IDC MarketScape

IDC MarketScape: European Cybersecurity Governance, Risk, and Compliance Consulting and Professional Services 2026 Vendor Assessment

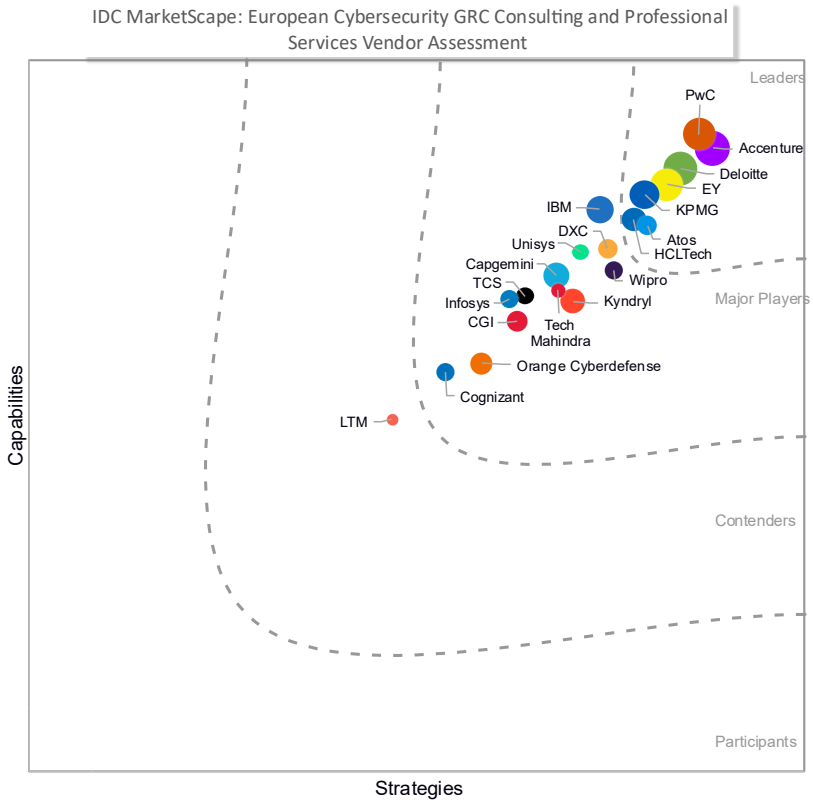
David Clemente

THIS EXCERPT FEATURES DXC AS A MAJOR PLAYER

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape: European Cybersecurity Governance, Risk, and Compliance Consulting and Professional Services Vendor Assessment



Source: IDC, 2026

July 2026, IDC #EUR154110926e

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

ABOUT THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: European Cybersecurity Governance, Risk, and Compliance Consulting and Professional Services 2026 Vendor Assessment (Doc # EUR154110926).

IDC OPINION

Europe's cybersecurity landscape is being shaped by rising threat activity, geopolitical uncertainty, and growing scrutiny from regulators and boards. Incidents targeting critical infrastructure, financial systems, and public services have intensified pressure on organizations to mature their security postures and invest in robust governance capabilities.

For security leaders operating in this environment, the question is no longer whether to build a GRC capability, but how quickly it can be done. Among the factors shaping the landscape, three stand out:

- **Regulatory convergence and complexity:** Overlapping EU frameworks such as the Network and Information Security Directive (NIS2), Digital Operational Resilience Act (DORA), EU AI Act, and the EU Cyber Resilience Act (CRA) are forcing organizations to manage intersecting compliance obligations, increasing demand for GRC consulting and professional services.
- **European digital sovereignty as a buying criterion:** Growing demand for EU-based security capability delivery, data residency compliance, and technology independence is reshaping how providers position and structure their GRC services for European buyers, particularly in regulated and government sectors.
- **AI disruption to GRC delivery models:** AI tooling is automating some tasks previously performed by consulting teams, compressing timelines, reducing costs, and intensifying buyer pressure on service providers to pass efficiency gains through to clients in pricing and engagement structures.

