Information Security at Accenture

Today's sophisticated and evolving threat landscape, exacerbated by the COVID-19 pandemic and the necessity to have large employee populations work remotely, reinforces that protecting the data of Accenture, our clients, and our employees is a 24/7 job that requires agile, dedicated people, strategies, processes and technologies.

Accenture's global Information Security organization of over 800 security professionals does this and more with a highly specialized team whose expertise spans technical architecture and security operations, governance and risk management, threat intelligence, compliance, behavior change and incident management.

True to Accenture's purpose of "delivering on the promise of technology and human ingenuity," the team provides strong leadership in support of Accenture's security technology investments and business processes. Additionally, through proactive and innovative communications and behavioral change programs aimed at incident prevention, the Information Security team fosters an overall culture that works as One Accenture to protect client and Accenture information.

In addition to its vast and cross-functional skillset, this team maintains a formal governance relationship with Accenture's Legal, Global IT, Geographic Services, Data Privacy and Business Continuity groups; while also keeping open lines of communication with law enforcement agencies, third-party security advisors, and the information security organizations of Accenture clients and suppliers.

> "To protect Accenture, our clients and our employees, the Information Security organization continues to adapt and optimize its risk resilience, addressing current cyber threats while preparing for new issues tomorrow might bring.

Kris Burkhardt
Accenture Chief Information Security Officer

An agile team

Comprised of distinct security-focused areas and an extensive governance network led by the Chief Information Security Officer, the teams work to stay ahead of threats through a strategic and coordinated approach.

Client data protection

Protecting client data is a top business priority and everyday discipline employed through our global Client Data Protection (CDP) program. Backed by strong security processes, policies and governance across Accenture and client engagements, this ISO 27001/27701 certified program ensures client teams understand and comply with data privacy and security obligations relevant to each client engagement.

A CDP plan is developed for each client project and provides end-to-end security risk management covering physical, application, infrastructure and data security. The program also arms the project teams with tools and controls that enable them to identify and mitigate security risks over the lifecycle of a client project. Accenture leadership reviews and monitors CDP monthly metrics, providing oversight and accountability to ensure the security controls provide an effective framework for protecting client and company information against vulnerabilities.

Accenture rates at the top of global rankings in maintaining a strong defense against threats, as rated by the leading cyber security rating vendors in each risk category.

Employee learning and communications

Our people are our greatest asset when it comes to building cyber resilience, with everyone playing a critical role to keep our clients, our employees and our enterprise information safe. Through comprehensive, interactive employee learning programs, Accenture's behavior change team continually strengthens this cyber security mindset using relatable, immersive learning and testing scenarios along with gamification methods that bring risks and consequences to life, ultimately driving positive security behaviors.

One of these learning programs is the award-winning Information Security (IS) Advocate program which consists of several voluntary learning 'tiers' that reward employee adoption of information security best practices.

Each year an average of 75 percent of Accenture employees voluntarily complete this program, receiving Information Security Advocate status 'badges' and embracing stronger security behaviors. The team has found that employees who complete the IS Advocate program are much less likely to contribute to a security incident.

These interactive employee learning programs, designed to educate every part of our organization from day one, have garnered industry recognition for their innovative approach and impressive results. Accenture consistently outperforms peers in third-party rankings.

