



# IMPLEMENTATION OF OWASP SAMM IN K12 SCHOOLS

---

Deveeshree Nayak  
Assistant Teaching Professor  
University of Washington Tacoma  
<https://www.linkedin.com/in/deveeshree/>

# Agenda

K-12 Cyber Threats and Trends

Integrating SAMM in K12 Planning Process

Resources For K12 Education

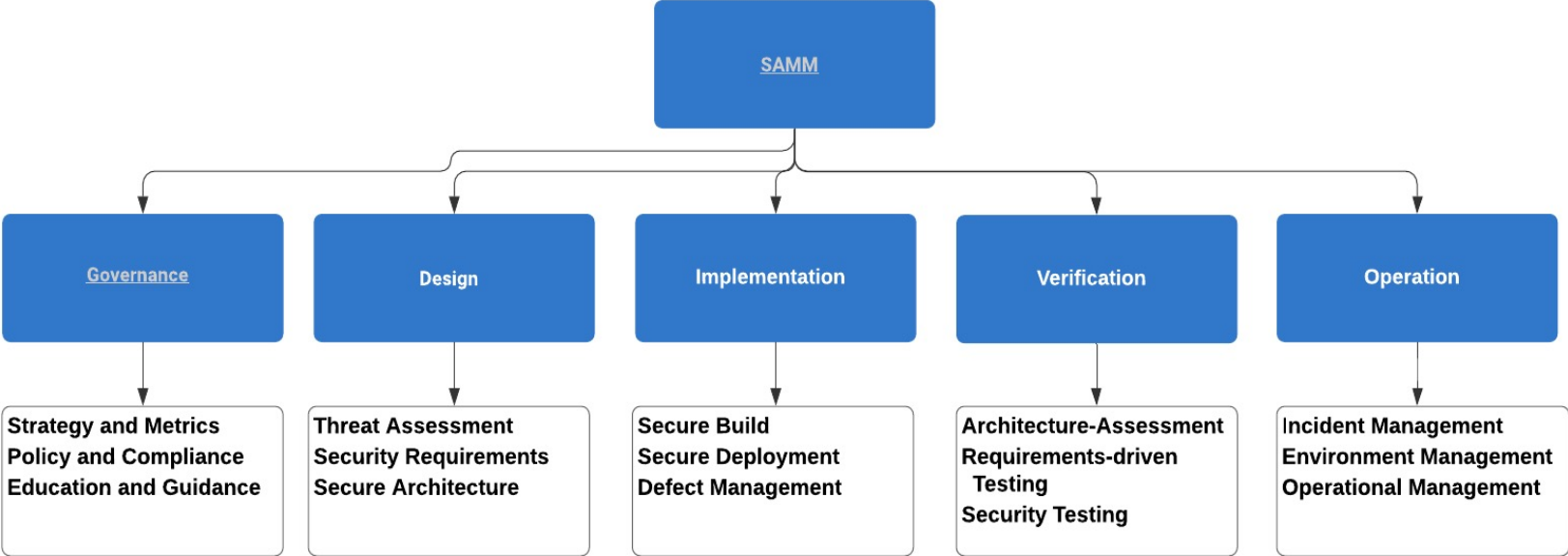
Q/A

# K-12 Cyber Threats and Trends

## Eastern Hancock hit with ransomware attack

By **Jessica Karins** - 5/25/21 10:03 PM

# SAMM



# Governance

## Strategy and Metrics

- Identify objectives and means of measuring effectiveness of the security program

- Establish a unified strategic roadmap for software security within the organization.

- Align security efforts with the relevant organizational indicators and asset values.

## Policy and Compliance

- Identify and document governance and compliance drivers relevant to the organization.

- Establish application-specific security and compliance baseline.

- Measure adherence to policies, standards, and 3rd-party requirements.

## Education and Guidance

- Offer staff access to resources around the topics of secure development and deployment

- Educate all personnel in the software lifecycle with technology and role-specific guidance on secure development.

- Develop in-house training programs facilitated by developers across different teams.

# Governance For K12

## Strategy and Metrics

Determine the security goals of K12 institutions and create a roadmap to implementing Cyber Security programs

## Policy and Compliance

Analyze the policies already in place (E.g. FERPA)

Develop documentation process of future policies, standards and requirements

## Education and Guidance

Offer Administrators, Educators, Human Resources, Transportation Managers, EMS, IT staffs, School Psychologists, and anyone who works at the k12 system access to free resources around the topics of secure development and deployment

# Design

## Threat Assessment

- Best-effort identification of high-level threats to the organization and individual projects.
- Standardization and enterprise-wide analysis of software-related threats within the organization.
- Proactive improvement of threat coverage throughout the organization.

## Security Requirements

- Consider security explicitly during the software requirements process.
- Increase granularity of security requirements derived from business logic and known risks.
- Mandate security requirements process for all software projects and third-party dependencies.

