

Consultant talent standard

Global Risk Advisory Cyber Risk – Cyber Security

Building a *globally uniform level of quality and capability* in our core services so that our clients experience a *consistent, exceptional Deloitte* is critical to become the undisputed leader in professional services. The following standard defines the capabilities required at the Consultant level for our Cyber Security service.

Leadership capabilities

We expect practitioners at all levels to embrace and live our purpose by challenging themselves to identify issues that are most important for our clients, our people, and for society and *make an impact that matters*. There are five Leadership capabilities that we require from all Consultants across the organization, regardless of service. Behavioral anchors for each capability are described below.

Capability	Description	Behavioral anchors
Living Our Purpose	Builds own understanding of our purpose and values; explores opportunities for impact	<ul style="list-style-type: none"> Behaves in accordance with Deloitte values Consistently challenges self to deliver outstanding quality and value Recognizes and explores opportunities for personal impact on clients and for colleagues and communities
Talent Development	Demonstrates strong commitment to personal learning and development; acts as a brand ambassador to help attract top talent	<ul style="list-style-type: none"> Solicits feedback to build understanding of own strengths and areas for development Actively participates in key learning and development opportunities for his / her level Acts as a brand ambassador with peers and colleagues to support attraction of top talent
Performance Drive	Understands expectations and demonstrates personal accountability for keeping performance on track	<ul style="list-style-type: none"> Ensures he / she is clear on expectations and asks clarifying questions when needed Is aware of own strengths and uses them effectively to deliver high quality results Assumes personal responsibility for achieving results and supports the team by taking on additional responsibilities when needed
Influence	Actively focuses on developing effective communication and relationship-building skills	<ul style="list-style-type: none"> Engages with others to build relationships and develop a network Demonstrates ability to understand the underlying interests and expectations of others Respects and responds with sensitivity to the concerns and viewpoints of others
Strategic Direction	Understands how their daily work contributes to the priorities of the team and the business	<ul style="list-style-type: none"> Understands objectives and desired outcomes for assigned areas of responsibility and sets personal goals accordingly Seeks to understand how specific areas of responsibility contribute to broader business objectives and outcomes

Core Professional and Technical capabilities

Below are the Core Professional and Technical capabilities for Cyber Security Consultants:

Capability	Description	Behavioral anchors
Risk Assessment and Mitigation	Ability to effectively perform the technical components of risk assessments to provide an accurate view of the client's current risk state	<ul style="list-style-type: none"> Applies Deloitte's risk frameworks, tools, and processes (e.g., Risk Intelligence Program Methodology, Risk Intelligence Map, Risk Intelligence Diagnostic) to effectively map and organize client's data Leverages an understanding of Key Performance Indicators (KPIs), Key Risk Indicators (KRIs), and risk assessment techniques to analyze client's data and assess risks

Delivery Excellence	Ability to manage own work against the project plan, applying quality assurance, and risk procedures to ensure a superior client experience	<ul style="list-style-type: none"> • Demonstrates ownership of work and commitment towards project objectives and Deloitte quality standards • Understands how assigned areas of responsibility contribute to project objectives and desired outcomes • Teams with others to create recommendations and propose solutions • Understands the importance of effectively managing relationships with project team to deliver excellent results • Is able to complete assigned work with quality and timeliness • Asks clarifying questions to project management to reduce ambiguity • Anticipates potential risks related to managed work / processes and escalates them in a timely fashion to project leadership or relevant stakeholders
Reporting and Presentations	Ability to develop reports and presentations using appropriate tools	<ul style="list-style-type: none"> • Develops technical components of reports and presentations • Presents outcomes of data analysis in a clear, organized, and logical manner • Adopts the reader's perspective when developing report and presentation content
Knows the Business and the Industry	Ability to understand the client's business, interpret sector trends, and learn leading practices	<ul style="list-style-type: none"> • Stays current on business trends and industry practices • Conducts research on economic, sector, and market conditions to better understand the client's needs • Applies business and industry experience to assigned areas of responsibilities
Executive Presence	Ability to articulate thoughts and ideas in a clear and composed manner to instill confidence in team and clients	<ul style="list-style-type: none"> • Understands the linkage between personal and Deloitte brand and demonstrates the professionalism and interpersonal maturity to reinforce both reputations • Respects and responds with sensitivity to the concerns and viewpoints of others • Gains the confidence of the client by demonstrating an understanding of and active interest in their business

Specialized Technical capabilities

Below is the Specialized Technical capability for Cyber Security Consultants:

Capability	Description	Behavioral anchors
Supports Development and Implementation of Cyber Security Solutions	Ability to leverage industry-leading cyber security frameworks, methods, and tools to increase effectiveness of cyber security solutions	<ul style="list-style-type: none"> • Conducts accurate analyses of client's control environments to effectively evaluate risk exposure by applying relevant frameworks (e.g., NIST 800-61, ISO27001) • Leverages proven cyber security frameworks and methodologies to support the assessment and design of client's security architectures • Enables informed and prioritized decision making by accurately identifying and categorizing critical information asset • Identifies and leverages industry leading practices to support the development of cyber security policies and procedures • Supports the assessment of client's cyber security technologies to identify and articulate opportunities for improvement across the digital, physical, and social elements of the client • Researches metrics and KPIs to validate ROI of security investments • Becomes familiar with domain and industry-specific standards and regulations; keeps up-to-date with emerging trends • Develops a basic fluency of cyber security technology solutions within a specific domain