WHITE PAPER | JUNE 2019

TECHGUARD SERVICES

IT Security Controls Audit

TECHGUARD SECURITY®

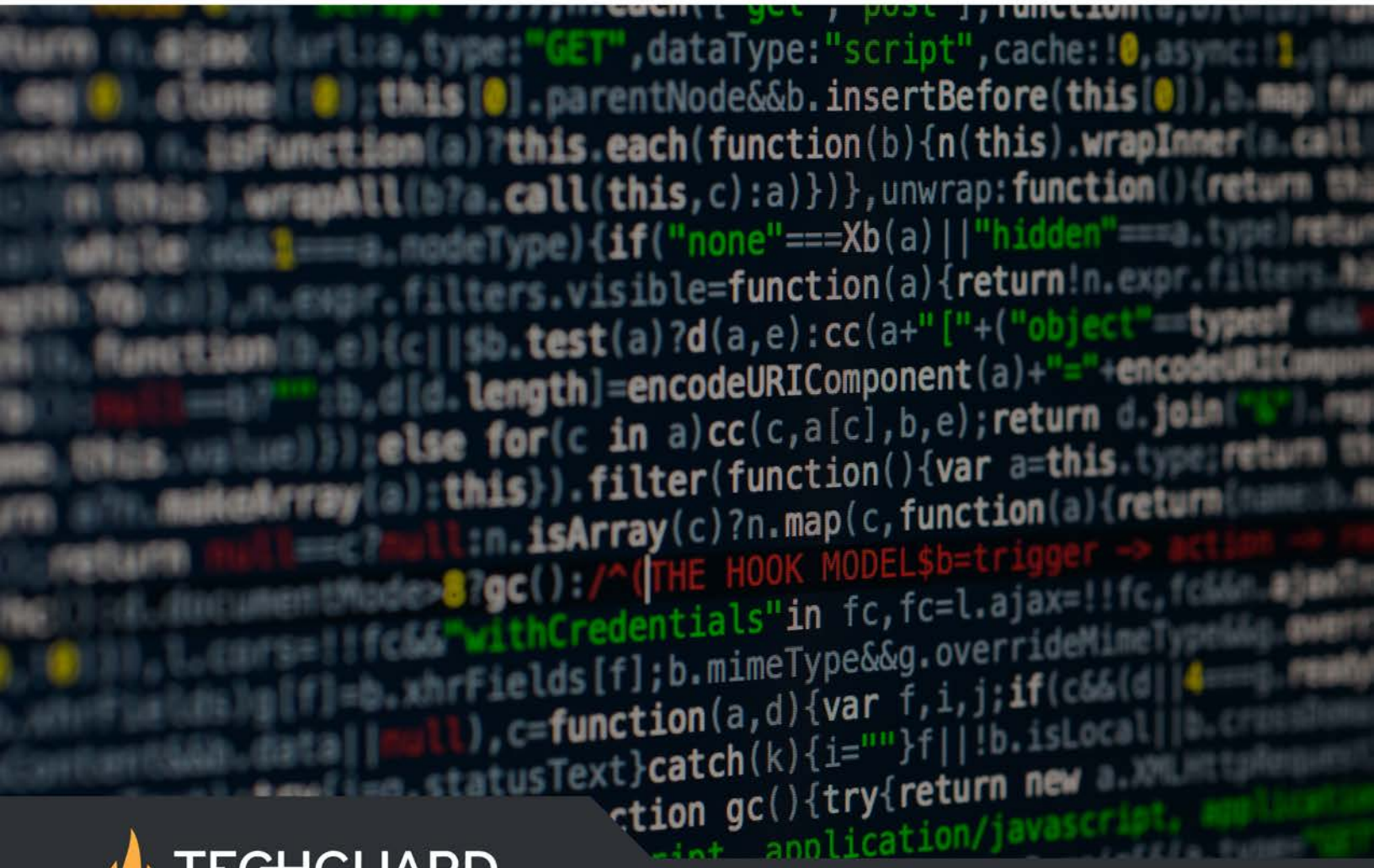
TechGuard Services
IT Security Controls Audit

