DGC
ACCOUNTING • TAX • ADVISORY

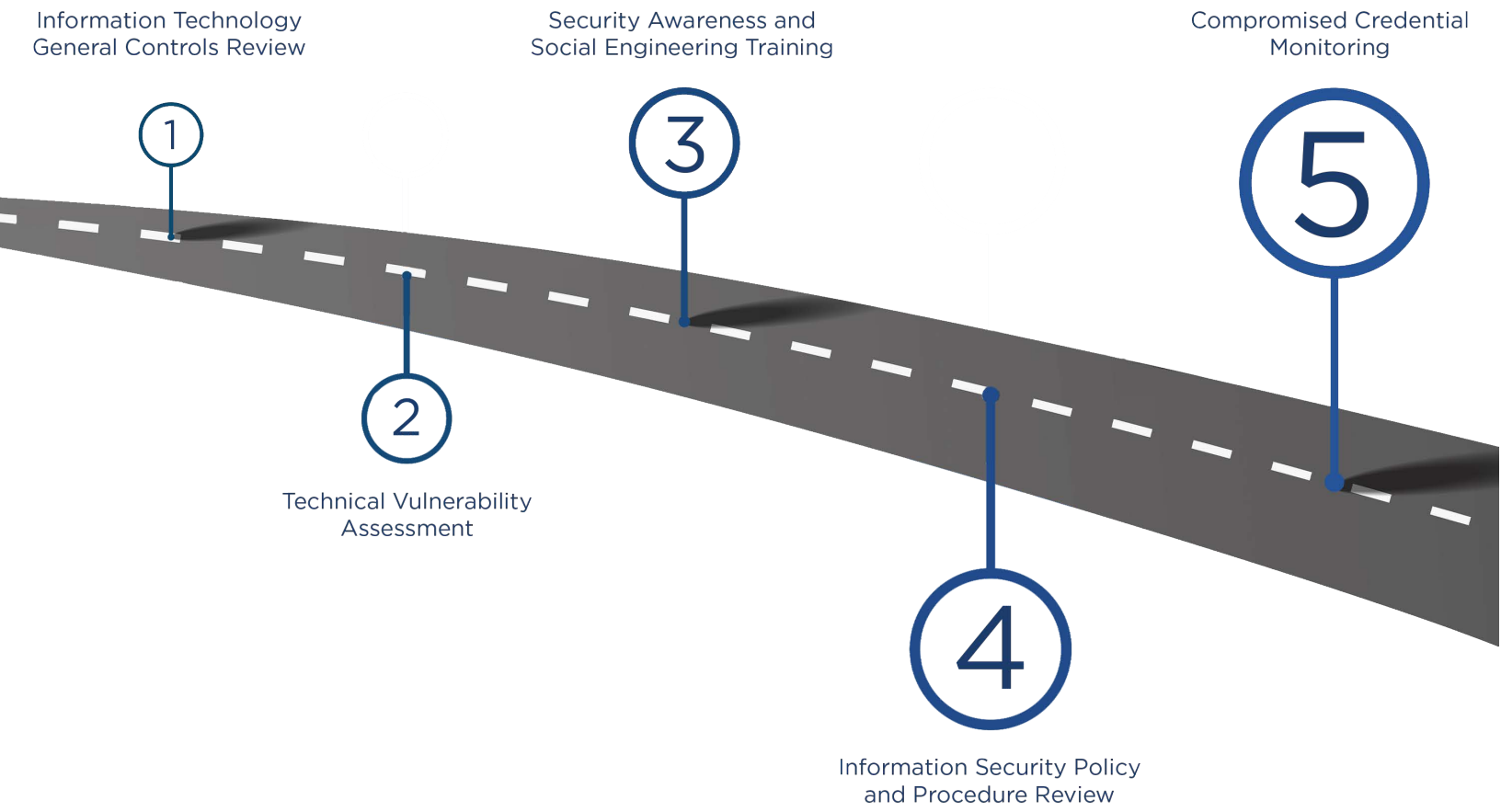
OVERVIEW

Information Security Roadmap Assessment

It's no secret that information security breaches are on the rise, affecting organizations of all sizes, and in all industries. Organizations in certain regulated industries are forced to address these threats because they are contractually or legally obligated to design and implement comprehensive information security programs. However, what if you don't operate in a regulated industry?

While non-regulated organizations are subject to the same threats as those within regulated industries, they have no enforced roadmap for the development, implementation, or management of an information security program. The toughest question facing these organizations is often, "Where do I even start?".

