SECURANCE
CONSULTING

Advantage of Insight AI

ABOUT SECURANCE

Since 2002, Securance has empowered enterprises with the insight and strategies they need to defend critical assets against cyber threats. Through independent assessments of our clients' technologies, and the controls and processes that safeguard and support them, we identify risks and vulnerabilities that could expose data, networks, and systems, hinder digital transformation, and threaten a business's position in the market. Our recommendations are customized to each organization's IT and operating environments, yielding cost-effective solutions and lasting value.

THE SECURANCE DIFFERENCE

- As a firm of IT executives, we staff each project with experts in cybersecurity, IT management, and compliance. All of our senior IT consultants have at least 15 years of experience leading and executing assessments of enterprise technology.
- We identify technical risks before they turn into business risks, such as information security incidents, outages, or loss of reputation.
- Securance is the only IT consulting firm that uses generative artificial intelligence (genAI) and large language models (LLMs) to focus its approach to assessing technology. We use a proprietary genAI tool to identify and predict compliance, security, and IT process weaknesses based on our clients' industries, organizations, and technology profiles, then adjust our methodologies to prioritize these risks.

> "Working closely with Paul Ashe, we were able to put together a plan of action that was both timely and caused minimal interruptions for staff. Communication throughout the project was very good. The final report was delivered on time and provided us with very useful information to close the gaps within our IT security and risk management programs.
>
> I highly recommend Securance and would look to them again for guidance."
>
> — Rick L. Gant, United Bankshares, Inc.

OUR SERVICES

Securance's industry-leading services help businesses in all industries improve their cybersecurity postures, improve compliance and risk management processes, and thwart cyber-attacks. We apply proven methodologies to each project, adjusting our approach to fit each customer's objectives and requirements.

Artificial Intelligence (AI) Security

AI security assessments help organizations ensure that they and their AI technologies are protected against common threats, such as data set poisoning, algorithm tampering, input attacks, spoofing, and sophisticated malware. In addition to vulnerability and penetration testing, Securance reviews AI-specific policies and procedures, access controls, patch management, encryption, data storage practices, and security awareness training.

Cybersecurity as a Service (CSaaS)

Five critical cybersecurity assessments in an affordable annual package. Perfect for SMBs and budget-conscious organizations that want to understand their threat profiles and be proactive about cyber defense.

Cybersecurity Assessments

Our consultants have experience configuring and securing every layer of the enterprise IT environment. Our technical assessment services include:

- Active Directory and InTune reviews
- Application and database security assessments
- Cloud security assessments
- Endpoint security assessments
- Firewall configuration reviews
- Internet of Things security assessments
- Mobile security assessments
- Network architecture reviews
- Operating system security assessments
- Router and switch configuration reviews
- Zero trust architecture consulting

Advanced Penetration Testing

Combines leading-edge commercial tools with in-depth manual testing to identify vulnerabilities in networks and systems. During the penetration testing phase, our experts will attempt to exploit vulnerabilities, escalate privileges, and move laterally through your infrastructure.

Businesses with advanced cybersecurity programs may also be interested in our **advanced persistent threat (APT) testing**. These long-term projects simulate true cyber-attacks, in which bad actors deploy APT tactics over a four- to six-month period. We will attempt to exploit select vulnerabilities using various tools, system utilities, and custom scripts.

> I can't say enough about how valuable a process this was for us, and the level of confidence it's given us in moving forward to improve our IT infrastructure. Thanks again for your excellent work. I know we'll be in touch with future needs or as additional recommendations are required.
>
> — Ryan Gruber, WCCDA

IT Process Review

A review of the design and operating effectiveness of IT processes and controls intended to protect the confidentiality, integrity, and availability of your data and systems. We can compare controls to any best-practice framework, such as the NIST Cybersecurity Framework, NIST Special Publication 800-53, 27001 and ISO 27002, the CIS Controls, or COBIT.

These types of assessments lend insight into the efficiency and strength of a company's information security program and typically cover:

- Access management and user provisioning
- Backup and recovery
- Change management
- Configuration management
- End user computing
- Enterprise IT security
- Incident management
- Information security governance
- Mobility management
- Monitoring and logging
- Patch management
- Physical security
- Remote access management
- Risk assessment and response
- Segregation of duties
- Software license compliance
- System development
- Technology asset management
- Vendor management

Incident Response

End-to-end breach and incident response services, from incident response planning and tabletop exercises to real-time response and remediation. Our emergency incident response packages guarantee "boots on the ground" within 8 hours.

Ransomware Readiness Assessment

A true test of your organization's ability to prevent, detect, and respond to ransomware attacks. Securance will review processes and controls supporting backup, disaster recovery, endpoint security, incident response, and security awareness training; simulate an attack on the network; and lead the security team through a scenario-based tabletop exercise.