Regulators are also raising the bar for scrutiny and accountability. The formal designation of certain technology providers as critical ICT third parties under DORA is a signal of how deeply regulatory oversight now reaches into the technology supply chain. For senior executives and board members, the days when cyber risk was a technical exercise are long gone; cyber risk is now firmly a governance responsibility with financial and legal implications.

Global and European providers, spanning large professional services firms, major IT services companies, and specialist consultancies, are investing heavily in GRC capability,

proprietary tooling, and AI-enabled delivery to meet growing client demand. Vendors are competing on the depth of their regulatory coverage, the sophistication of their risk quantification capabilities, and increasingly, their ability to demonstrate sovereignty-aligned delivery (however defined) for clients with data residency and security independence requirements.

Cybersecurity GRC is often as much an art as a science, where people, conceptual clarity, and pragmatism matter as much as technology. That balance is becoming increasingly difficult to realize in a region where regulators are intensifying scrutiny of how organizations — particularly those in critical infrastructure — manage cyber risk to prevent material incidents or cascading failures. The stakes for organizations and their advisors are growing.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

Using the IDC MarketScape model, IDC studied vendors that provide cybersecurity GRC consulting and professional services in Europe. The vendors included in the study had to meet certain criteria to qualify for this vendor assessment, including:

- **Geographic presence.** Vendors must offer cybersecurity GRC services in 10 or more countries in Europe.
- **Workforce capability.** Vendors must have 100 or more full-time employees in Europe who can perform one or more cybersecurity GRC service activities.
- **Sales presence.** Vendors must have a sales presence in at least three countries in Europe, demonstrating their ability to reach and serve a diverse customer base.

ADVICE FOR TECHNOLOGY BUYERS

European buyers of cybersecurity GRC consulting and professional services should begin by answering several key operational questions, including:

- Does my organization want to build and run our GRC capability?
- Does my organization want a service provider to build our GRC capability and then we run it?
- Does my organization want a service provider to build and run our GRC capability?

After choosing their preferred operational approach, European GRC buyers should consider the following topics as part of their service provider selection process:

- **Delivery models.** Identify which delivery models the service provider offers (for example, managed services, project-based services, outcome-based services, retainer-based services, and staff augmentation). Larger providers usually offer a variety of delivery models to suit a wide client base.

- **Geographic coverage.** Determine if the service provider's reach enables it to consistently address your organization's needs on the desired scale (country, regional, or global). Can the provider meet your organization's security compliance or sovereignty requirements across the required jurisdictions?
- **Use cases and credentials.** Identify use cases the service provider has successfully addressed based on previous projects, and request client credentials from similar engagements.
- **Pricing models.** These could include fixed fees, outcome-based arrangements, retainers, time-and-materials (increasingly rare), hybrid options, and more. An increasingly relevant factor in this process is the extent to which the use of AI tools is reducing the cost base of service providers and, in turn, increasing buyer demand for these cost savings to be shared with them.

VENDOR SUMMARY PROFILE

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each criterion outlined in the Appendix, the description here provides a summary of each vendor's strengths and opportunities.

DXC

DXC Technology is positioned in the Major Players category in the 2026 IDC MarketScape for European cybersecurity GRC consulting and professional services vendors.

DXC is a publicly listed IT services and consulting company, traded on the New York Stock Exchange. It was formed in 2017 through the merger of Hewlett Packard Enterprise Services and Computer Sciences Corporation, and is headquartered in Ashburn, Virginia.

European GRC offering

DXC Technology delivers cybersecurity GRC consulting and advisory services across Europe through discrete service offerings organized along a progressive delivery model structured across seven phases: Assess, Govern, Assure, Educate, Prepare, Test, and Act.

The portfolio encompasses Cyber Maturity Review (CMR), risk compliance assurance, CISO-as-a-service, security awareness, incident response planning and governance, Tabletop Exercises (TTX), and remediation governance and oversight, each with defined services, methods, and deliverables.

