KPMG

Evidence-Backed Cyber Governance Risk and Compliance (GRC) transformation enabled by ServiceNow and aligned to NCSC CAF

A KPMG Service for G-Cloud 15

KPMG
About us

Our UK Cyber team

We've worked with countless organisations across multiple sectors, including financial services, life sciences, healthcare, government, telecommunications, energy and natural resources, and legal services. Our clients range in sizes, span across geographies and industries and are subjects to various regulatory requirements and obligations.

330+ professionals

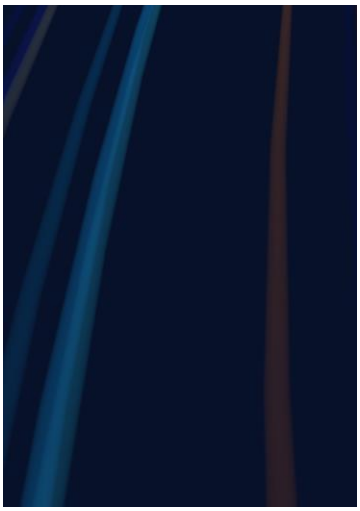
15+ office locations

Part of a global team of 6200+ individuals

Our services

UK Cyber operates across 8 different service lines, catering to a wide range of governance and technical needs.

Cyber strategy	Cyber risk
Cyber and enterprise resilience	Privacy compliance
Cyber tech transformation	Identity and access management
Cyber defence services	Cyber incident response



Our Cyber team is complemented by our Connected Technology team.

We have access to a 2000-strong team of client-facing technologists combined with alliance partners, with a diverse range of skills and experience.

This enables us to bring to our clients the most suitable resources, expertise and insights when needed.

We apply a data and technology driven approach to drive change through our digital transformation services.

Cyber Governance Risk and Compliance (GRC) transformation enabled by ServiceNow and aligned to NCSC CAF

Service Description:

This evidence-backed service builds in-house GRC / cyber risk capability, aligned to the Indicators of Good Practice from the CAF and Industry Frameworks such as NIST CSF and NIST 800-53. Our end-to-end service covers: discovery, design, automation via ServiceNow and transition to in-house teams. It's enabled by process, people and culture change.

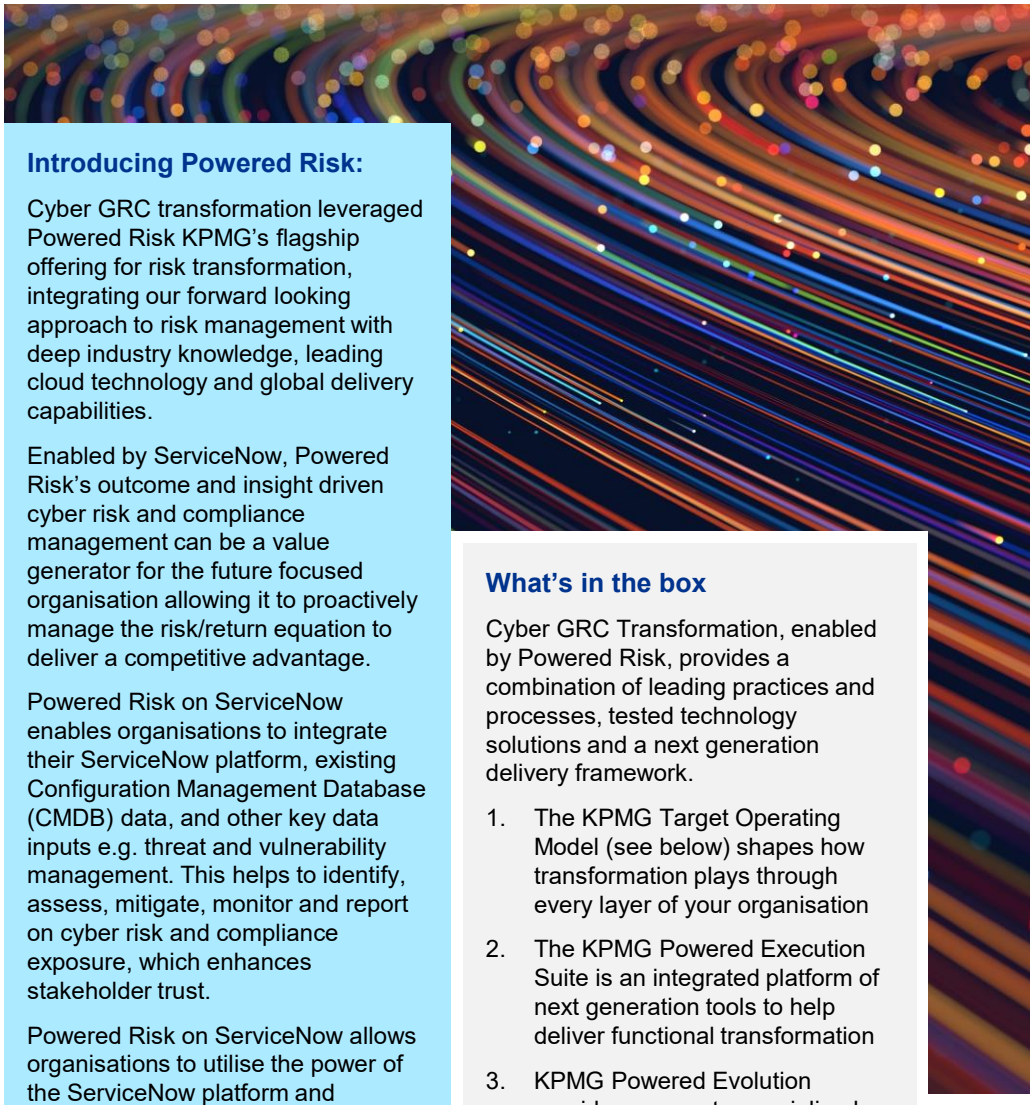
What are the benefits of KPMG's Cyber GRC transformation offering?

