



AUBURN

Course Wrap Up Topics



3 Pillars of a Cyber Security Organization

Governance

Ensures security program meets strategic business requirements

- Steering Committee
- Resource allocation and annual objectives
- Define and approve policies and standards
- Assess risks and remediation progress
- Review reporting and metrics for compliance and risk
- Monitoring operational performance

Security Management

Identify and oversees the security program

- Management of the security program
- Security policy/standards development and implementation
- Security architecture across cloud and assets
- Security awareness and education
- Projects to implement new security infrastructure
- Security guidance for non-security projects
- Security testing, audit and assurance
- Industry compliance programs

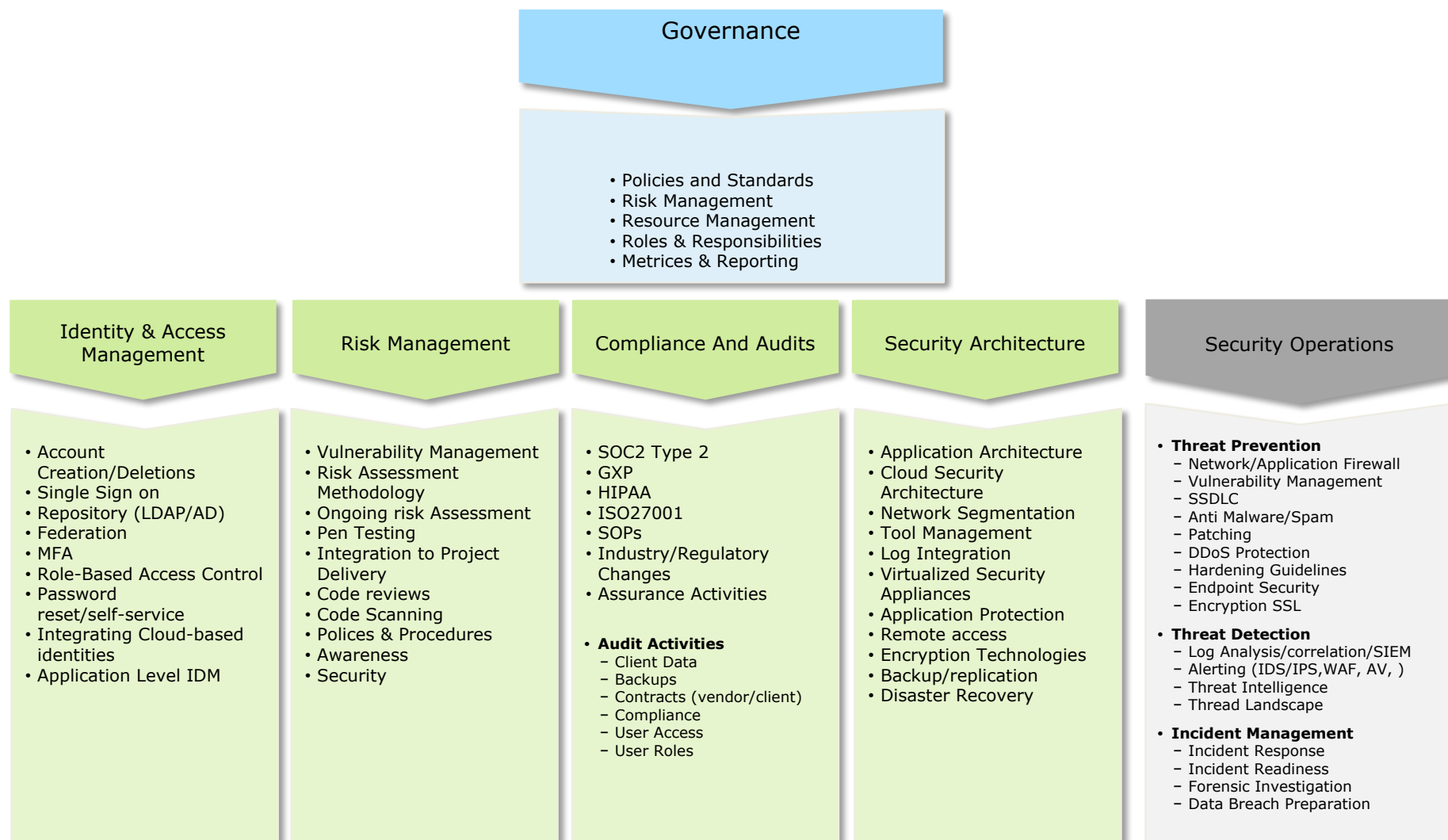
Security Operations

Mitigates security risks on a daily basis

- Monitoring and responding to security events
- Provisioning and deprovisioning access rights
- Providing input on the deployment of patches
- Monitoring vulnerability management processes and technologies
- Keeping current on changes to the threat landscape
- Maintaining and monitoring the technical security architecture
- Planning and participation in response to incidents
- Deploying patches for security products

