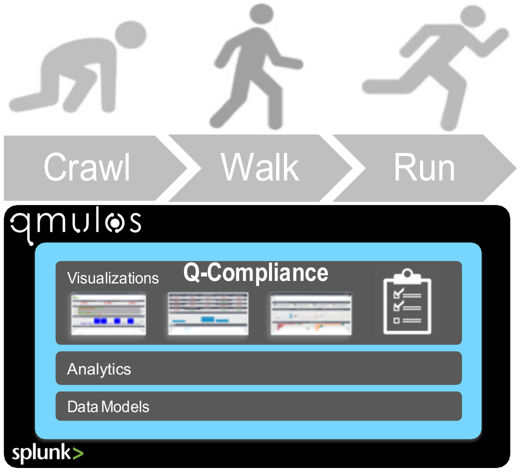
READINESS ASSESSMENT BRIEF

Q-Readiness Assessment

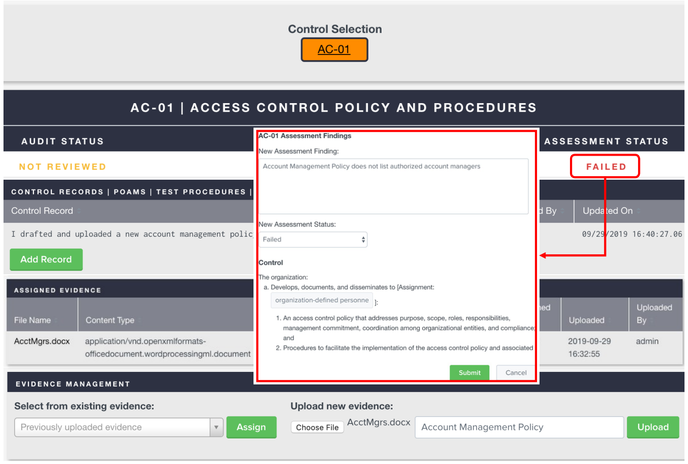
Crawl, Walk, and Run Towards Compliance with Real Operational Security Value



Achieving a strong security and compliance posture is not a Big Bang event. It is a journey in which organizations have to start with the basics and mature their people, processes, and technologies to develop the necessary capabilities. Part of this involves investing in the right tools that can grow and evolve with the organization. Qmulos' Q-Compliance is a best-in-class solution that allows organizations of any size, in any industry, at any level of maturity to streamline, automate, and improve their cybersecurity and compliance posture. With support for any maturity level, multiple compliance frameworks/regulations, and flexible pricing options, organizations can invest in a solution that grows with them in the continuously evolving cybersecurity landscape. Q-Compliance provides a flexible ***Crawl, Walk, and Run*** approach that allows organizations to quickly adopt industry best practices at any level of the cybersecurity and compliance maturity curve.

Crawl

Organizations in the "crawl" stage may not have all the security tools and capabilities to automate and continuously monitor their security controls. They may still be collecting and performing assessments manually and capturing the results in spreadsheets and other documents. Q-Compliance can benefit organizations in this stage with its capabilities that are similar to traditional Governance, Risk, and Compliance (GRC) tools such asthe ability to upload evidence (or link to a document repository), capture compliance work history, manually perform and capture the results of audits and assessments, and generate compliance artifacts such as System Security Plans (SSP). By adopting Q-Compliance in the crawl stage, organizations can replace their manual processes and disparate documents with a single tool and begin to build the foundation for a robust cybersecurity and compliance program built on industry best practices such as the Risk Management Framework, NIST SP 800-53 security controls, or other industry standards (such as HIPAA, PCI DSS, or even custom controls).



Control Selection

AC-01

AC-01 | ACCESS CONTROL POLICY AND PROCEDURES

AUDIT STATUS: NOT REVIEWED

ASSESSMENT STATUS: FAILED

CONTROL RECORDS | POAMS | TEST PROCEDURES |

Control Record	d By	Updated On
I drafted and uploaded a new account management polic		09/29/2019 16:40:27.06

ASSIGNED EVIDENCE

File Name	Content Type	ned	Uploaded	Uploaded By
AcctMgrs.docx	application/vnd.openxmlformats-officedocument.wordprocessingml.document		2019-09-29 16:32:55	admin

AC-01 Assessment Findings

New Assessment Finding:

Account Management Policy does not list authorized account managers

New Assessment Status:

Failed

Control

The organization:

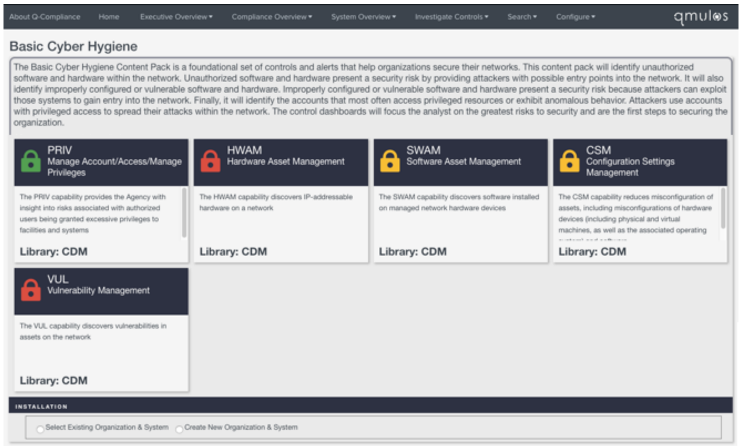
a. Develops, documents, and disseminates to [Assignment: organization-defined personne]:

1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the access control policy and associated

EVIDENCE MANAGEMENT

Select from existing evidence: Previously uploaded evidence

Upload new evidence: AcctMgrs.docx Account Management Policy



Basic Cyber Hygiene

The Basic Cyber Hygiene Content Pack is a foundational set of controls and alerts that help organizations secure their networks. This content pack will identify unauthorized software and hardware within the network. Unauthorized software and hardware present a security risk by providing attackers with possible entry points into the network. It will also identify improperly configured or vulnerable software and hardware. Improperly configured or vulnerable software and hardware present a security risk because attackers can exploit those systems to gain entry into the network. Finally, it will identify the accounts that most often access privileged resources or exhibit anomalous behavior. Attackers use accounts with privileged access to spread their attacks within the network. The control dashboards will focus the analyst on the greatest risks to security and are the first steps to securing the organization.

PRIV
Manage Account/Access/Manage Privileges
The PRIV capability provides the Agency with insight into risks associated with authorized users being granted excessive privileges to facilities and systems
Library: CDM

HWAM
Hardware Asset Management
The HWAM capability discovers IP-addressable hardware on a network
Library: CDM

SWAM
Software Asset Management
The SWAM capability discovers software installed on managed network hardware devices
Library: CDM

CSM
Configuration Settings Management
The CSM capability reduces misconfiguration of assets, including misconfigurations of hardware devices (including physical and virtual machines, as well as the associated operating
Library: CDM

VUL
Vulnerability Management
The VUL capability discovers vulnerabilities in assets on the network
Library: CDM

INSTALLATION

○ Select Existing Organization & System ○ Create New Organization & System

Walk

Organizations in the "walk" stage may be performing basic cyber hygiene functions such as identifying and managing their assets, scanning those assets for vulnerabilities, and implementing secure configurations on those assets. At this stage they may be producing technical evidence that can be ingested in Q-Compliance to begin continuously monitoring the effectiveness of these foundational security controls. Q-Compliance provides the "Basic Cyber Hygiene" content pack to enable organizations in this stage to quickly get started with monitoring these controls and prebuilt alerts