CYBERLEDGER

The Integration of Cyber Compliance, Posture, Intelligence, Resourcing, and Reporting

Today's rapidly evolving cyber landscape presents unprecedented challenges and opportunities for Federal leaders. Now more than ever, Chief Information Officers, Chief Financial Officers, Chief Information Security Officers, and their respective supporting staff must be equipped with end-to-end policies and tools that enable them to understand their organization's cyber security risk posture at an enterprise level.

Cyber threats to systems supporting the federal government and critical infrastructure are evolving and becoming more sophisticated. These threats come from a variety of sources and vary in terms of the types and capabilities of the actors, their willingness to act, and their motives.

The shared attributes of these cyber threats are:

Velocity—the speed by which new attacks are developed and propagate

Volume—the increase in cyber-attacks over the past decade has been exponential

Variety—the combination of modes and vectors of cyber attacks

Viciousness—there is a clear intent on the part of attackers to disrupt, damage, or destroy.

The bottom line is that Federal agencies are experiencing an ***Unrelenting*** barrage of cyber threats that disrupt agency operations, undermine public confidence and imperil mission objectives. Most agencies have an assorted collection of loosely integrated tools and capabilities to address these threats that does not provide reliable and actionable insight into the comprehensive cyber threat the agency faces.

CyberLedger is the consolidation and integration of cyber-focused capabilities that enable an organization to stay a step ahead of new threats and uncertainty by quantifying risks, optimizing and implementing the response, and disseminating the results. It is a data-driven approach to cyber risk management that provides an organization the insight and understanding necessary to continually addresses and mitigate risks and vulnerabilities to the "left-of-bang".

The CyberLedger integrated capabilities allow an organization to:

Assess and ***Quantify*** Cyber Compliance

Understand and ***Manage*** Cyber Posture

Adjust and ***Adapt*** to new Cyber Threats and Vulnerabilities

Justify and ***Allocate*** Resources—Budget, Time, People, and Political Capital, and

Collaborate and ***Share*** solutions

CyberLedger is a purpose-built Software-as-a-Service platform that can be deployed in either a hybrid or private cloud. It is designed specifically to support the integration of diverse data sources via tailorable APIs.

Our software has been architected to avoid tight-coupling of software to hardware, and for this reason our platform can be deployed to almost any cloud provider. The CyberLedger architecture incorporates numerous industry-leading best practices, including separation of concerns, responsive design and secure SaaS-based cloud solutions. By extending the separation of concerns to include hardware, such as the underlying servers and infrastructure, our solution can be hosted in any cloud without impacting the data, business logic or client tiers.

CYBERLEDGER

Security Compliance Assessment

This capability (Figure 1) provides continuous data driven analysis and visibility of security compliance across the enterprise and enabling holistic and consistent measurement of cyber security posture. Stakeholders can make informed, enterprise decisions based upon best practices and budgetary realities on where to focus cyber security efforts to improve the overall resiliency of functioning security controls.

***Figure 1: Assess** and **Quantify** Cyber Compliance*

Baseline data from Security Assessment Reports (SARs) comprise the foundation to analyze and evaluate compliance gaps to quickly identify areas of improvement. This data can either be generated in CyberLedger or imported from existing tools such as eMASS, Xacta, CSAM, and others.

The features in the Security Compliance Assessment capability include:

- Security control compliance scoring with security control implementation details at the Control Correlation Identifier (CCI) level
- Security control maturity level progress and compliance improvement target trends
- Authorization to Operate (ATO) compliance maintenance tracking metrics

Residual Risk Management

This capability (Figure 2) identifies and tracks progress in addressing residual risk across the organization's portfolio. It supports the identification, analysis, and mitigation of vulnerabilities to include prioritization and highlighting of high-risk vulnerabilities. This capability ingests existing open and past due Plan of Action & Milestones (POA&M), audit observations, and Technical Vulnerability Assessments (TVAs) from tools such as Fortify, Tenable and others.

