Cybersecurity governance, risk and compliance (GRC) consulting and managed services

Increase information security, regulatory compliance, data resilience and proactively manage risk within your environment

Public sector organizations face numerous threats to their information security, data privacy and data resilience including terrorism, malicious cyberspace activity, pandemics, accidents, transnational crime and natural disasters. Agencies must identify, address and mitigate these risks as a part of their mission. Along with these complex external threats, government agencies must also assess their internal mission risks while facing a dynamic, uncertain environment.

Within this increasingly intricate and interconnected public sector environment, simple devices have become smarter and more connected to the world around us via the Internet of Things (IoT). Building the capability and capacity to continually identify, understand and address these risks is essential. Assessing and responding to risks facing the public sector is a key driver in transforming government and promoting successful programs and missions.

Addressing the continually evolving threats and compliance issues within an RMF such as NIST 800-37 is critical. Agencies must understand their information security risks, develop mitigations in compliance with law and policy and communicate risk response strategies. Cyber risk management is not simply a compliance exercise—it goes to the core of agency mission delivery. Assessing the inherent cyber risks facing the public sector, and responding accordingly, can drive change in government and promote successful management of government programs and missions.

Our solution

Perspecta actively develops capabilities to enable agencies to address GRC both tactically and strategically. We have integrated Tenable.sc security technical integration guide (STIG) compliance data into the ServiceNow integrated risk management module. This compliance data is critical to tracking compliance against the RMF. We have further enabled risk management by using the unified compliance framework (UCF) data within ServiceNow which allows for a test once, comply many capability that minimizes work to show compliance against multiple cybersecurity RMFs.

Our cybersecurity GRC consulting and managed services provide:

- A variety of standard cybersecurity GRC consulting capabilities including assessments against the risk management, cybersecurity and other framework documents (NIST, ISO, CSF, HIPAA, etc.)
- Identity, credential and access management (ICAM) assessments to address NIST 800-63, OMB 19-17 and CDM requirements
- Zero trust architecture (ZTA) assessments for policy, identity, network and applications against the NIST 800-207 guidance and Perspecta zero trust maturity model including architecture and road map guidance
- Value-added solutions within ServiceNow integrated risk management (IRM) to accelerate the authority to operate (ATO) process

perspecta™

Benefits:

- GRC and information security operations platforms within ServiceNow; GRC and assessment platform within Trusted Agent
- RMF assessment
- Cyber engineering and architecture
- ICAM consulting and support
- ZTA assessments and architecture road map services
- Information security policy and standards consulting
- Information system security officer (ISSO)
- ATO services
- Data protection and privacy consulting
- Cybersecurity training
- FedRAMP / FISMA readiness assessment
- FedRAMP 3PAO assessment
- Integration of ServiceNow security operations and IRM with IT service and operations management
- FedRAMP / FISMA readiness and Third Party Assessment Organization (3PAO) assessments
- Skilled, cleared staff augmentation resources to fulfill the information system security officer role

Perspecta 3PAO has extensive experience in security control implementation and the evaluation of mission critical information systems for various government agencies. We provide clients with the technical, policy and operational insight required for a successful compliance assessment to achieve FedRAMP ATO certification, FISMA compliance to NIST 800-53, NIST 800-171 and the RMF NIST 800-37.

Our services and expertise help you shift your focus from a network-based perimeter approach to a risk-based ICAM approach to meet the requirements of cloud and mobile devices while monitoring for insider threat and other malicious activities. We focus on meeting the strategic, technical and operational ICAM challenges presented by the Cloud Smart strategy to maximize the security of your cloud investment.

Across our cybersecurity GRC capabilities, we provide workshops and transformation assessment and advisory services that can help clarify your specific needs and inform a strategy for utilizing governance and risk management to improve mission delivery and plan for a wide range of enterprise risks.

Why Perspecta

Perspecta has over 4,000 highly trained information technology and cybersecurity professionals actively supporting over $3 billion in U.S. public sector cybersecurity contracts operating worldwide. Perspecta provides a comprehensive portfolio of cybersecurity capabilities and deep public sector experience. We can bring cybersecurity GRC, service, operational and security management together to modernize, automate and transform your environment. Our Perspecta cybersecurity GRC solutions will provide valuable insights and capabilities to your organization to enhance innovation in your enterprise risk management.

Perspecta has designed and provisioned nearly 7 million active credentials for federal enterprise employees and contractors that comply with HSPD-12. We support more than 100 federal agencies in vetting, issuing personal identity verification (PIV) or common access cards (CAC) and integrating those credentials into local and physical access control systems—most notably, we have delivered more than 30,000 derived CAC credentials to mobile devices for a DOD customer on the Defense Information Systems Agency's (DISA) purebred architecture.

As a ServiceNow Premier partner, we can jump-start your GRC or IRM implementation while quickly and efficiently tailoring your environment to meet specific agency or department needs with minimal disruption. We have captured the implementation and onboarding requirements, including public sector best practices, to speed implementation and provide a complete set of in-instance technical documentation. Our workshops are specific to the RMF to ensure a smooth transition to a ServiceNow environment.

Our GRC expertise within ServiceNow has been further demonstrated on a large, DOD contract where we helped our customer re-engineer the ATO process to drive initial certification from more than three months to less than one week. Some of these continuous monitoring capabilities have also been implemented in the federal civilian sector, where our data integration expertise and understanding of the overall compliance requirements and process allowed us to integrate into a master GRC dashboard within rigorous contract deadlines.

Next steps

Participate in a Perspecta workshop or assessment to understand how to streamline and mature your GRC, identity or zero trust capabilities. You can also partner with us to turbocharge your ServiceNow IT service management (ITSM) and IT operations management (ITOM) environments with security operations and IRM / GRC to implement true enterprise risk management. Contact us for help in taming the ATO process.

Learn more at:
perspecta.com/offerings/cybersecurity

perspecta.com | contactus@perspecta.com
14295 Park Meadow Drive
Chantilly, Virginia 20151