The CMR service is grounded in a proprietary Cyber Reference Architecture spanning up to 12 domains and subdomains, calibrated against a six-level CMMI-based maturity scale. The methodology aligns to NIST CSF, ISO 27001, SANS Critical Controls, MITRE ATT&CK, and

DORA. Risk compliance assurance engagements use Archer and ServiceNow to manage risk workflows and compliance reporting.

DXC reports more than 1,500 security professionals and over 500 GRC engagements, supported by more than 3,600 security certifications. European delivery centers span the U.K., France, Italy, Germany, the Netherlands, Belgium, Bulgaria, Finland, and Iberia. Security operations centers (SOCs) are located in the U.K. (Erskine), Bulgaria (Sofia), and Italy (Bari), with a major center in Spain (Madrid).

Services are available as managed or on-demand engagements with onsite and remote staffing options. Engagements are documented across financial services, automotive, and IT service provider sectors.

DXC has structured an AI augmentation road map across its GRC service lines, with planned extensions including AI-accelerated maturity assessments, AI-generated incident scenarios, AI-assisted risk correlation, and continuous AI-driven control monitoring. Innovation is developed through LabX, DXC's internal AI incubation function, targeting production-ready solutions within 90 days and validated in DXC's own operations first.

A GRC transformation road map through FY28 includes predictive risk assessments, autonomous GRC workflows, and AI-based adversary testing. Client satisfaction is tracked via Net Promoter Score surveys, with a dedicated Client Success Manager maintained separately from operational delivery.

Strengths

- **Comprehensive, structured GRC delivery model:** DXC's seven-offering portfolio spans the full GRC life cycle, from assessment and governance through to remediation. DXC t supports continuous program management rather than point-in-time engagements.
- **Proprietary maturity methodology with defined outputs:** The CMR's Cyber Reference Architecture, CMMI-based maturity scale, and multi-framework alignment provide a structured, repeatable basis for client assessments and improved roadmaps.
- **Strong client retention and satisfaction metrics:** Independently reported retention rates and satisfaction scores, alongside a long average client relationship duration, reflect a stable European client base across regulated industries.

Challenges

- **AI-augmented GRC capabilities remain in development:** Several planned AI extensions across GRC service lines are in DXC's offering transformation road map, rather than currently deployed, with some workflows still reliant on manual tooling.
- **Competitive European market requires clear differentiation:** The European cybersecurity GRC market is served by a mix of global IT providers and specialist advisory firms, requiring DXC to differentiate its consulting depth across varied national regulatory contexts.
- **GRC visibility within a broad IT portfolio:** Operating as part of a large, diversified IT services business may limit the visibility of DXC's dedicated GRC consulting depth to buyers comparing specialist advisory providers.

Consider DXC when

- **Integrating GRC with broader managed IT services:** Organizations seeking to connect cybersecurity governance with wider IT operations, cloud, and security managed by a single provider benefit from DXC's integrated delivery model.
- **Developing or maturing incident response governance:** Organizations needing to build incident response plans, conduct tabletop exercises, or implement remediation oversight can draw on DXC's structured methodology and cross-sector delivery experience.
- **Running a scalable, multi-framework compliance program:** Enterprises needing ongoing compliance assurance across multiple frameworks, supported by technology partnerships and available as a managed service, align well with DXC's risk compliance assurance model.

APPENDIX

Reading an IDC MarketScape graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis or strategies axis indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category

focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represent the market share of each individual vendor within the specific market segment being assessed.

IDC MarketScape methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users.

Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information and end-user experiences to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market definition

According to the Open Compliance and Ethics Group (OCEG), "GRC is the integrated collection of capabilities that enable an organization to achieve Principled Performance — the ability to reliably achieve objectives, address uncertainty, and act with integrity."

