

DIR Managed IT Security Services

A. External controlled penetration testing

i. Scanning

What do outsiders see? The scanning offering provides an understanding of the vulnerabilities (weak security controls) that can be seen by unauthorized persons external to your network. Hackers typically perform scans to identify vulnerabilities that can later be exploited. This engagement identifies vulnerabilities and provides prioritized, actionable recommendations for improvement. Work to be performed by credentialed CISSPs.

Activities include:

- Identify requirements, address assumptions, and plan engagement
- Conduct interviews with technical and management staff
- Use commercial and open source scanning tools
- Manually validate high vulnerability findings
- Analyze data and make prioritized tactical & strategic recommendations
- Identify root causes for lasting remediation
- Prepare and deliver engagement status reports
- Prepare and deliver draft and final reports with technical supplements
- Prepare and deliver an executive briefing
- Provide knowledge transfer

ii. Penetration testing

Can someone break in? The penetration test identifies and exploits vulnerabilities to gain access to data without the authorization to do so, to assume and escalate system/user privileges that were not granted, and to control data without authorization. CIBER professionals will take the most direct route to circumvent security controls to meet the objectives of the test. Work to be performed by credentialed CISSPs.

Activities include:

- Identify requirements, address assumptions, and plan engagement
- Conduct interviews with technical and management staff
- Use commercial, open source scanning tools, and manual techniques
- Observe accesses gained, data controlled, controls breached, etc.
- Analyze data and make prioritized tactical & strategic recommendations
- Identify root causes for lasting remediation
- Prepare and deliver engagement status reports
- Prepare and deliver draft and final reports with technical supplements
- Prepare and deliver an executive briefing
- Provide knowledge transfer

iii. WAR Dialing

Do I have unauthorized modems? Unauthorized modems, typically installed for user convenience, circumvent security controls by creating a stealth and unmonitored backdoor into your internal network. CIBER professionals employ tools designed to identify and probe modems within your block of telephone numbers. Work to be performed by credentialed CISSPs.

Activities include:

- Identify requirements, address assumptions, and plan engagement
- Conduct interviews with technical and management staff
- Use commercial and open source war dialing tools
- Analyze data and make prioritized tactical & strategic recommendations
- Identify root causes for lasting remediation
- Prepare and deliver engagement status reports
- Prepare and deliver draft and final reports with technical supplements
- Prepare and deliver an executive briefing
- Provide knowledge transfer

iv. WAR Driving

Do I have unauthorized wireless access points (WAPs)? Unauthorized WAPs, typically installed for user convenience, circumvent security controls by creating a stealth and unmonitored backdoor into your internal network. CIBER professionals employ tools designed to identify and probe WAPs that may be operating within your facilities. Work to be performed by credentialed CISSPs.

Activities include:

- Identify requirements, address assumptions, and plan engagement
- Conduct interviews with technical and management staff
- Use commercial and open source wireless scanning tools
- Profile or perform forensics (signal cracking - locating) as required
- Analyze data and make prioritized tactical & strategic recommendations
- Identify root causes for lasting remediation
- Prepare and deliver engagement status reports
- Prepare and deliver draft and final reports with technical supplements
- Prepare and deliver an executive briefing
- Provide knowledge transfer

v. Social Engineering

Are users really implementing the security training they receive? This unique offering assesses whether or not user training is effective outside the training environment. CIBER professionals introduce your employees to a social engineering attack and assess the findings. Work to be performed by credentialed CISSPs.

Activities include:

- Identify requirements, address assumptions, and plan engagement
- Conduct interviews with technical and management staff

- Construct and deploy a social engineering attack
- Analyze data and make prioritized tactical & strategic recommendations
- Identify root causes for lasting remediation
- Prepare and deliver engagement status reports
- Prepare and deliver draft and final reports with technical supplements
- Prepare and deliver an executive briefing
- Provide knowledge transfer

vi. Applications Assessment

How secure are the applications themselves? The last line of defense is the application, are the security controls present and effective; is the application constructed using secure programming techniques? These questions are answered by the Application Assessment. Work to be performed by credentialed CISSPs.