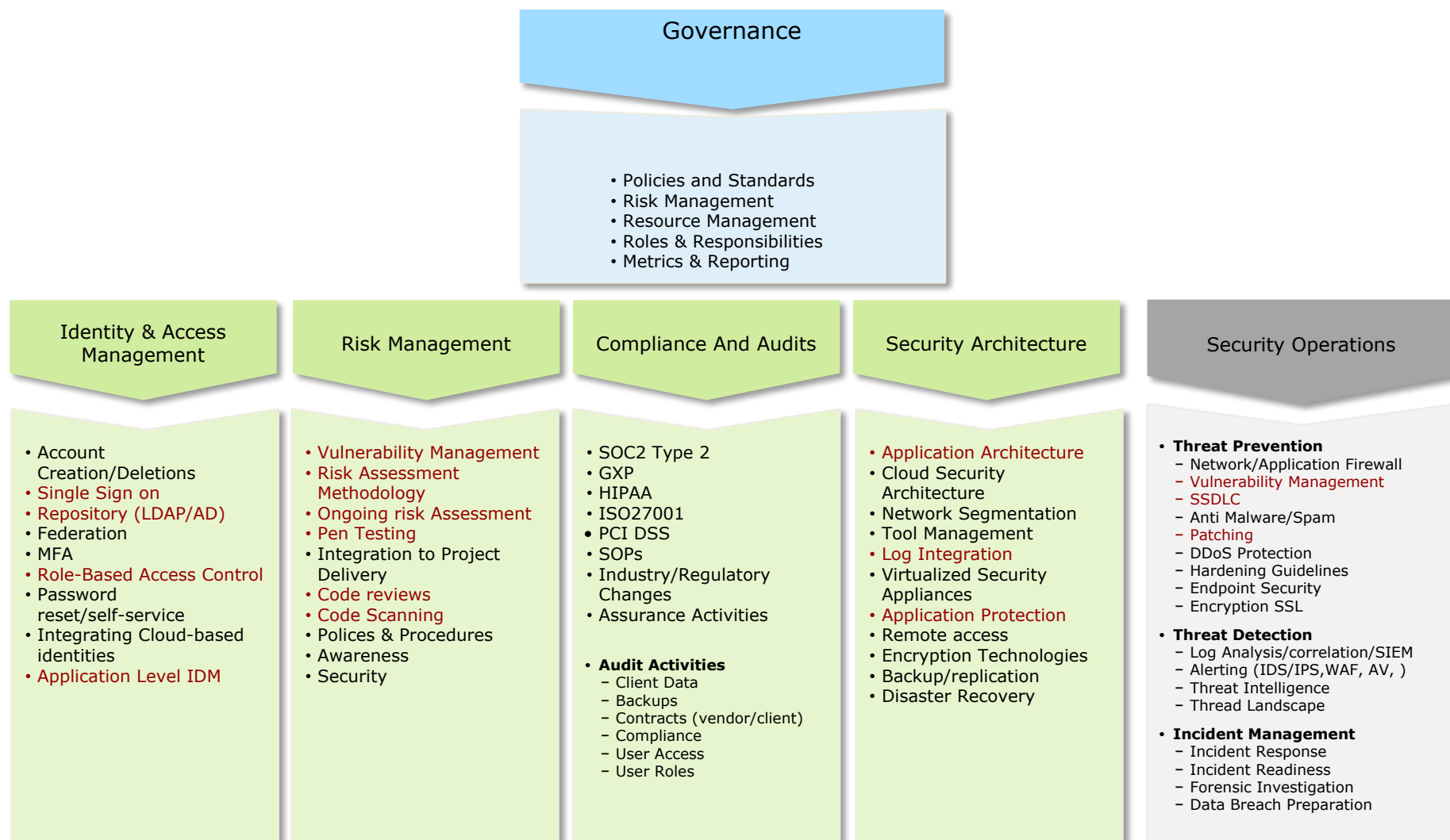


Organization Expanded View





Organization Expanded View





Security as a Software Engineer

- Threat landscape changes continuously
 - Technology changing more rapidly than ever
 - New languages, stacks, cloud services, apps
 - Systems are becoming more open and spread across services
 - Driven by cloud adoption and pervasiveness web applications in business and person lives
 - Technologies such as micro services, cloud services, multi-cloud create new thread landscape areas
- Assessing Risk plays an important part
 - Security testing needs to be driven by evaluating the areas that can potentially cause harm if breached.
 - Compliance risk, data leakage risk, open source risk, supplier/3rd party risk, reputation risk, etc.
 - Drives security tools that need to be employed



