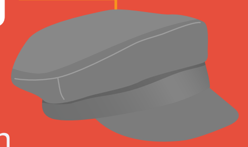
The Many HATS of an Information Security Officer

Do you have the right "hats" for your information security program?

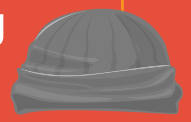
Risk Management

Perform threat analysis, estimate probability of occurrence, potential impact, and safeguards in place to measure risk.



Reporting

Responsible for reporting on the management and mitigation of info sec risk across the institution.

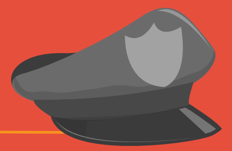


Security Testing

Ensuring adequate testing to validate controls are in place for the network and your people.

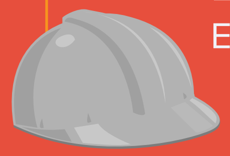
Disaster Recovery

Document resumption plan/process and test ability of business resumption based on unforeseen events within an established timeframe.



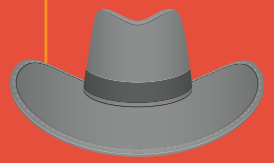
Incident Response

React, analyze, and respond appropriately to malicious activity. Develop and implant incident response plan.



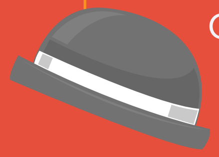
Education & Training

Ensuring enterprise-wide understanding of compliance environments.



Audit & Testing

Coordinating regular internal/external reviews, testing, and exception tracking.



Policies & Procedures

Creating and maintaining policies and procedures to ensure environment is structured and standardized.

Vendor Management

Identify critical vendors and perform ongoing oversight and evolution regarding your third party reliance.

Knowledge Share

Interpreting regulatory compliance and/or technology best practices, requirements, and law specific to your environment.

Program Development & Management

Ensuring a proactive strategic plan, processes, and controls are in place to achieve goals.

valasecure.com | ☎ (972) 429-8200

VALA SECURE