Activities include:

- Identify requirements, address assumptions, and plan engagement
- Conduct interviews with technical and management staff
- Use commercial and open source tools to assess security controls
- Manually validate high vulnerability findings
- Analyze data and make prioritized tactical & strategic recommendations
- Identify root causes for lasting remediation
- Prepare and deliver engagement status reports
- Prepare and deliver draft and final reports with technical supplements
- Prepare and deliver an executive briefing
- Provide knowledge transfer

IT Security Services

A. Security Governance and Advisory Services

2. Texas Administrative Code, Chapter 202

Compliance difficulties with meeting the Information Security Standards of Texas Administrative Code, Chapter 202 can require additional staff and specialized expertise not needed for daily operations. This offering provides the right skill sets for assessments or remediations. Work to be performed by credentialed CISSPs.

Activities include:

- Identify compliance requirements, address assumptions, and plan
- Conduct interviews to gain "current state" understanding
- Identify compliance requirement sources
- Perform gap analysis between "current" and "required" state
- Analyze data and make prioritized tactical & strategic recommendations
- Identify root causes for lasting remediation
- Prepare and deliver engagement status reports
- Prepare and deliver draft and final reports

- Prepare and deliver an executive briefing
- Perform the recommended remediation activities as requested
- Provide knowledge transfer

3. Texas Government Code, Chapter 2059

CIBER professionals provide the security consulting support required for Chapter 2059 compliance. Work to be performed by credentialed CISSPs.

Activities include:

- Identify Chapter 2059 support needs and plan engagement
- Consult, assess, remediate, or maintain controls as requested
- Perform assessments as requested
- Prepare and deliver engagement status reports
- Prepare and deliver draft and final reports as required
- Prepare and deliver an executive briefing as required
- Provide knowledge transfer

C. Infrastructure Services

i. Firewall and VPN policy and architecture review

The firewall and VPN policy and architecture review examines the presence and effectiveness of technical and non-technical security controls on your perimeter. This is especially useful to identify what is being allowed in (and out) and the level of security being afforded the encrypted link into the organization. Work to be performed by credentialed CISSPs.

Activities include:

- Identify requirements, address assumptions, and plan engagement
- Conduct interviews with technical and management staff
- Review documents and diagrams
- Perform manual configuration and ruleset reviews
- Analyze data and make prioritized tactical & strategic recommendations
- Identify root causes for lasting remediation
- Prepare and deliver engagement status reports
- Prepare and deliver draft and final reports with technical supplements
- Prepare and deliver an executive briefing as required
- Perform the recommended remediation (optional)
- Provide knowledge transfer

ii. IDS/IPS policy and architecture review

The IDS/IPS review examines the presence and effectiveness of your Intrusion Detection System or Intrusion Prevention System controls. It provides decision-makers with answers to questions like, will we

know if we're being hacked or is there an active preventive control that will stop a hack before it happens? Work to be performed by credentialed CISSPs.

Activities include:

- Identify requirements, address assumptions, and plan engagement
- Conduct interviews with technical and management staff
- Review documents and diagrams
- Review device configuration and management
- Analyze data and make prioritized tactical & strategic recommendations
- Identify root causes for lasting remediation
- Prepare and deliver engagement status reports
- Prepare and deliver draft and final reports with technical supplements
- Prepare and deliver an executive briefing as required
- Perform the recommended remediation (optional)
- Provide knowledge transfer

iii. Access control/identity management review/integration services

Access Control and Identity Management is paramount to your security organization. Are personnel getting the access they need and no more, do we manage access, why do we have 5000 accounts when we only have 250 employees? These are the questions addressed. CIBER professionals tailor the services to your specific needs. Work to be performed by credentialed CISSPs.