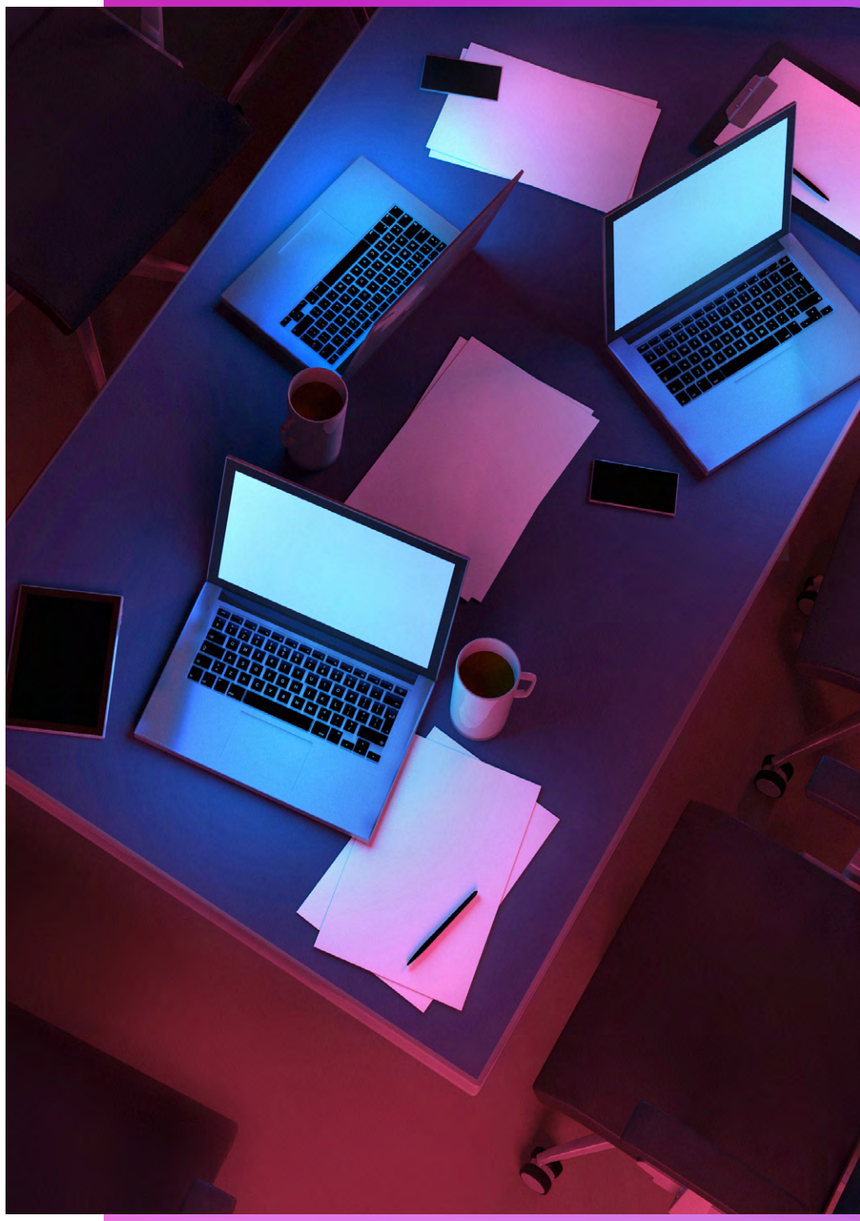
Governance, risk & compliance

Accenture's cyber governance, risk and compliance team maintains a broad yet highly focused framework of risk management controls, policies, processes, and metrics that are implemented across the enterprise in order to set expectations, measure outcomes and drive change to fortify Accenture's security posture.

The team adapts this approach as necessary, maintaining a flexible yet targeted strategy that reduces cyber risk through defined policies and enterprise-wide accountability. A governance framework helps drive this strategy, ensuring security procedures are integrated into everyday business. Facing such unique circumstances as the COVID-19 pandemic and targeted global cyber attacks, the teams' current strategy is built to drive adaptive cyber resilience across the organization.

Using threat intelligence, Accenture continually measures its security posture and resilience, validating this stance through risk assessments. Simultaneously, the team works to strengthen security controls and technologies, while enhancing information security and data protection training. Improving our acquisition security and how we identify risks within our infrastructure outsourcing also works to drive continuity in our overall efforts to build a strong cyber defense.

Further, the work of our cyber governance, risk and compliance team measures and improves Accenture's Information Security organization effectiveness through an ongoing focus on regulatory and business risk, as well as threat intelligence—ensuring an agile, cyber-resilient enterprise in the face of ever-changing and unpredictable threats and challenges.



Technology monitoring & compliance

Accenture generates billions of data interactions daily, transmitting information through various networks, platforms, and systems. Keeping technical infrastructure and data secure while allowing employees the appropriate flexibility to be successful is a continual challenge, especially among Accenture's globally dispersed and largely remote workforce.

Expanded, advanced security operations

Accenture has over 50,000 physical and virtual servers, operating 95 percent of its business applications in the cloud. Accenture's Security Operations Center (SOC) uses some of the most advanced security technologies to monitor and hunt threats across the enterprise, that in turn help implement solutions at speed and scale. Such an approach includes:

- Real-time threat detection and compliance reporting conducted through Security Information and Event Management (SIEM).
- Vulnerability management to remove malware and effectively patch vulnerabilities, closing the attack surface proactively and preventing penetration of the network.
- Agent-based distributed hunting to search for malware and indicators of compromise, allowing us to secure rapid results and if needed, remediate the issue within minutes versus hours.
- A centralized patch management system to track compliance and identify/distribute required patches quickly.

Incident response

Accenture's Cyber Incident Response Team (CIRT) monitors and manages a broad security landscape. Highly trained professionals provide 24/7 coverage and can deploy on site anywhere in the world, in most cases within a matter of hours. Incident response plans are rehearsed monthly, and two of these drills are managed by security specialist third parties. Simulations may cover both internal and external scenarios.

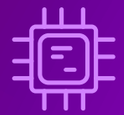
A specialized group within this team (known as the Red Team) continually threat hunts and tests Accenture defenses by simulating attacks against the company's digital infrastructure. Red Team members possess the skills and knowledge of potential attackers, along with the resources needed to mitigate the vulnerabilities they exploit.

Working in conjunction with the Red Team, the Threat Hunting Team operates under an "assumed breach" model, proactively searching for signs of latent threats in and outside the environment. Threat hunters look for suspicious behaviors and other evidence that suggest threat actors may have breached the environment. Working alongside incident responders, hunters investigate and resolve complex security incidents such as hacking attempts, active intrusions, and malware infections.

Accenture maintains certification to ISO 27001:2013 standard and meets/exceeds benchmarks against leading industry controls and frameworks.

CIS Critical Security Controls Version 7.1
Maintains at or above its peers and industry verticals in all 20 categories, validated by third-party assessment and benchmarking.

ISO 27701
Maintains certification for data-privacy standards.



NIST Cyber Security Framework (CSF)
Assessed as "at" or "exceeding" in all categories against its peer and industry verticals by BSI.

CSA Security, Trust & Assurance Registry (STAR)
Awarded, and maintains, the highest Gold-level certification for Accenture-managed cloud infrastructure.

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services—all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 537,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at **www.accenture.com.**