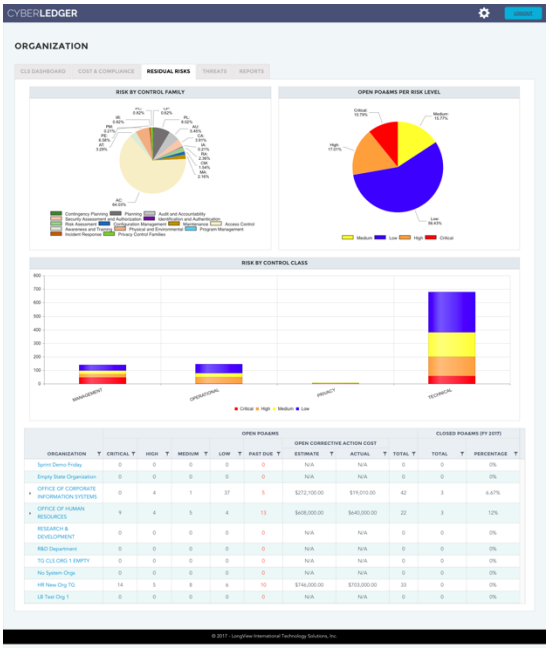

***Figure 2: Understand** and **Manage** Cyber Posture*

Unmitigated risks and activity details are incorporated into Plan of Action & Milestones (POA&M) to support the centralized management of corrective actions and solutions across the enterprise. The resulting POA&Ms can be retained in CyberLedger or exported to project management solutions such as PrimaVera or MS Project as well as standard office productivity applications.

The features in the Residual Risk Management capability include:

- Unified identification, tracking, and analysis of high risk vulnerabilities ingested from siloed scanning tools detailing outstanding network, application, server, and database vulnerabilities
- Centralized management and identification of effective corrective actions and solutions across the enterprise
- Identification, visualization, and evaluation of corrective action costs associated with residual risk mitigation

Risk and Threat Profile

This capability (Figure 3) offers dynamic risk and threat profile development in accordance with NIST SP 800-30 Rev. 1 Guide for Conducting Risk Assessments. It includes organization specific elements and criteria necessary to better align cyber resources and funding to address High Value Assets (HVA).

CyberLedger ingests threat intelligence and catalogs attack patterns In accordance with a comprehensive schema and classification taxonomy that can be used to evaluate how susceptible an asset may be to a particular threat. The threat sources include Mitre's CVE, CWE, CPE, and CAPEC as well as CVSS, TAXII, STIX, and CybOX. Vulnerability sources include Tenable, Trustwave, HP, and IBM.

The features of the Risk and Threat Profile capability include:

- Create risk & threat profiles in accordance with NIST SP 800-30 Rev. 1 Guide for Conducting Risk Assessments
- Ingest threat intelligence feeds using leading industry threat sources and in accordance with NIST guidelines
- Identify HVA in support of Cybersecurity Strategy and Information Plan for Federal Civilian Government (CSIP)
- Integrate HVA metrics with cost-benefit analysis to enrich cyber spending measurement tracking with prioritization to highest risk needs
- Conduct enterprise grading and prioritization for resources and susceptible threats

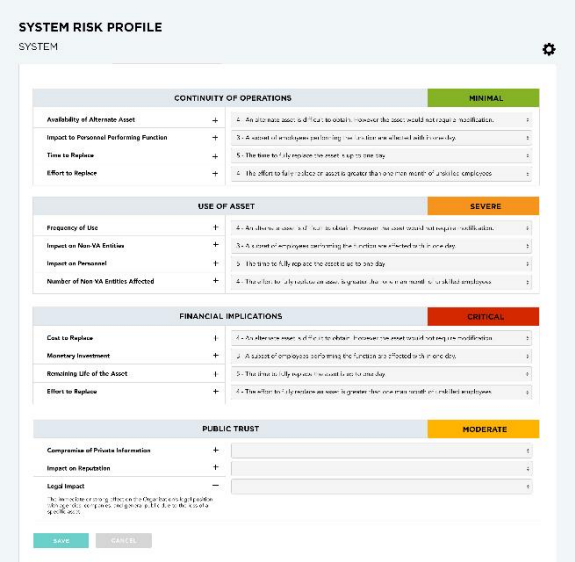

***Figure 3: Adjust** and **Adapt** to new Cyber Threats and Vulnerabilities*

Cost Benefit Analysis

This capability (Figure 4) supports the analysis, justification and allocation of available funding for the highest priority IT security investments. It recognizes the interdependencies of enterprise assets and facilitates the optimization of cyber security resources.