IDC's view of the market expands on this definition. Applied to cybersecurity, the GRC market is a functional market within IDC's broader security services taxonomy and includes the following segments:

- **Governance.** Corporate governance management applications support corporate board members, C-suite executive teams, and second line-of-defense professionals in defining and implementing corporate policies. This segment includes applications for policy management and compliance management.
- **Risk management.** Risk management assists in identifying, analyzing, monitoring, and managing all types of risks threatening an organization, including IT risk, compliance risk, security risk, security maturity, and third-party risk.
- **Compliance.** Compliance management encompasses adherence to all necessary regulatory and legal requirements, as well as managing any changes to the regulatory environment and its impact on the enterprise. This segment includes regulatory compliance management and regulatory change management.
- **Audit and regulatory management**. Audit management solutions help organizations plan, manage, and analyze processes (both manual and automated). Numerous

types of audits must be managed within an organization, including compliance audits, IT audits, security audits, and third-party audits.

- **Business resilience/continuity/recovery.** Business resilience/continuity/recovery solutions to identify exposure to internal and external threats.
- **Third-party risk management.** TPRM services are designed to help organizations identify, assess, mitigate, and monitor risks associated with third-party supplier and vendor engagements and/or due diligence for target acquisitions.
- **GRC professional services.** This is the focus of this IDC MarketScape. GRC services include consulting, design, implementation, and engineering services to support the creation and implementation of GRC programs and software solutions. In addition, advisory services consist of executive guidance: strategy, road maps, board training, education, virtual executive services, and program management.

LEARN MORE

Related research

- *IDC ProductScape: Worldwide Governance, Risk, and Compliance Software Vendor Assessment, 2026* (IDC #US54465726, April 2026)
- *IDC's Worldwide Security Services Taxonomy, 2026* (IDC #US53982726, March 2026)
- *IDC MarketScape: Worldwide Cybersecurity Governance, Risk, and Compliance Consulting Services 2025–2026 Vendor Assessment* (IDC #US53936925, December 2025)
- *IDC MarketScape: Middle East Governance, Risk, and Compliance Services 2025 Vendor Assessment* (IDC #META53726425, August 2025)
- *Worldwide Security Governance, Risk, and Compliance Services and Software Forecast, 2025–2029* (IDC #US53611425, June 2025)
- *Worldwide Security Governance, Risk, and Compliance Services Forecast, 2025–2029* (IDC #US53611525, June 2025)

Synopsis

This IDC MarketScape examines the services required for a successful cybersecurity GRC program that can be managed either by customers or service providers. It raises questions that buyers and vendors in this space can use as a guide to make informed decisions and achieve desired outcomes.

The design of cybersecurity GRC services can be broad and defined by vendors according to their capabilities. At its core, GRC services should equip an organization to fulfill compliance requirements in a sustainable manner, while effectively managing cybersecurity

risks. These services must also account for engagement with, and input from, senior executives, board members, regulatory and supervisory authorities, and other key stakeholders.

"Security industry guru Dan Geer once defined security as 'the absence of unmitigable surprise,'" said David Clemente, research director of IDC's European Security Services program. "Investments in cybersecurity GRC must provide as much mitigation as possible, reducing the likelihood of unpleasant surprise while enabling the organization to fulfill its primary objective. These two goals often appear in tension; security applying the brakes versus employees speeding ahead.

Cybersecurity GRC thus becomes as much an art as a science, where people and process are as important as technology, and conceptual clarity and pragmatism are needed to navigate political, financial, and technology trade-offs across the organization. This is particularly true in Europe, where regulators are increasing their scrutiny of cybersecurity risks, with growing interest in how organizations are managing these risks to prevent material incidents or cascading failures."

ABOUT IDC

International Data Corporation (IDC) is the premier global market intelligence, data, and events provider for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight help IT professionals, business executives, and the investment community make fact-based technology decisions and achieve their key business objectives.

IDC Italy

Viale Monza, 14
20127 Milan, Italy
+39.02.28457.1
X: @IDCitaly
idc-insights-community.com
www.idcitalia.com