BS 31111 audit and assessment

A top-down approach to managing cyber risk, using the BS 31111:2018 standard – helping leaders to understand risks, mitigate them and stay resilient

At a governance level in your organisation, you have ultimate accountability for managing cyber risk.

This means that, as the number and sophistication of cyber incidents increases, it's up to you to maintain a clear, high-level understanding of the changing risks you face – and what you are doing to mitigate them.

To help you develop this understanding, it's natural to involve your IT team. But you cannot delegate the responsibility away. After all, in an increasingly digital age, cyber risk is business risk.

This responsibility can be challenging for any governing body. So to help you develop the high-level understanding you need, we offer an audit and assessment service using the BS 31111: 2018 standard– which was published in 2018 to support a governance-led approach to cyber security.

BS 31111 audit and assessment is a component of our wider **cyber security assessment service (jisc.ac.uk/cyber-security-assessment)** – delivered by Jisc's trusted in-house cyber security experts, who are experienced, trained and certified.

How does the BS 31111 assessment help me?
At a governance level, our BS 31111 audit and assessment service helps you to identify cyber risks, understand them and ensure that appropriate processes are in place – in order to help build resilience to cyber-attacks and other disruptive events, while improving operational performance.

In turn, this helps you to demonstrate the steps you're taking to stakeholders and regulators.

The service helps you to:

- **Identify and understand cyber risk**
  The assessment helps you to understand your digital investment and the cyber-risks that are associated with it – understanding both positive and negative outcomes

- **Understand your level of resilience**
  Using this assessment, you can understand and identify your level of preparation – including not only prevention measures, but also response capabilities that will help you manage a cyber incident

- **Plan in a changing landscape**
  As digital technologies change, so do the associated risks. This assessment helps you understand how you manage and understand changes in the cyber landscape, whether or not you're planning for digital transformation

- **Allocate resources appropriately**
  Armed with this assessment, you can ensure that you've allocated adequate resources – whether financial, human, information-based or technological – that you need to manage risk, stay resilient and operate efficiently

To find out more about BS 31111 audit and assessment, please:

Contact your account manager **https://ji.sc/ContactAM**

or email **professional.cyberservices@jisc.ac.uk**

Please visit **jisc.ac.uk/network/security** to see our range of cyber security services.