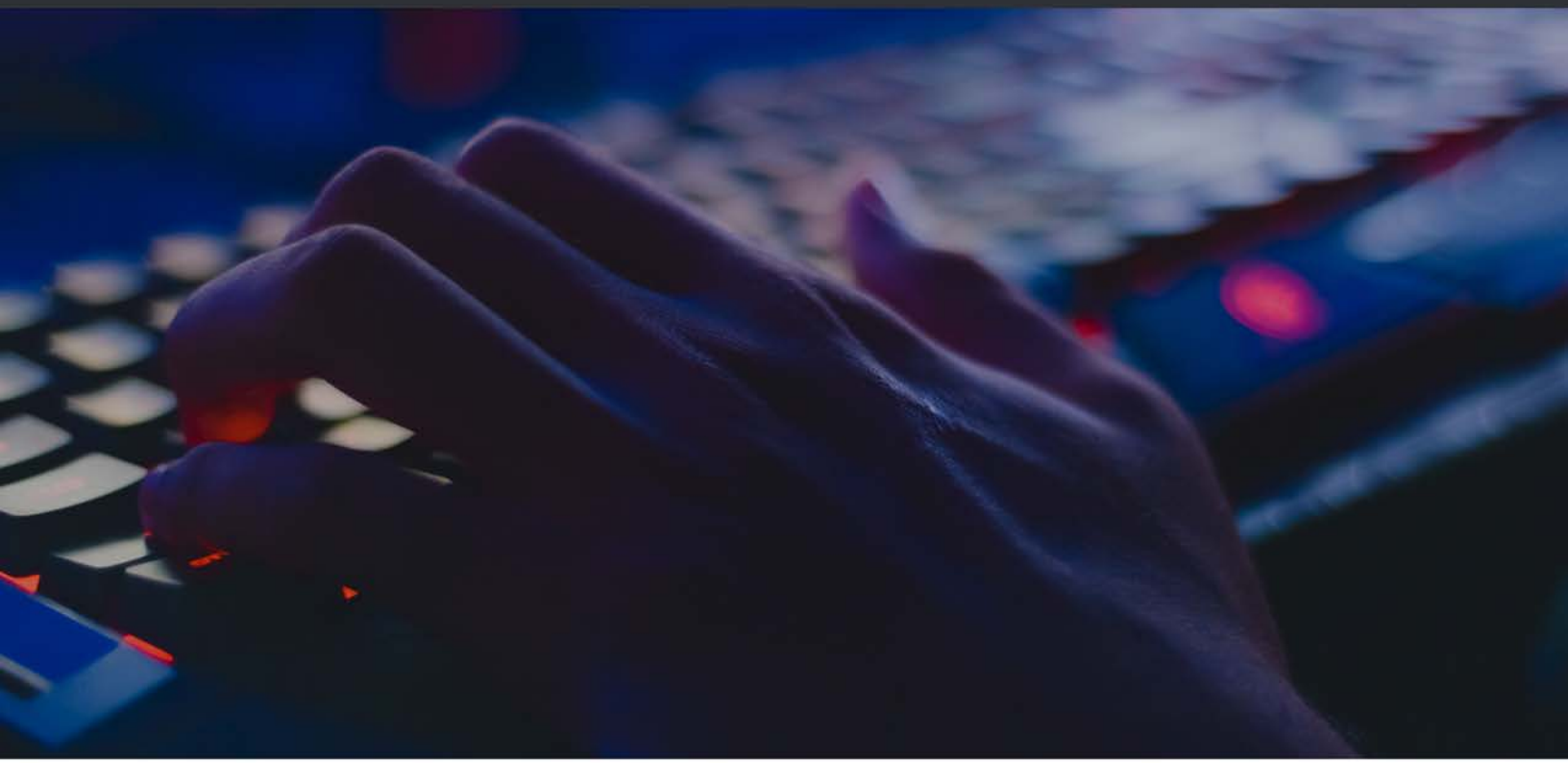
CONTENTS

WHAT IS AN IT SECURITY CONTROLS AUDIT?

An Information Technology (IT) Security Controls Audit consists of a comprehensive review of your technical and non-technical controls. IT Security Control Audits assess an organizations compliance with controls that cover technical, administrative and physical security.

An audit validates the effectiveness and implementation of established IT security controls and identifies security controls which have not been addressed.





WHY SHOULD AN IT SECURITY CONTROLS AUDIT BE PERFORMED?

In today's connected world, malicious actors are both motivated and creative in devising ways to exploit weaknesses in our people, processes and/or technology. In addition, regulatory bodies are mandating tighter controls on organizations who process or store sensitive data with stiff penalties for non-compliance.

Organizations should routinely evaluate their security controls to determine whether remediation or mitigation efforts are operating as intended.

An IT Security Controls Audit performed by a third party can provide you with an unbiased evaluation and identify gaps or ineffective controls you may not be aware of.

HOW DOES TECHGUARD APPROACH IT SECURITY CONTROLS AUDITS?