- Improved CAF compliance and efficiency of completion and reporting
- Improved cyber risk controls, monitoring, assurance and attestation
- Improved cyber risk reporting, governance and decision-making
- Improved Board-level ownership for cyber risk oversight and management
- Ability to establish a data-driven cyber risk appetite
- Improved cyber-risk input into cyber business case analysis and development
- Improved quantification of cyber risk and investment prioritisation
- Improved cyber risk process/product standardisation driving adoption and productivity
- Systematic reduction of cyber risk exposures, aligned to risk appetite

Our service features

- Cyber GRC maturity assessments, discovery and as-is state analysis
- Cyber GRC Target Operating Model design and deployment
- Cyber GRC capability/controls design including end-to-end risk management processes
- Enterprise Cyber Risk Framework design, aligned to CAF and NIST
- Cyber risk culture programme discovery, design and implementation
- Cyber risk programme delivery and embedding, driving adoption and compliance
- Cyber risk quantification, stress testing and strategic/tactical risk exposure reporting
- Risk assessment, risk assurance and attestation design and delivery
- ServiceNow Advanced Risk implementation - design to deployment and embedding

What is Cyber GRC Transformation?



Overview

Cyber Risk and business professionals are faced with important questions:

- How can the cyber risk and compliance functions dynamically respond to existing and emerging risks, as well as increasingly risks, as well as increasingly complex regulations and reporting, e.g. GovAssure?
- How do I respond to public and citizen mistrust in how departments handle their data or the impact of new technologies, and how can the cyber risk function allay their fears?
- How do I get value from my cyber risk and compliance data and inform business decisions from solutions already in the marketplace?
- How can I change the organisation's mindset and culture to embed cyber risk and management and new ways of working across all operations?
- How do I proactively manage the magnitude of cyber risks, compliance obligations and issues facing my organisation?
- How do I build tomorrow's cyber risk function today in the context of wider organisational transformation and balance people/automation?
- How do I empower the first line to take ownership of cyber risk and control management activities?

Introducing Powered Risk:

Cyber GRC transformation leveraged Powered Risk KPMG's flagship offering for risk transformation, integrating our forward looking approach to risk management with deep industry knowledge, leading cloud technology and global delivery capabilities.

Enabled by ServiceNow, Powered Risk's outcome and insight driven cyber risk and compliance management can be a value generator for the future focused organisation allowing it to proactively manage the risk/return equation to deliver a competitive advantage.

