Capita

IT Disaster Recovery Policy

The purpose of this policy is to ensure Capita's critical assets are ready "….to support business operations in the event of emerging events and incidents and related disruptions that could affect the continuity of critical business functions" (ISO 27031).

This policy mandates the implementation of Capita's IT Disaster Recovery Standard to minimise the impact of serious incidents and recover IT systems/business functions and technical infrastructure to an acceptable level whilst reducing operational disruption to Capita's business, colleagues, and clients.

We are committed to:

- Maintaining policies, controls, standards, and procedures that identify and manage vulnerabilities that could impede our ability to be resilient.
- Promoting and fostering a leadership culture that supports effective technical resilience management and that addresses threats to meeting appropriate service delivery levels.
- Understanding the regulatory changes and challenges given the diverse nature of our business.

What you can expect from us:

- We monitor controls (preventative, detective, and corrective) across the group to identify and manage vulnerabilities. In addition, we maintain frameworks that:
    - Provide group wide coverage that ensures Capita responds, manages, and resolves matters in a consistent way that includes identified stakeholders.
    - Support our risk appetite and impact tolerances on technical resilience.
    - Leverage functional policies and standards to identify vulnerabilities and report accordingly.
    - Aim to minimise and mitigate reputational, legal, regulatory, people, and financial impacts on both Capita and its clients.
    - Monitor and escalate any non-compliance with this policy as necessary - which may include our audit and risk committees and ultimately to the board.

What we expect from our 1st Line of Defence, typically MDs and their operational teams:

- To have primary ownership, responsibility, and accountability for identifying, assessing, and managing all Capita's IT Disaster Recovery related risks and controls as depicted within the standard.
- Maintain a register of your customers that have a contractual requirement for Capita to provide IT DR and associated Recovery Time Objectives and Recovery Point Objectives for these contracts.
- Maintain a register of critical assets (applications/service/infrastructure) that you are responsible for.
- Develop and document an IT Disaster Recovery Plan appropriate for the Division/Business Unit.
- Ensure you have a complete set of Technical Recovery plans for each critical business service as detailed in the IT DR Plan.
- The IT Disaster Recovery plan must be updated at a minimum annually or following significant change.
- Ensure that the IT Disaster Recovery Plan is tested at a minimum annually.

How we will achieve this:

- Every division and function must adhere to our IT Disaster Recovery Standard.
- We require all our divisions, businesses, and functions to follow the applicable technical policies, standards, and frameworks and oversee the effective management of risks that impact our ability to operate a technologically resilient business.
- We review policy compliance through groupwide risk-based monitoring and periodic auditing activity and report on policy compliance and related risks through risk governance which ultimately includes the reporting of significant matters to our plc risk committees and board.
- Ensure that Suppliers who provide services to Capita are technically resilient and meet all Capita contracted and regulatory requirements.
- Understanding your business in terms of property, people, technology, and suppliers will provide full oversight of Capita's technical resilience needs and dependencies (and by default potential vulnerabilities).
- Ensure your business or function has an Incident and Major Incident response capability in line with business requirements.
- Take ownership of the Incident, Crisis, and IT Disaster Recovery Management arrangements for the divisional or functional area for which you are responsible.