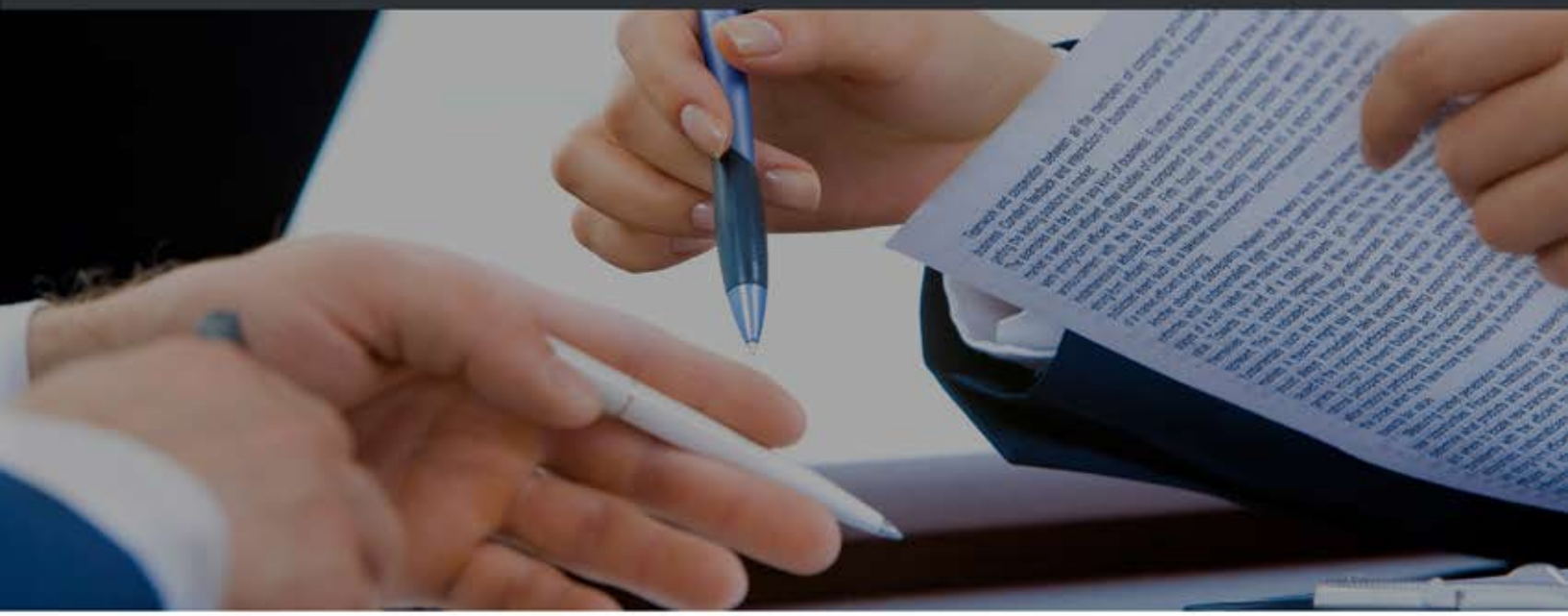
At TechGuard Security, we have adopted the Center for Internet Security (CIS) Top 20 Critical Security Controls (CSC) as our baseline for IT Security Controls Audits and use this as our standard when an organization does not have a regulatory requirement to adhere to a specified framework.

CIS controls are a prioritized set of security best practices created by cybersecurity experts around the world and are continuously evaluated and refined. Many common frameworks can be cross-mapped to the CIS Top 20 CSC.

Other security control frameworks TechGuard can assess against include:

- National Institute of Standards and Technology (NIST)
- Internal Organization for Standardization (ISO)
- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Federal Financial Institutions Examinations Council (FFIEC)

Ultimately, our goal is to assess the effectiveness of the controls in place and provide reasonable and achievable recommendations to improve the current control set, which provides the client with a lower risk profile and a roadmap to mature your cybersecurity program.



WHAT IS THE TECHGUARD DIFFERENCE?

We pride ourselves in building and maintaining long-term relationships with our clients. This ensures each client receives a tailored, customized service based on their unique organizational needs. From the initial kickoff meeting to delivery of the finalized IT Security Controls Audit Report, client satisfaction is our number one concern.

At TechGuard, we place the utmost value on the delivery of quality services. Every client is assigned a Project Lead who will serve as their single point of contact throughout the engagement.

In addition to the detailed written report provided at the end of the assessment, clients engage in a presentation with their Project Lead. Our report delivery presentation provides the opportunity to discuss details of important action items, next steps, and answer any questions related to remediation recommendations.

TechGuard has been dedicated to delivering high-end, professional cybersecurity solutions since 2000 - making us a trusted partner in both the government and private sectors.

TechGuard Security is an ISO 9001:2015-registered, certified SDB, DBE and Woman-Owned Business Enterprise. TechGuard Security was founded to address national cyber defense initiatives and US critical infrastructure security. We provide a comprehensive suite of cybersecurity solutions to help reduce your risk of cybersecurity-related incidents.