Powered Risk on ServiceNow enables organisations to integrate their ServiceNow platform, existing Configuration Management Database (CMDB) data, and other key data inputs e.g. threat and vulnerability management. This helps to identify, assess, mitigate, monitor and report on cyber risk and compliance exposure, which enhances stakeholder trust.

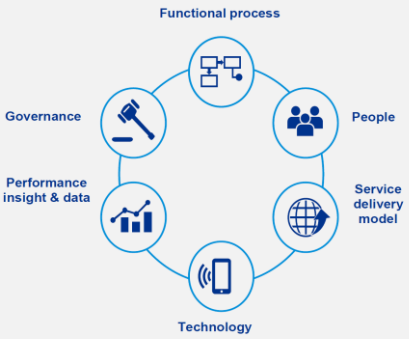
Powered Risk on ServiceNow allows organisations to utilise the power of the ServiceNow platform and available data to form strong insights on their cyber risk and compliance posture.

Powered Risk delivers on the promise of deploying capabilities to help an organisation identify, assess, mitigate, monitor and report on cyber risk and compliance exposure, which enhances stakeholder trust. A trusted business has the competitive advantage of being able to innovate and disrupt with confidence.

What's in the box

Cyber GRC Transformation, enabled by Powered Risk, provides a combination of leading practices and processes, tested technology solutions and a next generation delivery framework.

1. The KPMG Target Operating Model (see below) shapes how transformation plays through every layer of your organisation
2. The KPMG Powered Execution Suite is an integrated platform of next generation tools to help deliver functional transformation
3. KPMG Powered Evolution provides access to specialised resources to drive continuing evolution.



Our Approach

Implementation plan:

Powered projects are delivered over five phases as follows:

Vision: in this phase the high-level scope, the project plan, the approaches and strategies for how the platform will be implemented during the remainder of the project are documented and accepted. In addition, during this phase preparation for activities in the validate phase take place.

Validate: in this phase the designs for the items in scope/platform will be finalised, documented and accepted by the customer to facilitate entry into the construct phase.

Construct: in this phase the platform is configured, and integrations built in accordance with the design. A series of test phases collectively determine if the system was built in accordance with the design. Data is also cleansed in preparation for migration and tests will be conducted to confirm the ability to migrate and reconcile data from the legacy platforms to the new platform.

Deploy: during this phase the platform is subject to user acceptance test, users are trained, data is migrated and the project transitions from implementation to production.

Evolve: during this phase the new platform is in production and the customer starts operating the target processes on it, with the agreed level of post go live hypercare support.

Timescales are driven by a number of variables including the scale and complexity of each customer's scope together with quality of data and availability of resources. We would agree the implementation plan, resource requirements and project milestones as part of the process of procuring our services.

Onboarding and offboarding support:

The range of on boarding activity required for clients adopting a KPMG powered service would be agreed as part of the procurement of the service. As part of the service, we build and agree a plan covering all relevant activities, planned times, durations, responsibilities, accountabilities and outputs. Typical elements comprise:

Onboarding:

- Development of the project charter, if needed, and associated project guiding principles
- Assistance to develop/articulate the case for change
- Change management and communications strategy to aid who needs to be communicated with, how and when in relation to the changes the project is planning to implement
- Provision of orientation sessions in the powered methodology, powered assets, platform principles, powered execution suite tools to prepare clients teams for the program, including workshop execution
- Engagement with client teams to understand the 'as is', to take into account change impact assessment during workshops
- Definition of collective roles and responsibilities including that for outputs

Execution of a project kick off event and associated materials to formally launch the project and to aid new joiners in orientation the migration of client data is often a critical path item on the on-boarding plan. We work with our clients to assist them to transition data to the new platform. As part of this we would provide standard templates and knowledge transfer to allow the client and/or their existing service provider to extract and provide data in the correct format.

Offboarding:

Each implementation has a post go live ("evolve phase") in which KPMG will provide post go live support working with each client's business as usual (BAU) team to fully transition on going service delivery to the clients' BAU support team according to the agreed plan.

