Information Security at Accenture

Resilient through change

Today's sophisticated and evolving threat landscape, diversifying business areas, and evolving hybrid workplace reinforce the need for highly modern cyber capabilities to ensure resilience in the face of change.

800+ security professionals
in Accenture's global Information Security organization

We adapt at speed to this changing environment to protect the data of Accenture, our clients and employees—a 24/7 job that requires agility, strategies, processes and technologies.

True to Accenture's purpose of "delivering on the promise of technology and human ingenuity," our 800-person team provides strong leadership, supporting Accenture's security technology investments and business processes with expertise in technical architecture, security operations, risk management, threat intelligence, compliance and incident management. Through proactive and innovative communications and behavioral change programs aimed at incident prevention, the Information Security team fosters a culture that works as One Accenture to protect client and Accenture information.

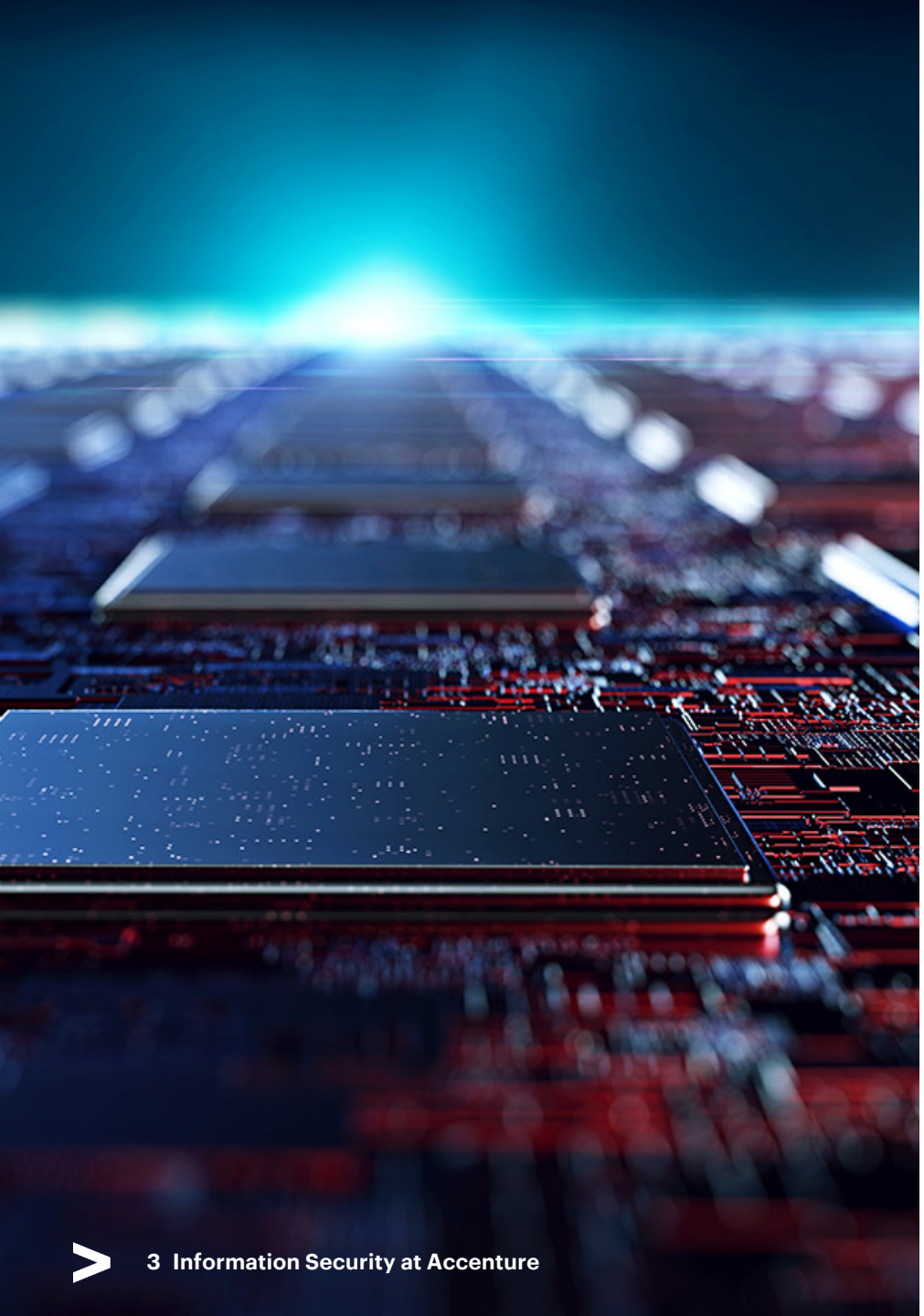
The team maintains an extensive governance network, including formal relationships with these groups in Accenture:

- Legal
- Global IT
- Corporate Services & Sustainability
- Data Privacy
- Business Resilience Services

Information Security also collaborates 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



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.