Activities include:

- Identify requirements, address assumptions, and plan engagement
- Conduct interviews with technical and management staff
- Review documents and access and identity management controls
- Use manual and/or automated tools to perform the review
- Analyze data and make prioritized tactical & strategic recommendations
- Identify root causes for lasting remediation
- Prepare and deliver engagement status reports
- Prepare and deliver draft and final reports with technical supplements
- Prepare and deliver an executive briefing as required
- Perform the recommended/requested integration services
- Provide knowledge transfer

iv. Network architecture review

Is our current network architecture helping or hindering our efforts to secure our data? Is there a better way to assemble the components so we keep the same level of operational capabilities and pick up some security benefits? The Network Architecture Review provides the high level review from a security perspective. The results are actionable and prioritized recommendations for improvement. Work to be performed by credentialed CISSPs.

Activities include:

- Identify requirements, address assumptions, and plan engagement
- Conduct interviews with technical and management staff

- Review documents and diagrams
- Analyze data and make prioritized tactical & strategic recommendations
- Prepare and deliver engagement status reports
- Prepare and deliver draft and final reports with technical supplements
- Prepare and deliver an executive briefing as required
- Perform the recommended remediation (optional)
- Provide knowledge transfer

v. Host hardening and secure build development

Running systems that have not been patched, contain unnecessary services known to be hacker exploits, and not being sure if the configuration fielded still remains an invitation to compromise. This offering performs the analysis necessary to identify the applications and services needed to support the organization and a hardening scheme to create and field a more secure system. Work to be performed by credentialed CISSPs.

Activities include:

- Identify requirements, address assumptions, and plan engagement
- Conduct interviews with technical and management staff
- Prepare and deliver engagement status reports
- Prepare and deliver hardening procedures and checklists
- Perform the recommended hardening/secure build activities
- Provide knowledge transfer

D. Risk and Vulnerability Assessment Services

i. Perimeter vulnerability scans

How secure are the perimeters to my organization and what are the current risks to the organization for a breach to the confidentiality, integrity, and/or availability of the information entrusted to us? This assessment service specifically targets the presence and effectiveness of perimeter security controls. Work to be performed by credentialed CISSPs.

Activities include:

- Identify requirements, address assumptions, and plan engagement
- Conduct interviews with technical and management staff
- Review documents and diagrams
- Use commercial and open source scanning tools on the entity perimeter
- Manually validate high vulnerability findings
- Analyze data and make prioritized tactical & strategic recommendations
- Identify root causes for remediation
- Prepare and deliver engagement status reports
- Prepare and deliver draft and final reports with technical supplements
- Prepare and deliver an executive briefing
- Provide knowledge transfer

ii. Perimeter penetration scans

Can someone break in to our network? What could they see or do if they could? These are the questions answered by a Perimeter Penetration Scan. The scan identifies and exploits vulnerabilities to gain access to data without the authorization to do so, to assume and escalate system/user privileges that were not granted, and to control data without authorization. CIBER professionals will take the most direct route to circumvent security controls to meet the objectives of the test. Work to be performed by credentialed CISSPs.

Activities include:

- Identify requirements, address assumptions, and plan engagement
- Conduct interviews with technical and management staff
- Review documents and diagrams
- Use commercial and open source tools to penetrate the entity perimeter
- Use manual techniques to penetrate the perimeter
- Identify access gained and data controlled to validate penetration
- Analyze data and make prioritized tactical & strategic recommendations
- Identify root causes for remediation and risk reduction
- Prepare and deliver engagement status reports
- Prepare and deliver draft and final reports with technical supplements
- Prepare and deliver an executive briefing
- Provide knowledge transfer

iii. Internal network vulnerability assessments

How robust are the security controls in our internal network? The Internal network vulnerability assessment identifies and examines the presence and effectiveness of the technical and non-technical internal network controls. Work to be performed by credentialed CISSPs.

