National Cyber Security Centre
a part of GCHQ

Cyber Security Toolkit for Boards

Cyber security is central to an organisation's health and resilience, which means it's the Board's responsibility.

Managing cyber security is a continuous, iterative process, but broadly speaking there are three overlapping components, summarised below.

For these steps to be effective, you'll also need to get the environment right.

For more information, please visit www.ncsc.gov.uk/collection/board-toolkit

1 Gather information

Get the information you need to make well-informed decisions about the risks you face.

Establish what is important to you.
Find out what your estate looks like.
Identify your vulnerabilities.
Identify what might be of value to an attacker.
Identify who might target you, and how they would do it.

2 Prioritise your risks

Use this information to understand and prioritise your risks.

Good risk management should go beyond just compliance.

Integrate cyber security into organisational risk management processes.

3 Take steps to manage your risks

Take steps to manage those risks.

Make arrangements with any suppliers, providers or partners to mitigate the risks posed by supply chain attacks.

Have plans in place for when things go wrong.

Implement suitable defences, focused on mitigating your risks.

Getting the environment right

Embedding cyber security in your organisation
Cyber security is not just 'good IT' - it must enable an organisation's digital activity to flourish.

Developing a positive cyber security culture
Board members should lead by example to help promote a healthy cyber security culture.

Growing cyber security expertise
As the demand for cyber security professionals grows, you need to plan ahead to ensure your organisation can draw upon the expertise you need.

@ncsc
National Cyber Security Centre
www.ncsc.gov.uk