Security as a Software Engineer

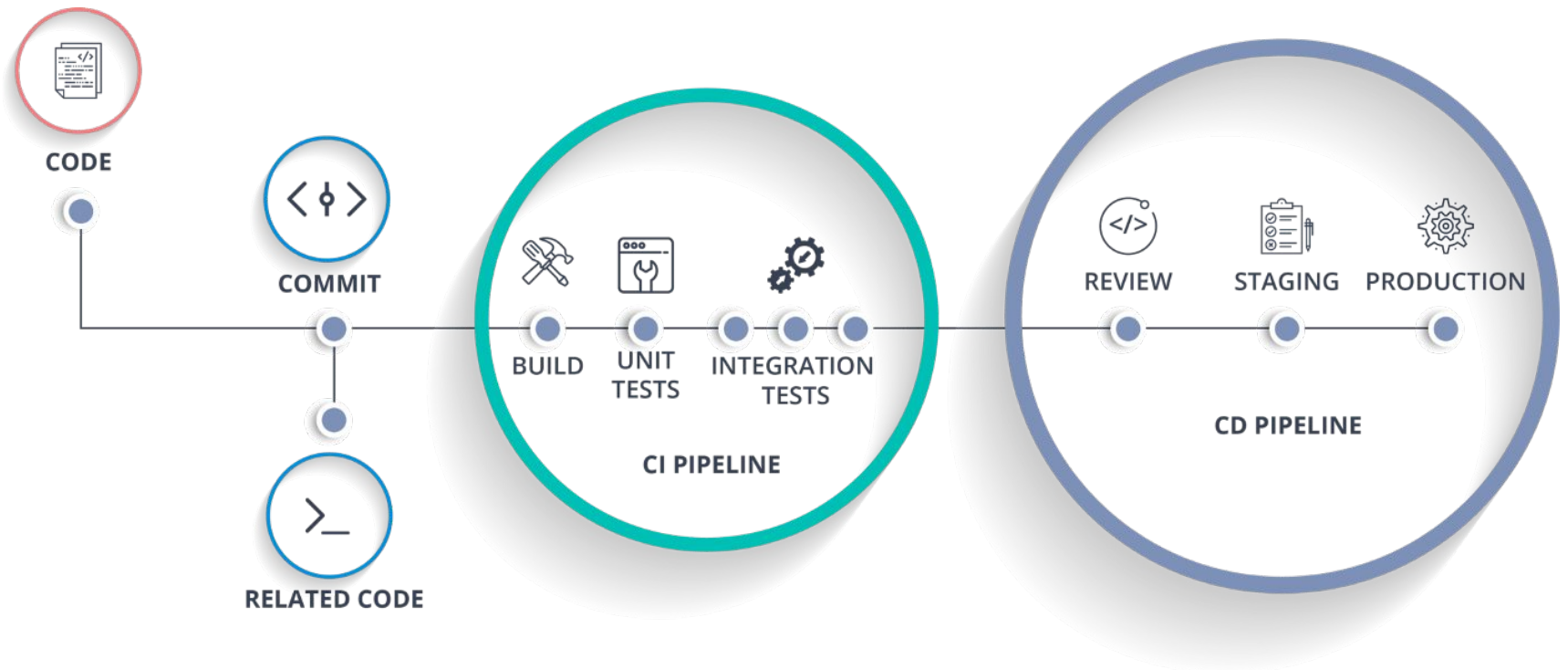
- Risk assessment and security tools allow development teams to identify, classify, and remediate weaknesses found during automated analysis & testing
 - Code review and inspection with security lens
 - Dependency scanning to verify software composition
 - Static application security testing (SAST)
 - Dynamic application security testing (DAST)
- Expect pushback when trying to adopt new security tooling, especially when impacting the Agile development process.
 - Educate teams that the benefit of using these tools is in the analysis coming from the tool and not the automation that runs the analysis.
 - Integrating security within the CI/CD pipeline helps streamline your DevSecOps tool chain.