Activities include:

- Identify requirements, address assumptions, and plan engagement
- Conduct interviews with technical and management staff
- Review documents and diagrams
- Use commercial and open source scanning tools on the internal network
- Manually validate high vulnerability findings
- Analyze data and make prioritized tactical & strategic recommendations
- Identify root causes for remediation
- Prepare and deliver engagement status reports
- Prepare and deliver draft and final reports with technical supplements
- Prepare and deliver an executive briefing
- Provide knowledge transfer

iv. Network risk assessments

What risks to the confidentiality, integrity, and availability of data are we as an organization taking with the current security controls we have on our network? This assessment identifies the vulnerabilities on

the network and assesses their ability to acceptably defend against human unintentional, human intentional, natural, and structural threats. Work to be performed by credentialed CISSPs.

Activities include:

- Identify requirements, address assumptions, and plan engagement
- Conduct interviews with technical and management staff
- Review documents and diagrams
- Use commercial and open source scanning tools on the network
- Manually validate high vulnerability findings
- Analyze data and make prioritized tactical & strategic recommendations
- Identify root causes for remediation and risk reduction
- Prepare and deliver engagement status reports
- Prepare and deliver draft and final reports with technical supplements
- Prepare and deliver an executive briefing
- Provide knowledge transfer

v. Host vulnerability assessments

How robust are the security controls in our hosts? The host vulnerability assessment identifies and examines the presence and effectiveness of the technical and non-technical controls on organizational host systems. Work to be performed by credentialed CISSPs.

Activities include:

- Identify requirements, address assumptions, and plan engagement
- Identify systems to be reviewed
- Conduct interviews with technical and management staff
- Review documents and diagrams
- Use manual techniques and/or tools to evaluate system configuration
- Analyze data and make prioritized tactical & strategic recommendations
- Identify root causes for remediation
- Prepare and deliver engagement status reports\
- Prepare and deliver draft and final reports with technical supplements
- Prepare and deliver an executive briefing
- Provide knowledge transfer

vi. Host risk assessments

What risks to the confidentiality, integrity, and availability of data are we as an organization taking with the current security controls we have on our hosts? This assessment identifies the vulnerabilities on host systems and assesses their ability to acceptably defend against human unintentional, human intentional, natural, and structural threats. Work to be performed by credentialed CISSPs.

Activities include:

- Identify requirements, address assumptions, and plan engagement
- Identify systems to be reviewed
- Conduct interviews with technical and management staff
- Review documents and diagrams
- Use manual techniques and/or tools to evaluate system configuration
- Analyze data and make prioritized tactical & strategic recommendations
- Identify root causes for remediation and risk reduction
- Prepare and deliver engagement status reports
- Prepare and deliver draft and final reports with technical supplements
- Prepare and deliver an executive briefing
- Provide knowledge transfer

vii. Applications architecture assessment

How effective are the security controls in our applications architecture? The Applications Architecture assessment identifies and examines the presence and effectiveness of the technical and non-technical controls in our applications and their operational environment. Work to be performed by credentialed CISSPs.

Activities include:

- Identify requirements, address assumptions, and plan engagement
- Conduct interviews with technical and management staff
- Review documents and architectural diagrams
- Review technical and environmental (e.g., policy/program) architectures
- Analyze data and make prioritized tactical & strategic recommendations
- Identify root causes for remediation and risk reduction
- Prepare and deliver engagement status reports
- Prepare and deliver draft and final reports with technical supplements
- Prepare and deliver an executive briefing
- Provide knowledge transfer

viii. Applications penetration testing

Can someone break in to and take control of our business applications and databases? What could they see or do if they could? These are the questions answered by an Applications Penetration Test. The test identifies and exploits vulnerabilities in the application or its environment to gain access to data without the authorization to do so, to assume and escalate system/user privileges that were not granted, and to control data without authorization. CIBER professionals will take the most direct route to circumvent security controls to meet the objectives of the test. Work to be performed by credentialed CISSPs.

