SECURANCE
CONSULTING

Advantage of Insight AI

ABOUT SECURANCE

Since 2002, Securance has empowered enterprises with the insight and strategies they need to stay ahead of evolving IT risks. Through independent audits 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 compliance efforts, 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 audit executives, we staff each project with experts in technology risk management, security, and compliance. All of our senior IT consultants have at least 15 years of experience leading and executing various IT and compliance audits.
- We identify technology risks before they turn into business risks, such as information security incidents, outages, or loss of reputation.
- Securance is the only IT audit firm that uses generative artificial intelligence (genAI) and large language models (LLMs) to focus its approach to assessing technology risks. We use a proprietary genAI tool to identify and predict compliance, security, and internal control 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 IT risk profiles, streamline internal controls and compliance efforts, and prevent cyber attacks. We apply proven methodologies to each project, adjusting our approach to fit each customer's objectives and requirements.

IT Risk Assessment and Audit Plan

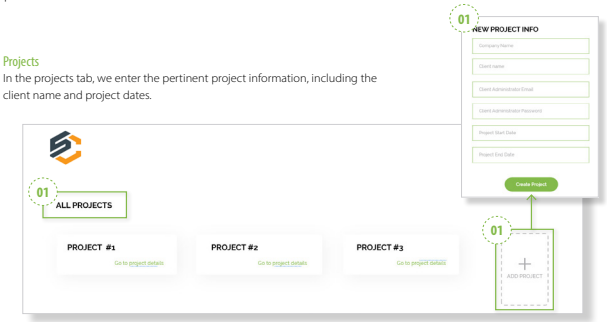
A review of the risks: affecting auditable IT processes and technologies, including applications, databases, operating systems, infrastructure components, and security tools. We use our proprietary risk assessment tool, SCGRC, to translate our findings into an IT risk matrix and three-year audit plan.

- SCGRC is a web-based application that identifies risks affecting auditable technologies, such as enterprise applications, databases, operating systems, cloud services, and network devices, and IT processes. After conducting an interview-based IT risk assessment, our consultants use SCGRC to analyze the data and generate a plan that focuses audit efforts on significant risks and helps internal audit teams to prioritize their budgets.

Securance utilizes a proprietary technology to support the risk assessment process and produce a multi-year IT audit plan. The portal organizes the project information, risk categories selected, auditable technologies and processes, and interview participants.

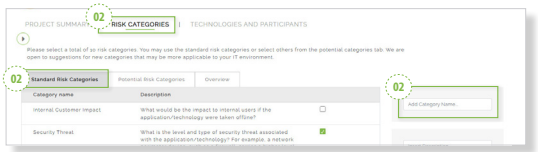
01 Projects

In the projects tab, we enter the pertinent project information, including the client name and project dates.



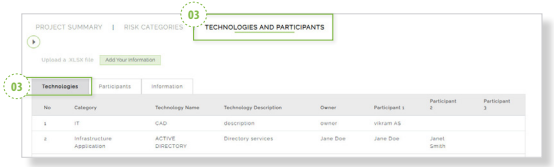
02 Categories

We work with our client to select the appropriate risk categories from our catalog of pre-defined categories. Our solution is customizable and allows us to create custom risk categories, if necessary.



03 Technologies and Participants

In the Technologies and Participants tab, we first import or input all auditable technologies and processes to be evaluated.



IT General Controls 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, ISO 27001 and 27002, or COBIT.

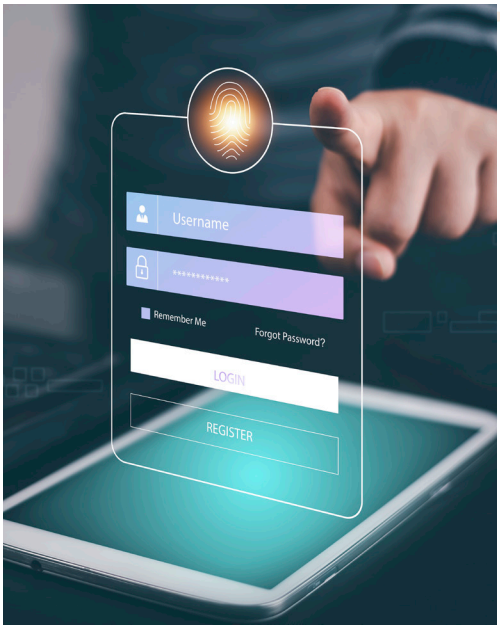
These types of assessments lend insight into the efficiency and strength of a company's information security program and typically cover:

- 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

Cybersecurity Reviews

Technical assessments that reveal security vulnerabilities and exposures within the IT environment. These services include:

- Application and database security assessments
- Artificial intelligence (AI) security assessments
- Cloud security assessments
- Firewall configuration reviews
- Internet of Things security assessments
- Operating system security assessments
- Ransomware readiness assessments
- Router and switch configuration reviews
- Vulnerability assessments and penetration tests
- Zero trust architecture consulting