Security as a Software Engineer

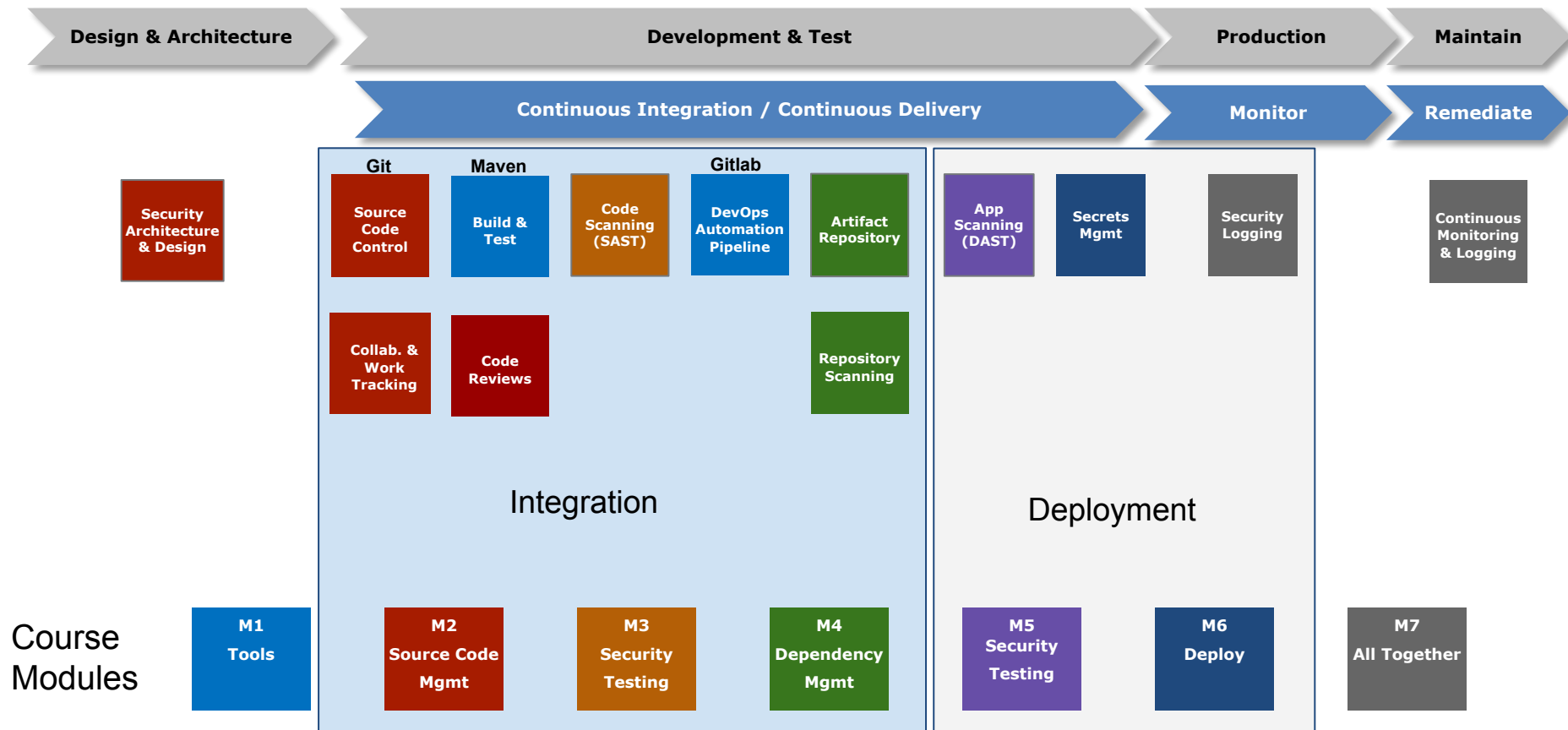
- Important to be proactive instead of reactive when dealing with security issues.
 - A reactive organization is responding to ongoing issues as they come
 - A proactive organization is taking necessary steps incorporating security tools to reduce weaknesses before they are live in production.
- Reactive approach - only focus on addressing known Common Vulnerabilities and Exposures (CVEs) in your software
- Proactive approach - focus on Common Weakness Enumeration (CWE) that exist for you specific software system, examining for weakness based on your software technology and structure as developers are coding.
- Build strong security inspection and testing automation from the first line of code.

DevSecOps





DevSecOps Pipeline





AUBURN UNIVERSITY
