits include improved organizational understanding of the business context for resources to support critical functions and related cybersecurity risks allowing the organization to focus and prioritize efforts, consistent with risk management strategy and business needs

The CSAM Blueprint provides new levels of transparency for business stakeholders and technology owners with the ability to answer important technology portfolio planning questions such as:

1- What critical applications have the greatest threat exposure with security control gaps?

2- Where is the sensitive information at rest or in transit?

3- Are there appropriate roles, skills, and accountabilities to protect the landscape?

4- What applications and technologies are about to go unsupported due to their end-of-life?

5- What business activities are impacted?

6- How do the current application and technology remediation plans mitigate future security risk?

The CSAM Blueprint provides improved visibility to implement safeguards to ensure delivery of critical infrastructure services, implement detection activities to timely identify the occurrence of a cybersecurity event, implement response activities to take action regarding a detected event to contain the impact, and maintain plans for resilience which restore any capabilities or services that were impaired due to the event. Understanding the answers to the Blueprint questions enables the IT security teams to focus their efforts on proactively addressing the security vulnerabilities for applications and technologies that support the most sensitive assets and have the highest exposure to cyber threats. The CSAM configuration can be implemented on a number of EA Platforms and can include CSAM Libraries which include 1- NIST Controls and Supplemental Guidance, 2- Federal Information Security Classifications, and 3-NICE Cyber Security Roles and Skills.

Author: Ed McPherson
June 2021

To learn more about ADMG, visit **EAStrategy.com** or contact us at **info@eastrategy.com**