Using structured risk analysis tools, a set of CDP controls are defined, incorporating Accenture Information Security and Data Privacy policies and standards, client contractual requirements, and regional privacy controls and frameworks.

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 CDP 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 and adaptable framework for protecting client and company information against vulnerabilities.

Governance, risk and compliance

Accenture's cyber governance, risk and compliance (GRC) team maintains a broad, highly focused framework of risk management controls, policies, processes, and metrics that are implemented across the enterprise.

The team establishes strategy and expectations, measures outcomes, and drives change to fortify Accenture's security posture. Our security framework is underpinned by a hybrid set of internationally recognized standards including but not limited to ISO 27001/27701, NIST CSF, CSA STAR, and CIS Critical Security Controls. Accenture continually measures its security posture and resilience, validating this stance through risk assessments and external audits.

Threat intelligence sources are also incorporated into the governance framework, helping to drive our security strategy, understand the threat landscape, and ensure security risk and procedures are integrated into the business. Facing such unique circumstances as geopolitical issues, advanced, targeted cyber-attacks, and hybrid working environments, the current strategy is built to drive adaptive cyber resilience across the organization while preparing for the future.

Key strategic security programs under the GRC function include:

- Secure integration of acquisitions.
- Supplier cyber risk management.
- Insider risk management.

The GRC team measures and improves Accenture's Information Security organization effectiveness through an ongoing focus on regulatory and business risk—ensuring an agile, adaptive cyber-resilient enterprise.

Maintaining a strong defense against threats

Accenture ranks at the top of global rankings as rated by the leading cyber security rating vendors in each risk category.

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

CIS Critical Security Controls Version 8 maintains at or above industry peers across all control areas, validated by third-party assessment and benchmarking

NIST Cyber Security Framework (CSF) assessed as operating industry-leading cybersecurity systems at the Highest NIST Implementation Tier by BSI

ISO 27001/27701 maintains BSI's largest global certifications for Information Security and Data Privacy standards

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

Employee learning and communications

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.

Accenture's Information Security behavior change team continually strengthens this cyber security mindset through innovative learning and awareness initiatives. These metrics-based change programs use relatable, immersive learning and testing scenarios, including VR-based experiences, along with gamification methods that bring risks and consequences to life, ultimately driving positive security behaviors.

One of these creative initiatives is the award-winning Information Security (IS) Advocate program. Employees have their own personalized learning paths with custom courses that are designed based on their roles within the organization and their unique risk profiles. As they make their way through the IS Advocate learning journey, employees are rewarded for their adoption of information security best practices, receiving IS Advocate status "badges."

> "Our people are our greatest asset, but also our greatest vulnerability. Creating a culture of security among employees is critical."
>
> **Kris Burkhardt**
> Accenture Chief Information Security Officer

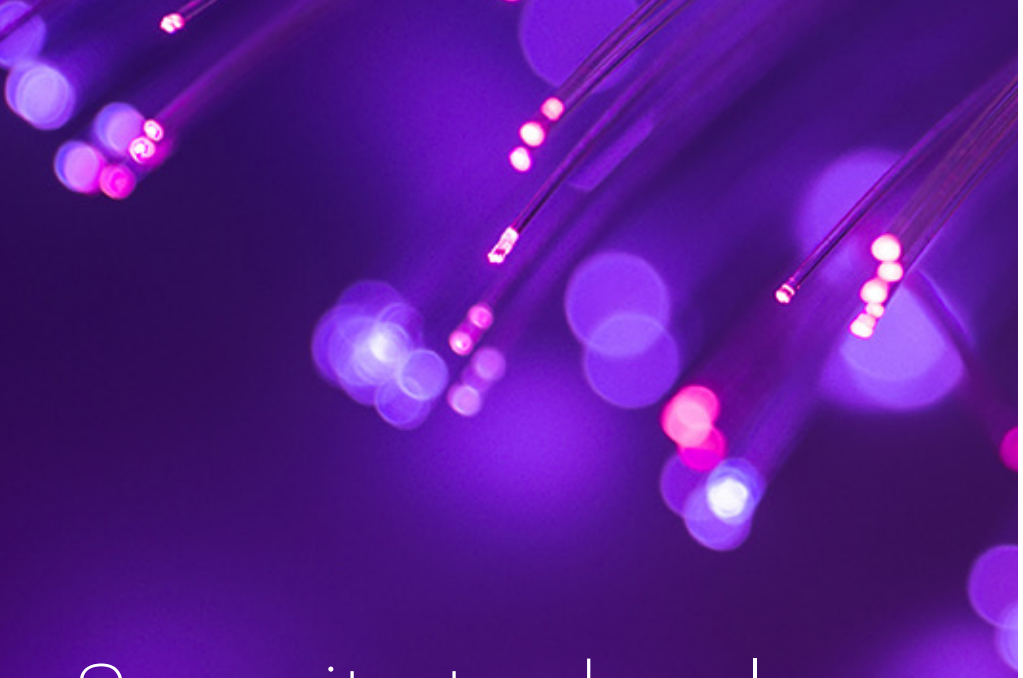
On average, 76 percent of employees voluntarily participate in advanced levels of our Advocate program—achieving status badges and embracing stronger security behaviors. The team has found that employees who complete the IS Advocate program are half as likely to contribute to a security incident.

