

CYBERSECURITY ASSESSMENT

Cybersecurity risk and maturity - where are you? Good security starts with visibility and awareness - the more you know the better you can protect against today's threats. Unfortunately many organizations find themselves asking how secure they truly are, especially in today's world of ever changing attacks. Find out with our GoSecure Cybersecurity Assessment.

KEY BENEFITS

- Provide external expert perspective to executive management
- Gain understanding of your cybersecurity state
- Identify cybersecurity-gaps and related risk to business
- Evaluation of current state cybersecurity maturity
- Gain actionable recommendations quickly
- Help guide your cybersecurity roadmap

Assess Your Cybersecurity Posture to Better Protect your Organization

The GoSecure Cybersecurity Assessment (CSA) is an assessment of the overall state of your cybersecurity so that you can strategically plan and tactically improve your posture. Our CSA assesses your strategic control environment and references against industry best practices established in respected standards and frameworks such as ISO/IEC 27001/27002:2013 and NIST CSF. The CSA assesses and tests vulnerabilities within your tactical control environment; vulnerabilities which expose your business to threat events.

GoSecure CSA results are contextualized to your business, as well as to organizations of comparable size, type and industry. As part of the CSA, we provide you with prioritized recommendations which are targeted to helping you improve your business' overall cybersecurity. The standard CSA encompasses the following phases:

- Cybersecurity Governance Review
- Cybersecurity Infrastructure Review
- External/Internal Intrusion Tests
- Web Application Intrusion Tests
- Social Engineering

General Objective and Scope

The CSA-Essentials assesses the organization's strategic and tactical security within a defined scope and focuses around areas of cybersecurity that have the highest potential likelihood of incidents and breaches for small and medium businesses. The following cybersecurity categories were addressed as part of the engagement:

- Asset Management
- Human Resource Security
- Information Security Incident Management
- Information System Security
- Network Security Architecture
- Wireless Access Security
- Network Traffic Inspection
- Server and Workstation Security
- Services Security

Note: see Appendix 2 and 3 for descriptions of the CSA categorizations.

Our Cybersecurity Assessment Approach

GoSecure's Cybersecurity Assessment (CSA) methodology is founded on leading international information security standards and current best practices. The CSA is designed to evaluate an organization's cybersecurity posture and capabilities.

Though not scoped within the CSA-Essentials, areas with relatively lower likelihood of incidents and breaches may still constitute important risks to the context and particularities of your organization. As such, it is recommended that a more complete form of cybersecurity assessment be performed as your organization improves its cybersecurity overtime.

Results and Priorities

1.1 Network Segmentation and Isolation

1.2 Network Service and Infrastructure Resilience

Observations

- Isolation rules are permissive. This includes lack of security controls across critical server zones.
- The internal network is strategically zoned into VLAN segments however, these zones are not designed for security. For example, user workstations are in the same zone as servers.
- The management zone in the internal network is not sufficiently isolated from other zones.
- The internal network is isolated from the Internet, but there are Internet-facing services that are placed in the internal trusted zones of the network and not in a separate DMZ.

Recommendations

- Define user access by role or groups. Ensure that users are only assigned to roles and groups with the least required permissions to perform their job responsibilities.
- Implement separate segments for each user workstation and server. Ensure that isolation rules between these segments are restricted to the least required resources between these segments.
- Implement out-of-band restriction that limit accesses to the least required for business operations. Also, ensure that all Internet-facing services are well controlled for security within the DMZ.
- Develop an information technology policy framework that can be challenging as it depends on the specific needs of each organization.

References

ISO/IEC 27001:2013 A.1.1.1 - Information security roles and responsibilities
 NIST CSF 1.1.1 - 1.1.2 - Segregation of duties
 NIST CSF 1.1.1.4 - 1.1.1.4 - Segregation of duties
 NIST CSF 1.1.1.4 - 1.1.1.4 - Segregation of duties

IS THE GOSECURE CYBERSECURITY ASSESSMENT FOR ME?

The GoSecure CSA is intended for organizations interested in validating, developing or better understand their business's cybersecurity posture and risks. To this end, the CSA is uniquely designed to provide you with cost-effective and high-value cybersecurity insights that are contextualized to your business. The CSA provides you with actionable recommendations, including activities which can be implemented quickly whilst ensuring minimal impact to business operations. With the CSA, you benefit from our 16 years of cybersecurity expertise and operational know-how. It prioritizes activities to enable you bridge cybersecurity gaps between your business' current posture and target objectives.

Why GoSecure Cybersecurity Assessment?

While conventional assessment services limit themselves to a top-down only evaluation, the GoSecure CSA applies a combined top-down and bottom-up approach to provide you with a truly holistic and robust depiction of your organization's cybersecurity. Our signature CSA approach leverages the complementary expertise of our advisory services and ethical hacking to provide you with actionable insights and recommendations. Our advisory group specializes in strategic-level control assessments of the management, technical and administrative controls that safeguard your information environment while our ethical hacking team performs tactical-level verifications of your technical environments to validate the effectiveness of implemented security controls.

Gain a holistic depiction of your organization's cybersecurity posture by examining both strategic security and tactical operational security.