Activities include:

- Identify requirements, address assumptions, and plan engagement
- Conduct interviews with technical and management staff
- Review documents and application diagrams
- Use commercial and open source tools to circumvent security controls
- Identify access gained and level of control over protected data

- Analyze data and make prioritized tactical & strategic recommendations
- Identify root causes for remediation
- Prepare and deliver engagement status reports
- Prepare and deliver draft and final reports with technical supplements
- Prepare and deliver an executive briefing
- Provide knowledge transfer

ix. Secure code reviews

How secure is the application code we produce? Are we building strong or weak code in terms of its ability to ward off attacks from unauthorized users? CIBER security professionals use a regimen of automated and manual tools to identify the strength of code and the vulnerabilities that may exist. Work to be performed by credentialed CISSPs.

Activities include:

- Identify requirements, address assumptions, and plan engagement
- Conduct interviews with technical and management staff
- Review application SDLC documentation
- Use commercial and open source tools to review code for errors
- Manually validate coding error findings
- Manually review code (as requested)
- Analyze data and make prioritized tactical & strategic recommendations
- Identify root causes for remediation and risk reduction
- Prepare and deliver engagement status reports
- Prepare and deliver draft and final reports with technical supplements
- Prepare and deliver an executive briefing
- Provide knowledge transfer

xi. Commercial product assessment

How do I get past the commercial hype so that I can acquire products that do what I want them to do? As security professionals, CIBER can see past commercialism and reduce competing products to their common denominators. As security professionals, we are also skilled at requirements definition and best practices to aid you in your acquisition decision and product selection. Work to be performed by credentialed CISSPs.

Activities include:

- Identify requirements, address assumptions, and plan engagement
- Conduct interviews with technical and management staff
- Create evaluation matrix and metrics
- Assemble commercial product candidates
- Assess candidates against functional security and business requirements
- Analyze data and make product selection recommendations
- Prepare and deliver engagement status reports
- Prepare and deliver draft and final reports with technical supplements
- Prepare and deliver an executive briefing
- Provide knowledge transfer

xii. Data security assessment

How secure is the data that I am responsible for? CIBER provides this assessment option in a very tailorable format to meet all client needs. Work to be performed by credentialed CISSPs.

Activities can include:

- Identify requirements, address assumptions, and plan engagement
- Conduct interviews with technical and management staff
- Review documents and diagrams
- Use commercial and open source tools as appropriate
- Use manual tools and techniques as appropriate
- Manually validate high vulnerability findings by automated tools
- Analyze data and make prioritized tactical & strategic recommendations
- Identify root causes for remediation and risk reduction
- Prepare and deliver engagement status reports
- Prepare and deliver draft and final reports with technical supplements
- Prepare and deliver an executive briefing
- Provide knowledge transfer

xi. Security Policy and Guideline Development

“Our organization is taking write-ups from auditors for having undocumented policies, standards, or guidelines”.

“We have invested significant funds in security technology but now feel we need the structure that only policies and a best practice framework can provide”.

If either of these statements seem familiar, the CIBER Global Security Practice can provide the needed assistance. Our professionals work with your personnel to develop policies, standards, or procedures that are tailored to your organization. If required, we can recommend and populate a policy framework based on international standards or best practices and add traceability back to legislated or contractual requirements. Work to be performed by credentialed CISSPs.

Activities include:

- Identify requirements, address assumptions, and plan engagement
- Conduct interviews with technical and management staff
- Review current policies and guidelines
- Identify legislated and contractual requirements
- Perform traceability to requirements and/or framework
- Use understandings to craft or enhance policies, guidelines, etc.
- Present documents for review and moderate discussion
- Incorporate guidance
- Prepare and deliver engagement status reports
- Prepare and deliver draft and final policy or guideline documents
- Prepare and deliver an executive briefing as required
- Provide knowledge transfer