These interactive learning programs, designed to educate employees in every part of our organization from day one are focused on strengthening foundational knowledge and response to emerging threats. Agile and flexible, with a mix of global and grass-roots initiatives, and leveraging local Information Security leaders and "champions," the behavior change program has garnered industry recognition for its innovative approach and impressive results.

76% of Accenture employees voluntarily participate in advanced levels of our Advocate program

Those who completed IS Advocate training were **half as likely** to be involved in a security incident.

28+ Awards
for our behavior change program



Security technology

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 enjoy omni-connected experiences and be successful is a continual challenge, especially with Accenture's globally dispersed workforce.

Infrastructure monitoring and compliance

Accenture manages a massive, complex set of infrastructure spanning hundreds of thousands of endpoints, from the laptops our employees use, and the servers or network devices in traditional data centers, to more modern architectures leveraging native cloud services.

Our cohesive security compliance program includes:

Real-time threat detection and monitoring of threats via our security information and event management (SIEM) and endpoint detection and response (EDR) tools.

Aggressive perimeter scanning, detection, and testing, along with a dedicated attack surface management team, supports our work to continually search, find or exploit gaps before hackers do.

A comprehensive vulnerability scanning and configuration compliance approach which ensures timely patching of security vulnerabilities, as well as monitoring for secure configuration of servers, network devices, containers, and native cloud services

A one of a kind, in-house built, security dashboard which allows our infrastructure admins to see all their security actions in one place.

Monitoring/ 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.

CIRT is composed of six specialized teams, which collectively detect and defend the Accenture network infrastructure against malicious cyber attacks.

Accenture Security Operations Center (ASOC)

Responds to employee-reported security incidents and questions 24 hours a day, 365 days per year.

Red and Threat Hunting Teams

Simulate attacks against infrastructure to ensure mitigation strategies and incident response processes are working appropriately and that the most vulnerable systems are protected.

Data Loss Prevention (DLP)

Safeguards proprietary data by alerting Accenture users or blocking data transactions with unapproved domains or URLs.

Monitoring Team (Security Operations Center)

Performs real-time, 24/7 monitoring of security events, identifies suspicious activities and unsafe practices and works to prevent future occurrences.

Infrastructure

Reverse-engineers malware, manages intrusion detection systems, performs network-level forensics, and investigates potentially compromised systems.

Response & Investigations

Collect, analyze, and preserve evidence for incident reporting.

CIRT at-a-glance

120+ team members
based around the world

Possessing **130+ security-related certifications** and Proficiency in **15+ languages** across the team

About Accenture

Accenture is a leading global professional services company that helps the world's leading businesses, governments and other organizations build their digital core, optimize their operations, accelerate revenue growth and enhance citizen services—creating tangible value at speed and scale. We are a talent and innovation led company with 738,000 people serving clients in more than 120 countries. Technology is at the core of change today, and we are one of the world's leaders in helping drive that change, with strong ecosystem relationships. We combine our strength in technology with unmatched industry experience, functional expertise and global delivery capability. We are uniquely able to deliver tangible outcomes because of our broad range of services, solutions and assets across Strategy & Consulting, Technology, Operations, Industry X and Accenture Song. These capabilities, together with our culture of shared success and commitment to creating 360° value, enable us to help our clients succeed and build trusted, lasting relationships. We measure our success by the 360° value we create for our clients, each other, our shareholders, partners and communities. Visit us at **www.accenture.com**