Our Approach Cont'd

Onboarding and offboarding support:

The range of on boarding activity required for clients adopting a KPMG powered service would be agreed as part of the procurement of the service. As part of the service, we build and agree a plan covering all relevant activities, planned times, durations, responsibilities, accountabilities and outputs. Typical elements comprise:

Onboarding:

- Development of the project charter, if needed, and associated project guiding principles
- Assistance to develop/articulate the case for change
- Change management and communications strategy to aid who needs to be communicated with, how and when in relation to the changes the project is planning to implement

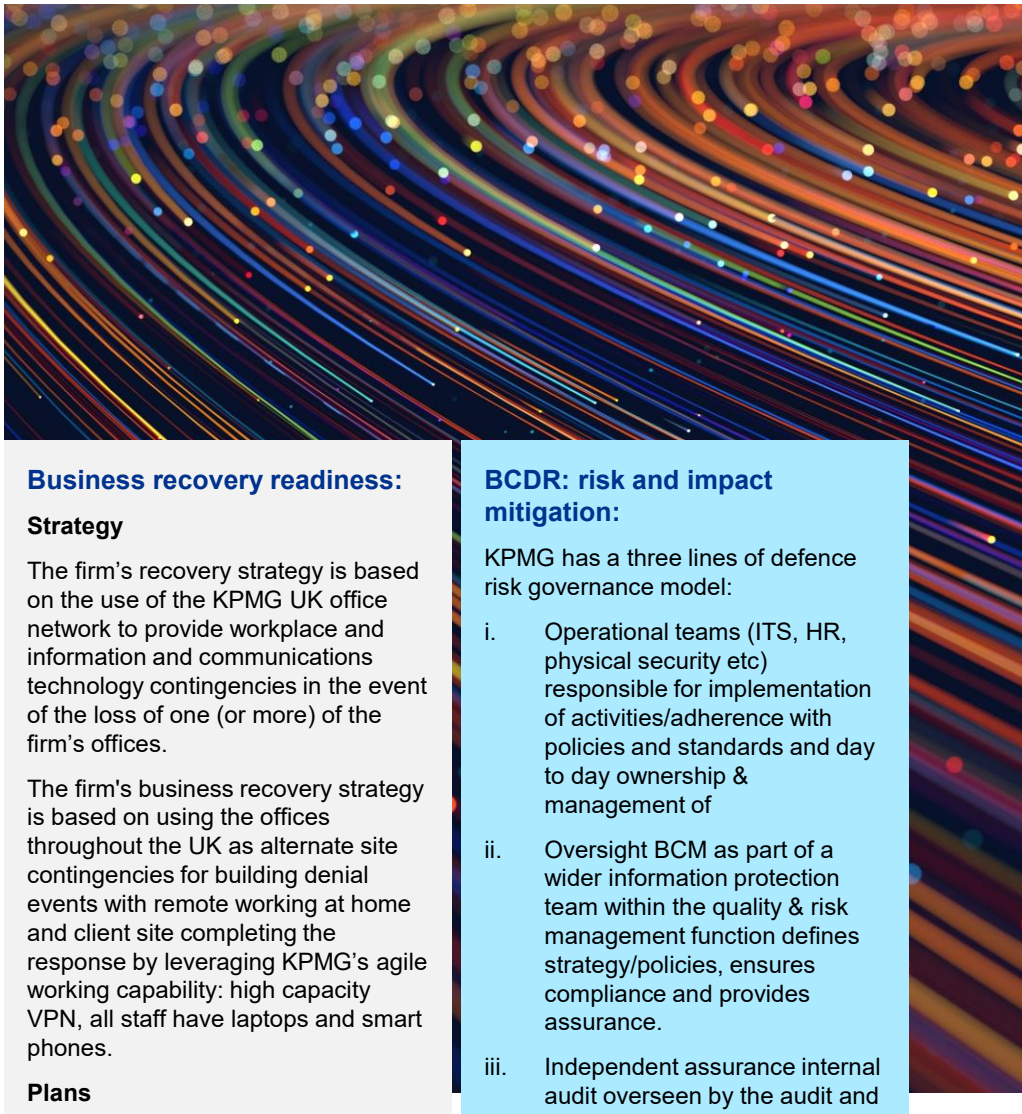
Onboarding and offboarding support:

- Provision of orientation sessions in the powered methodology, powered assets, platform principles, powered execution suite tools to prepare clients teams for the program, including workshop execution
- Engagement with client teams to understand the 'as is', to take into account change impact assessment during workshops
- Definition of collective roles and responsibilities including that for outputs
- Execution of a project kick off event and associated materials to formally launch the project and to aid new joiners in orientation the migration of client data is often a critical path item on the on boarding plan. We work with our clients to assist them to transition data to the new platform. As part of this we would provide standard templates and knowledge transfer to allow the client and/or their existing service provider to extract and provide data in the correct format.