To maximize the value of the services we provide to our clients, we staff all projects with senior IT security professionals who have at least 15 years of experience and up-to-date knowledge of the cyber landscape. Our staff members maintain professional certifications, such as:

- Certified Information Systems Auditor (CISA)
- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Certified Internal Auditor (CIA)
- Certified Public Accountant (CPA)
- Certified Ethical Hacker (CEH)
- Certified Business Continuity Professional (CBCP)
- Certified HIPAA Professional (CHP)
- Cybersecurity Maturity Model Certification Accreditation Body Registered Practitioner (CMMC-AB RP)
- Certified Data Privacy Solutions Engineer (CDPSE)
- Healthcare Certified Information Security and Privacy Practitioner (HCISPP)
- Cisco Certified Internetwork Expert (CCIE)
- Certified Network Defender (CND)
- Certified Vulnerability Assessor (CVA)
- Certified Scrum Master (CSM)
- Project Management Professional (PMP)
- ISO 27001 Lead Auditor

Compliance Services

Gap analyses against federal, state, and industry regulations and frameworks reveal weaknesses in security controls that create the potential for fines or penalties:

- CIS Controls
- CJIS
- COBIT
- CMMC
- FISMA
- FTC Red Flags Rule
- GLBA
- HIPAA
- ISO
- NIST
- PCI DSS
- State privacy and security statutes
- GDPR

IT Strategic Planning

IT strategic plans position organizations to maximize their IT capabilities, make smart investments in new technology, and improve their bottom lines. We help companies align their IT strategies with business drivers, industry benchmarks, and internal metrics, providing frameworks for continuous improvement in IT services, customer experience, and user satisfaction.

Virtual CISO

A chief information security Officer (CISO) for a fraction of the cost of hiring a full-time CISO. Securance's virtual CISOs (vCISOs) apply their expertise to design, implement, and oversee mature cybersecurity programs, including governance, compliance, risk assessments, incident and vulnerability management, security awareness training, and technical testing.

> "Whenever challenges presented themselves, Securance overcame them with the determination and perseverance necessary to meet all critical deadlines."
>
> — County of Riverside, California

OUR METHODOLOGY

Your organization is unique; so is our approach to your needs. While businesses in the same vertical may share common security concerns and technologies, no two IT environments are the same. We account for this when developing our project approach and adjust our methodologies to accurately capture risks, meet or exceed your objectives, and deliver customized reports and recommendations that speak directly to your team.

> The folks at Securance first learned our needs, then our environment— not just a high-level view, but their people dug into our culture and interviewed our employees at every level of the organization. As a result, we don't have a boilerplate program. We have a customized, workable, real-life solution.
>
> — Altra Federal Credit Union

REPORTING

We deliver reports that are actionable and easy for technical and non-technical stakeholders to understand. With input from your management staff, we develop recommendations that fit your environment and will help you improve security, mitigate risks, and streamline compliance efforts. Our reports include:

Executive Summary

Summarizes the assessment scope, approach, findings, and recommendations in plain English. Intended for senior management, the executive summary includes a matrix of prioritized findings and a heat map.

Management Report

Detailed explanation of the project scope, approach and methodology, findings, and co-developed, actionable recommendations.

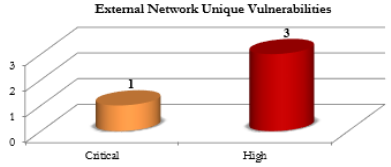
Roadmap

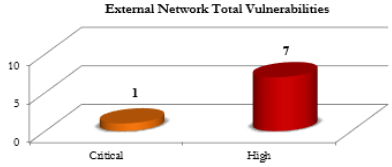
If applicable, prioritizes remediation activities and provides estimated costs, human resource requirements, and timeframes.

Finding Legend:

Urgent-Risk (Level 5) Immediate remediation required.	*Note: If finding is a technical vulnerability, it provides remote intruders with remote root or remote administrator capabilities.*
Critical-Risk (Level 4) Immediate action recommended with remediation ASAP.	Note: If finding is a technical vulnerability, it provides intruders with remote user, but not remote administrator or root user, capabilities.
High-Risk (Level 3) Immediate action recommended with remediation in 90 days.	*Note: If finding is a technical vulnerability, it provides hackers with access to specific information, including security settings, stored on the host. This level of vulnerability could result in potential misuse of the host by intruders.*
Medium-Risk (Level 2) Action recommended with remediation in 180 days.	*Note: If finding is a technical vulnerability, it may expose some sensitive information, such as precise versions of services, from the host. With this information, hackers could research potential attacks to try against a host.*
Low-Risk | Informational (Level 1) Effective control.	No immediate changes recommended. Opportunity for slight improvement.
Advisory Comment	Action suggested at the discretion of management.

Threat Level	Server	Vulnerability Description	Fix | Recommendation
Critical	• 2xx.xxx.xxx.x	**Microsoft IIS Repost.asp File Upload** - The script '/scripts/repost.asp' is installed on the remote IIS web server and allows an attacker to upload arbitrary files to the '/Users' directory if it has not been configured properly. *REF: CVE-1999-0360;* *http://www.securityfocus.com/bid/1811/discuss;* *http://www.osvdb.org/285*	Create the '/Users' directory if necessary and ensure that the Anonymous Internet Account ('IUSER_MACHINE') only has read access to it.
High	• 2xx.xxx.xxx.xx • 2xx.xxx.xxx.xx	**DNS Server Cache Snooping Information Disclosure** - The remote DNS server responds to queries for third-party domains which do not have the recursion bit set. This may allow a remote attacker to determine which domains have recently been resolved via this name server, and therefore which hosts have been recently visited. For instance, if an attacker was interested in whether your company utilizes the online services of a particular financial institution, they would be able to use this attack to build a statistical model regarding company usage of that financial institution. Of course, the attack can also be used to find B2B partners, web-surfing patterns, external mail servers, and more. *REF: http://www.rootsecure.net/content/downloads/pdf/dns_cache_snooping.pdf*	Use another DNS software.





SECURANCE CONSULTING

13916 Monroes Business Park • Tampa, FL 33635 • 877.578.0215
www.securanceconsulting.com