Digital Risk Assessment Worksheet

A digital risk assessment is a check-up for your business's digital health.

By identifying potential threats to your digital systems, like viruses, malware, hackers, or human error, you can help prevent data breaches, cyberattacks, system failures, and other events that can hit your business hard.

Our digital risk assessment worksheet highlights some key areas to help you reduce risks to your business or a particular project.

Please note that as all businesses are different, this is designed only as an overview, and not an exhaustive list.

vodafone business

Digital Risk Assessment Worksheet

Digital Risk Assessment Worksheet

Identify your critical assets and data

Review and understand your data, systems and potential risks, so you can decide which areas should be your highest priority.

- ✓ Identify what data you collect, process and store, and decide which is critical to your operation, reputation, or compliance. This might include financial data, customer information, intellectual property, or other sensitive information.
- ✓ Identify the systems and applications you use to process and store data, and decide which are key to your operations or contain critical data. This might include databases, file servers, email systems, or other applications.
- ✓ Assess the likely impact of a breach or loss of each critical asset or data type. This might include the potential cost, reputational damage, or legal or regulatory action.
- ✓ Identify the threats and vulnerabilities that could lead to a breach or loss of each critical asset or data type. This might include cyber attacks, insider threats, events like fire or flood, or other risks.
- ✓ Assess the chances and potential impact of each threat and vulnerability, and prioritise them based on the highest risk.

Tools and resources

There are a number of useful tools and resources you can use to help you identify weak spots.

- ✓ Vulnerability scanners scan networks, systems, and applications for potential vulnerabilities and weaknesses that attackers could exploit.
- ✓ Penetration testing tools simulate attacks on your systems and applications to identify potential weaknesses, and test if your current security is effective.
- ✓ Security information and event management (SIEM) tools monitor and analyse your network traffic and system logs to detect potential security incidents, and respond quickly.

Take simple, practical steps

Once identified, implement strategies or controls to plug any gaps in your security.

- ✓ Restrict access to sensitive data to only people authorised to use and process it.
- ✓ Update anti-virus software or install the latest security patches.
- ✓ Make sure all passwords are strong and changed regularly.
- ✓ Implement regular online or face-to-face cybersecurity training for your team.

Look to the future

Digital security is never a once-and-done exercise. Cybercriminals are constantly evolving new tactics, so make sure you stay ahead of the game.

- ✓ Regularly review and update your risk assessment so it stays current and relevant as your business changes and grows.
- ✓ Create cybersecurity policies and procedures that set out password management, access controls, updating software, and how you collect, process, store and delete data.
- ✓ Carry out regular security audits to make sure your digital security practices are up-to-date and effective.
- ✓ Develop an incident response plan that outlines what steps to take following a cybersecurity incident, including how you would contain it, tell your stakeholders, and restore your systems and data. And test it.
- ✓ Think about buying cyber insurance designed to cover digital risks if your standard business insurance excludes it.