



CYBER THREAT ASSESSMENT

Identify and address your organization's cybersecurity threats so that you can protect your business and brand for generations to come.

Reviewing and understanding your business environment, critical systems and processes, views of stakeholders, policy maturity and their interconnectivity, are more important than ever before. Valor utilizes industry best practices, along with qualitative and quantitative measures to clarify risk for leaders and their people. We recommend action-based strategies to help your organization make informed decisions around the threats that impact you most. Our Cyber Threat Assessment provides you with the insight you need to build a strong, sustainable cybersecurity program.

SIMPLIFIED CYBERSECURITY DELIVERED

2023

Our Approach

Our assessment process is built based on industry-recognized security frameworks, including the NIST CSF, NIST 800-53, CIS Top 18, and PCI DSS. We leverage an established capability maturity model index (CMMI) to objectively evaluate your program and provide realistic maturity rankings across industry standards.



Phase 1: Project Planning and Kick-Off

During Phase 1, the Valor team collaborates with you to establish the objectives and scope for this engagement, as well as communication methods and a cadence for status reporting. Following this initial step, we coordinate document and interview requests with your team.

- ◆ Clear engagement objectives
- ◆ Document and interview requests
- ◆ Established communication methods



Phase 2: Program Analysis

During Phase 2, our team holds both on-site and remote discovery sessions with key stakeholder and subject matter experts within your organization. Following this step, our team builds a current state gap analysis of your policies, procedures and technologies against industry standards.

Using our Capability Maturity Model, we evaluate each domain across your security program. As a result of this analysis, we are able to identify process inefficiencies and areas for improvement.

- ◆ Analysis of the current conditions of your IT infrastructure, business processes and utilized technologies
- ◆ Identify process inefficiencies and areas for improvement
- ◆ Understanding of the confidentiality, integrity and availability of business systems



Phase 3: Strategic Roadmap

In the final phase of the Valor assessment, our team communicates the findings of our analysis to your leadership team, helping you gain executive buy-in for the most immediate risks facing your organization.

During this phase, we establish achievable target cyber maturity goals for your program, provide future state recommendations and deliver an action-based roadmap for short-term and long term cyber maturity.

- ◆ Alignment across cybersecurity priorities, organizational objectives and policies
- ◆ Improved decision-making around the level of risk associated with the current business environment
- ◆ More efficient resource allocation
- ◆ Increased investment in future projects

Assessment Focus Areas

Access Control	Asset Management	Audit and Accountability
Awareness and Training	Configuration Management	Identification and Authentication
Incident Response	Maintenance	Media Protection
Personnel Security	Physical Protection	Recovery
Risk Management	Security Assessment	Situational Awareness
System and Communications Protections	System and Information Integrity	Data Privacy

Valor Success Story

Effectively Assessing Cyber Threats to Help a World-Class Private Equity Firm Make Informed Decisions

Valor led the threat assessment and evaluation of all cyber-related due diligence activities for a multi-million dollar equity transaction. The merged U.S.-based firm has more than 2,000 users across 5 countries.

6

Week Timeline

Valor completed this implementation in just 2 months.

20

Applications

The scope for this global implementation.

Different From the Rest

At Valor, we take a different approach to identifying and addressing cyber threats.



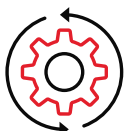
Actionable Deliverables

Our assessment process doesn't just point out your weaknesses and the urgent need for change. It provides clear, action-based guidance for addressing key security threats and improving your overall risk posture.



Ongoing Support

We never deliver a report and leave our partners, we often stay on board to help them implement our recommendations and mature their security posture. We work hard to collaboratively help execute your strategic roadmap.



End-to-End Services

Valor provides a full lifecycle suite of services and end-to-end support services. We have experts in security program development, data privacy, and business resilience to help you improve across all risk domains.

Partner with Valor today to see how we can help meet your readiness objectives. Contact Valor at info@valor-cybersecurity.com

400 Granby Ave | Norfolk, Virginia 23510 | USA

VALOR
CYBERSECURITY