Offboarding:

Each implementation has a post go live ("evolve phase") in which KPMG will provide post go live support working with each clients business as usual (BAU) team to fully transition on going service delivery to the clients' BAU support team according to the agreed plan.

Service Details



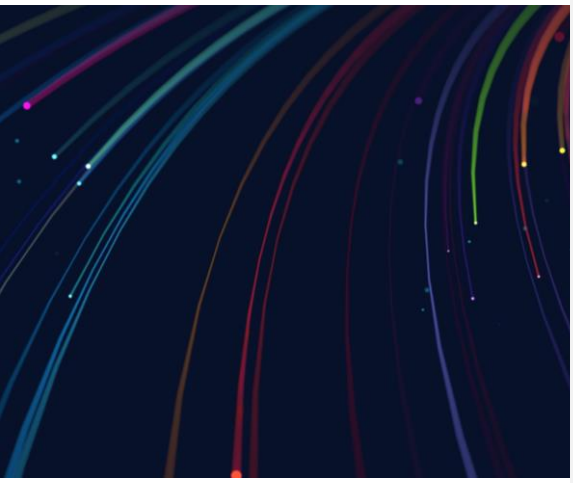
Data backup and restore, and disaster recovery provision

KPMG has comprehensive business continuity and physical security procedures in place to cover its day to day and business operations.

The KPMG business continuity and readiness statement executive summary dated November 2022 includes the following: the business continuity team follow the business continuity institute best practice guidelines and comply with the international standard iso22301: 2012

The firm has iso27001 accreditation, the scope of the external audit extended for the first time in 2010 to include the business continuity management across the UK firm externally audited every six months.

Incident & crisis management response: role holders are trained and exercised.



Business recovery readiness:

Strategy

The firm's recovery strategy is based on the use of the KPMG UK office network to provide workplace and information and communications technology contingencies in the event of the loss of one (or more) of the firm's offices.

The firm's business recovery strategy is based on using the offices throughout the UK as alternate site contingencies for building denial events with remote working at home and client site completing the response by leveraging KPMG's agile working capability: high capacity VPN, all staff have laptops and smart phones.

Plans

Business continuity coordinators are responsible for the maintenance and execution of client service recovery plans.

The business recovery plans are reviewed within an ongoing programme of scenario based tabletop exercises.

The plans are maintained and centrally monitored using business continuity planning software. These plans are supported by the firm's infrastructure (ITS, facilities and HR) support plans

Exercising

Business recovery plans: exercised once every year.

Detailed audits of the content of all plans are completed annually

BCDR: risk and impact mitigation:

KPMG has a three lines of defence risk governance model:

i. Operational teams (ITS, HR, physical security etc) responsible for implementation of activities/adherence with policies and standards and day to day ownership & management of

ii. Oversight BCM as part of a wider information protection team within the quality & risk management function defines strategy/policies, ensures compliance and provides assurance.

iii. Independent assurance internal audit overseen by the audit and risk committee, external audit (ISO27001 BCM audit on a biannual basis) and client audits.

KPMG operates a twin data centre model, providing provision to manage disruptions affecting hosted it infrastructure and business applications.

The primary and secondary data centres are dedicated data halls hosted in purpose built UI tier iii equivalent facilities. The buildings are separately owned by two of the market leaders in data centre colocation.

KPMG operates a twin data centre model, providing provision to manage disruptions affecting hosted it infrastructure and business applications.

Service Details

BCDR risk and impact mitigation, continued:

The data centres are sufficiently physically separated to minimise exposure to shared risk/threat occurrence, whilst within distances to support synchronous replication of data to minimise data loss opportunity in the event of DR.

Both facilities are located in the UK. Production IT systems are typically hosted on an active passive infrastructure design, providing high availability and managed failover between data centres, underpinned by resilient fibre links.