With our InfoSec Roadmap Assessment, DGC helps these types of less-regulated organizations to develop a roadmap for information security which is right-sized and immediately actionable. The DGC InfoSec Roadmap Assessment includes the following components which are designed to measure an organization's security maturity and provide a roadmap for risk mitigation.



(Continued)

Information Security Roadmap Assessment (cont.)

1. Information Technology General Controls Review

DGC helps organizations tackle that tough first question of, "Where do I start?" by selecting an industry-standard information security framework against which to assess their information security maturity. To this end, DGC leverages the Center for Internet Security (CIS) Top 20 Critical Security Controls, a framework that can be customized to the overall size and relative maturity of a company's information security program. The CIS Top 20 represents a prioritized set of actions which are designed to protect your organization and data from known cyber-attack vectors.

Following discussion and walkthrough with management and IT personnel, the result of this assessment is a formal view of the information security controls which have been implemented by the organization, as well as a list of technical and administrative gaps with associated recommendations for remediation.

2. Technical Vulnerability Assessment

While the IT General Controls Review component of the Roadmap Assessment relies on a review of current processes, procedures, and tools against an industry benchmark, the technical vulnerability assessment is designed to identify actual exploitable vulnerabilities on the organization's network. Via a combination of automated scans and manual vulnerability analysis, the DGC team provides a comprehensive view of the vulnerabilities and misconfigurations which exist in the environment.

The result of this assessment includes a technical vulnerability report, which identifies individual systems and network services which could be exploited by an attacker to gain a foothold in the environment, along with recommendations to close these attack vectors.

3. Security Awareness and Social Engineering Training

No information security program is complete without the development and implementation of security awareness training for employees. Without this required component, security controls, processes, and procedures -- no matter how well-designed, will never operate effectively.

DGC manages a training platform on behalf of the organization to provide web-based information security training to all employees. A critical and included component of this platform is the execution of simulated "phishing" attacks, where the DGC team will send fake emails to employees which imitate real-life attacks. Users who click on these simulated phishing links or open attachments are subject to additional training, and periodic reporting is available to management. This training and awareness program is designed to protect the organization against real phishing attacks, which are still the number one way that hackers breach corporate networks.

(Continued)

Information Security Roadmap Assessment (cont.)

4. Information Security Policy and Procedure Review

An often-overlooked component of many nascent information security programs is an assessment of those compliance requirements to which your organization may *already* be subject. Many states require the implementation and documentation of certain information security controls which are designed to protect the personal information of state residents which may be collected, held, or processed by the organization. These standards often also include dedicated information security breach reporting requirements.

If your organization has not identified the relevant standards and developed the appropriate documentation, then you are already at risk of non-compliance in the event of a security incident. Fines issued as a result of a security incident are often related to the quality of the information security program that was in place at the time of the breach, meaning an organization that is under-prepared often faces higher fines than one that has conducted their due diligence. The DGC Roadmap Assessment includes a review of information security policies against relevant standards, in order to provide recommendations to close identified process gaps.

5. Compromised Credential Monitoring

While most components of the DGC Roadmap Assessment focus on the identification and mitigation of risks which are internal to the organization, compromised credential monitoring is geared towards identifying risks which exist externally. The pervasive reuse of corporate email addresses and passwords across public third-party services puts the organization at risk if any of these third parties are breached. For example, consider the LinkedIn breach from 2012. Thousands of email addresses and passwords were stolen from the social networking giant as a result of this breach. If these email addresses and passwords were valid in your environment, then this third-party breach could have significant consequences for your organization, even though the breach itself occurred entirely externally to your company.

Cybercriminals often leverage previously breached credentials to attempt to gain access to corporate networks, in an attack known as “credential stuffing.” The DGC Roadmap Assessment includes compromised credential monitoring, where ID theft websites, hacker forums, and other Dark Web websites are scoured to identify information which may present a risk to your organization, prior to it being used against you.

DGC is an accounting and business advisory firm with a dedicated IT Risk Assurance & Advisory practice. We offer a range of IT Audit, compliance, and cyber & information security services that can help identify, evaluate, measure and manage compliance and cybersecurity risks. For more information, contact Nick DeLena, CISSP, CISA, CRISC, CDPSE at 781-937-5191 / ndelena@dgccpa.com or Scott Goodwin, OSCP, OSWP at 781-937-5722 / sgoodwin@dgccpa.com.