The analysis capability provides context and allows for multiple perspectives to conduct risk-based cost benefit analysis to support budget estimates.

The features of the Cost Benefit Analysis Capability include:

- Analyze and map interdependencies between enterprise asset vulnerabilities and contributing sub-enterprise asset and system vulnerability mitigation costs
- Manage current and out year budgets to maximize Cybersecurity maturity investment improvements
- Prioritize corrective action costs and impacts in relation to key risk performance indicators, (such as: asset value, security

compliance gap, threat susceptibility, and residual risk)
- Evaluate assets, threats, vulnerabilities, and countermeasures to determine activities that are most important to critical-service delivery and prioritize expenditures to maximize the impact of investments.

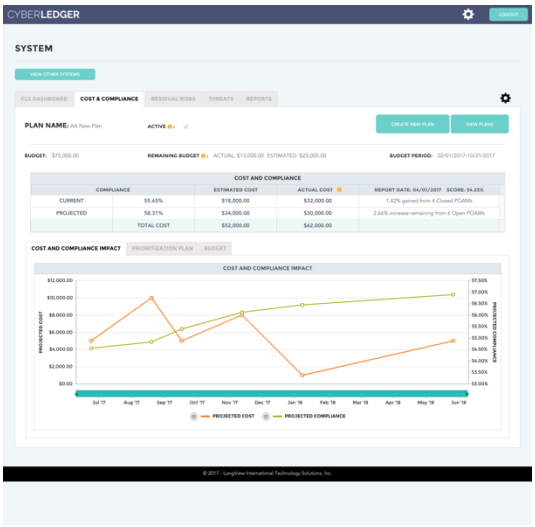

*Figure 4: **Justify** and **Allocate** Resources—Budget, Time, People, and Political Capital*

Cyber Security Framework (CSF) Reporting Capability

This capability (Figure 5) allows organizations a common framework to understand, collaborate and report their cyber posture. It supports cyber security maturity improvements for making better informed risk-based decisions through capabilities that assess and evaluate risks per NIST CSF functional areas. The capability allows users to design and develop a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state) based on the five concurrent and continuous CSF Functions - Identify, Protect, Detect, Respond, and Recover.

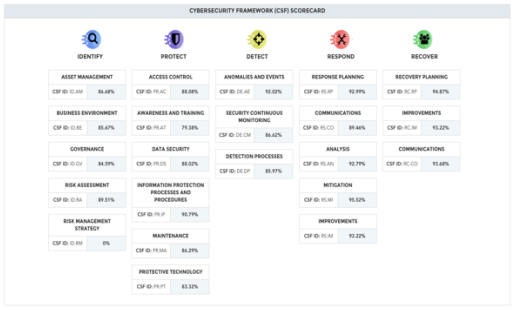

*Figure 5: **Collaborate** and **Share** solutions*

The features of the CSF Reporting capability include:

- Create custom target profiles using CSF functions on-demand and tailor security objectives based on the full catalog of NIST 800-53 Rev. 4 security controls
- Create current "as is" state and automated Cybersecurity posture calculation from security data available
- Create on-demand assessment of key performance indicators metering the progress towards defining target state
- Supports automated reports in either NIST CSF or RMF formats.

Summary

Organizations can benefit from a data-driven approach to cyber risk management that provides the insight and understanding necessary to continually addresses and mitigate risks and vulnerabilities to the "left-of-bang".

Benefits of CyberLedger

- Decrease the number of attack planes
- Reduce redundancy of solutions
- Reduce costs (via cost avoidance)
- Reduce the impact to operations
- Improve information quality
- Improve decision-making and resource allocation
- Increase responsiveness and resiliency.