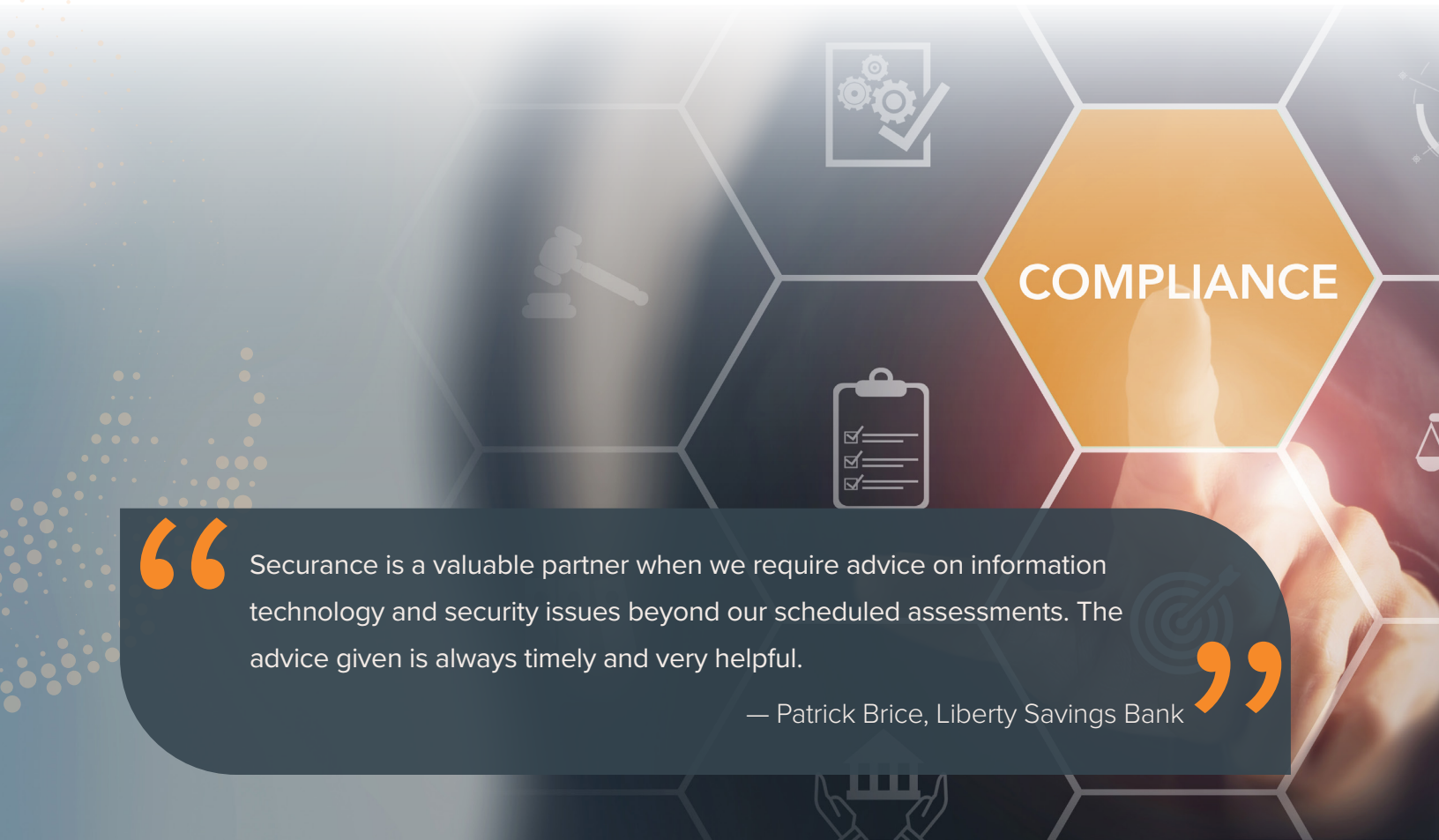
To maximize the value of the services we provide to our clients, we staff all projects with senior IT audit professionals who have at least 15 years of experience and up-to-date knowledge of enterprise technology, compliance requirements, and cyber risks. Our staff members maintain professional certifications, 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 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)
- 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:

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



> Securance is a valuable partner when we require advice on information technology and security issues beyond our scheduled assessments. The advice given is always timely and very helpful.
>
> — Patrick Brice, Liberty Savings Bank

> In working with Paul and his team, my staff and I found them intelligent, collaborative and instructive. The audit took place with very little impact on our production environment.
>
> — Nancy Byrnes, Fairfield Public Schools

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.

> We have always been very pleased with the work product and the cost value that Securance offers. Our Technology Services department is very complimentary of Securance's staff and always impressed with their knowledge and understanding of IT security and IT management.
>
> — Ingram Quick, *Louisville* | *Jefferson County Metro Government*

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 audit 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, and management's responses to the audit. Each finding describes the condition, effect, cause, and criteria against which the technology or process was reviewed.

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.

FUNCTION	CATEGORY	SUBCATEGORY	TIER	COMMENT
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried.	2 – Risk Informed	See Finding 10.
		ID.AM-2: Software platforms and applications within the organization are inventoried.	2 – Risk Informed	See Findings 10 and 20.
		ID.AM-3: Organizational communication and data flows are mapped.	1 - Partial	See Findings 1, 2, and 5.
		ID.AM-4: External information systems are catalogued.	2 – Risk Informed	See Finding 10.
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.	1 - Partial	See Finding 11.
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.	2 – Risk Informed	See Finding 1.

SECURANCE CONSULTING

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