KPMG provides a disk to disk backup strategy supplemented by snapshot and clone solutions to provide the lowest RTO. Disk backups are replicated between data centres for additional assurance. Long term data retention is provided through a choice of archive disk or tape backup where required. The KPMG network is fully resilient, with all offices linked by dual network paths into an MPLS wide area network, providing connectivity to KPMG's data centres.

KPMG has several risk assessments for suppliers in place, which cover business continuity, health and safety and data security.

KPMG provides related consulting services to clients.

Pricing overview, including volume discounts or data extraction costs

Consulting prices are as per the G cloud 15 rate structure. Projects can be charged using either fixed price and time and materials approaches, according to the situation, and can be delivered on site and/or remotely.

Volume discounts would be considered on a case by case basis.

Typically, data extraction is addressed by clients with input from KPMG but we work closely with our clients to develop the data migration strategy and plan, providing templates with the target platform format, to enable our clients to cleanse and map extracted data. We can apply varying levels of data migration automation techniques to address large volumes or complex requirements.

Service constraints like maintenance windows or the level of customisation allowed

Maintenance:

Cloud software is updated regularly to apply minor fixes and to a schedule for more significant updates. These types of maintenance activities are usually well documented and pre advised by the cloud software vendor and, where notified, are considered in project planning and particularly design and regression testing activities. The cloud software vendors which are the subject of a powered implementation typically apply updates at times aimed at minimising disruption to project and day to day operational use.

Customisation:

The powered approach is to 'configure rather than customise', adopting standard cloud software functionality to enable ease of upgrade and to take advantage of new updates and releases with minimal issues. ServiceNow provides the ability to create scoped applications for any customisation that is necessary to protect the core platform from changes that would impact upgrades. KPMG has leveraged this feature and aligned with ServiceNow recommendations for leading practice application creation for the powered risk services.

Service Details

Service levels like performance, availability and support hours

The service levels and support hours for cloud software vendors are per the relevant authority's direct agreement with that vendor.

KPMG can provide managed services with extended support hours coverage and would be happy to discuss this and specific service level requirements on a case by case basis.

How you'll repay or compensate buyers if you do not meet service levels

Any service credit regime for cloud software vendors are per the relevant authority's direct agreement with that vendor.

KPMG can discuss specific service credit requirements on a case by case basis.

The ordering and invoicing process

The ordering process for G cloud services is laid out in the 'G cloud buyers' guide on the www.Gov.Uk website. Invoicing arrangements will be as per the agreed G cloud order form and will vary from engagement to engagement.

How buyers or suppliers can terminate a contract:

Our terms provide for a range of scenarios where both Buyer and Supplier are able to terminate contracts, to defined notice periods, for:

- Convenience
- Failure to remedy a material breach
- Insolvency.

In addition, Supplier has the right to terminate if: (a) circumstances arise or have arisen which KPMG reasonably considers does or may impair its impartiality, objectivity or independence in respect of the provision of the Services; or (b) for legal, regulatory or other justified ethical reasons.

After sales support

KPMG can provide a range of services to assist users of this service post implementation ranging from managed services, staff secondment, impact assessments on the implementation due to cloud software vendor upgrade/major patches and associated regression testing.

Any technical requirements

Each cloud software vendor provides details directly of their supported web browsers and personal computer and related requirements. These are not onerous and typically do not present an issue for most organisations.

KPMG also uses a range of collaboration tools, as appropriate, to assist in the delivery of the services. Microsoft office 365 & teams are used by all colleagues within the firm, with other tools such as Jira and confluence being used if required for the project. KPMG is also able to use other collaboration tools if used on client provided laptops.

Project team members will need to be provided with a software VPN and virtual machine or client laptop.

Contact Us

Amit Kumar

Director, **Head of AI and Cloud Propositions**

KPMG LLP, CIO Advisory
15 Canada Square
London E14 5GL
Amit.m.kumar@kpmg.co.uk

Douglas Dick

Partner,
Head of Cloud Engineering Risk Controls

KPMG LLP, FS Tech Risk
15 Canada Square
London E14 5GL
douglas.dick@kpmg.co.uk

kpmg.com/uk

Document Classification: KPMG Confidential

CREATE. | CRT164925A January 2026