## Secure Architecture

- Insert consideration of proactive security guidance into the software design process.
- Direct the software design process toward known secure services and secure-by-default designs
- Formally control the software design process and validate utilization of secure components.

# Design For K12

## Threat Assessment

Determine the threat level by conducting threat assessments and offer security training to all departments of K12

## Security Requirements

Determine the known risks and adopt a long term security plan

Mandate security requirements process for all technologies used in k12 institution and update them in a timely manner

## Secure Architecture

Proactively remind students about the secure-by-default designs concepts



# Implementation

## Secure Build

- Build process is repeatable and consistent

- Build process is optimized and fully integrated into the workflow.

- Build process helps prevent known defects from entering the production environment

## Secure Deployment

- Deployment processes are fully documented.

- Deployment processes include security verification milestones.

- Deployment process is fully automated and incorporates automated verification of all critical milestones.

## Defect Management

- All defects are tracked within each project.

- Defect tracking used to influence the deployment process.

- Defect tracking across multiple components is used to help reduce the number of new defects.

# Implementation For K12

## Secure Build

Build process and objective for each know Cyber threat, integrate them with the K12 practice workflow

## Secure Deployment

Document each step and process timely manner during assessment and verify the correctness of it as well

Deploy and assign an Information Security person or someone who is trained in Cyber Security

## Defect Management

Track risks through risk assessment and seek help to reduce the number of risks

# Verification

## Architecture Assessment

- Review the architecture to ensure baseline mitigations are in place for typical risks.
- Review the complete provision of security mechanisms in the architecture.
- Review the architecture effectiveness and feedback results to improve the security architecture.

## Requirements-driven Testing

- Opportunistically find basic vulnerabilities and other security issues.
- Perform implementation review to discover application-specific risks against the security requirements.
- Maintain the application security level after bug fixes, changes or during maintenance.

## Security Testing

- Perform security testing (both manual and tool based) to discover security defects.
- Make security testing during development completer and more efficient through automation complemented with regular manual security penetration tests.
- Embed security testing as part of the development and deployment processes.

# Verification for K12

## Architecture Assessment

Review the architectures of networks, Fire, Electric, Gas, Physical Security and Water to ensure baseline mitigations are in place for typical risks.

## Requirements-driven Testing

Conduct a thorough review after the security requirements in place to determine any specific risks

## Security Testing

Perform security testing (both manual and tool based) to discover security defects of Networks, Electric Connection, Water Source, Gas and other hazards

# Operations

## Incident Management

- Best-effort incident detection and handling
- Formal incident management process in place
- Mature incident management

## Environment Management

- Best-effort patching and hardening
- Formal process with baselines in place
- Conformity with continuously improving process enforced

## Operational Management

- Foundational Practices
- Managed, Responsive Processes
- Active Monitoring and Response

# Operations For K12

## Incident Management

Advise stakeholders to be ready to face any types of Cyber Attacks and conduct timely emergency drills

## Environment Management

Practice patching of security updates and improve security practices based on Security demands.

## Operational Management

Determine the lesson learned from the security tests and implement the correction

Focus on active monitoring, offer importance to physical security, be vigilant and respond to the incident timely manner

# Resources For K12 Education

<https://k12cybersecure.com/resources/k-12-cybersecurity-self-assessment/>

<https://k12cybersecure.com/wp-content/uploads/2020/08/example-k12-cybersecurity-report.pdf>

[https://rems.ed.gov/docs/K12\\_Cyber\\_Webinar\\_Final11\\_13\\_2014\[1\].pdf](https://rems.ed.gov/docs/K12_Cyber_Webinar_Final11_13_2014[1].pdf)

<https://rems.ed.gov/IntegratingCybersecurityForK12.aspx?AspxAutoDetectCookieSupport=1>

[https://rems.ed.gov/Resource\\_Plan\\_Basic\\_All\\_Hazard.aspx](https://rems.ed.gov/Resource_Plan_Basic_All_Hazard.aspx)

[https://rems.ed.gov/docs/School\\_Guide\\_508C.pdf](https://rems.ed.gov/docs/School_Guide_508C.pdf)

<https://www.k12cybersecurityconference.org/>

<https://www.nist.gov/news-events/events/2021/12/7th-annual-nice-k12-cybersecurity-education-conference>

[https://www.nist.gov/system/files/documents/2017/04/26/nice\\_k12\\_implementation\\_plan.pdf](https://www.nist.gov/system/files/documents/2017/04/26/nice_k12_implementation_plan.pdf)

<https://www.nsa.gov/resources/students-educators/k12-partnership/>

<https://www.ncsc.gov.uk/information/cyber-security-training-schools>

<https://www.iamcybersafe.org/s/>

<https://doe.sd.gov/schoolsafety/documents/Cybersecurity.pdf>

**Q/A**



**Thank You**