Superfast Business Wales

Business Guide

IT Risk Management

As your business increasingly relies on its IT systems and takes advantage of the opportunities present by Superfast Broadband, so it becomes ever-more important to identify and control the variety of threats ranging from hackers to equipment failure that these systems face.

www.business.wales.gov.uk/superfastbusinesswales | 03000 6 03000

Busnes Cymru Business Wales

UNDEB EWROPEAIDD EUROPEAN UNION
Llywodraeth Cymru Welsh Government
Cronfa Datblygu Rhanbarthol Ewrop
European Regional Development Fund

Llywodraeth Cymru Welsh Government

IT Risk Management

As your business increasingly relies on its IT systems and takes advantage of the opportunities present by Superfast Broadband, so it becomes ever-more important to identify and control the variety of threats ranging from hackers to equipment failure that these systems face. It's vital to understand these threats, assess the probability of them occurring and consider the impact upon your business should they actually happen. This in a nutshell is the role of IT risk management.

What we're looking at here is a component of organisational risk management that focuses specifically upon IT systems, services and networks. The intention is to identify potential IT- related risks and put appropriate measures in place to mitigate against these.

So, risk management plays a key role in the security of your IT systems, since it's effectively identifying the threats that your security software and processes need to defend against. It also has strong links with your business continuity plans, as these plans need to specify how you intend to deal with system failures should the risks you've identified actually occur.

This guide will look at why IT risk management is so important to a business and how to implement a risk management process through a series of well-defined steps.

> IT risk management does not work 'out of the box'. It is not a product to purchase or a policy to put in place. Instead, it is a process of business risk management that must be performed on an ongoing basis. (Gartner)

Understand

What Does Risk Management Do?

To some people risk management simply means insurance. However, insurance at best can only provide money–and that will not necessarily come at the right time or be sufficient in itself to save your business.

Risk management, therefore, concerns itself with:

- Identifying the potential risks to your IT infrastructure
- Assessing the probability of these risks actually occurring
- Planning how to reduce the impact on your business should they happen
- Planning for the recovery of operational capability if the risk does occur despite the precautions taken

Identifying risks

Your IT systems and the information they hold face a wide variety of threats. These can range from online risks through to infrastructure failure and human error.

Any of the above problems have the potential to severely disrupt your business, lose customer orders and damage your reputation, in some cases irreparably. Risk management is all about identifying the potential risks at the earliest possible opportunity, on the basis that forewarned is forearmed. Having identified the threats that might be posed to your IT systems you can then go about putting measures in place to minimise or completely remove them.

Assessing the risks

This aspect of risk management is concerned with estimating the probability and likely impact of individual risks so that they can be prioritised accordingly. This prioritisation will be based not only upon the likelihood of the risk occurring, but also upon the importance of the information, service or resource that is under threat because of it. The assessment should also take into account the risk appetite of the organisation. In business today, risk plays a critical role, with almost ever y business decision requiring executives and managers to balance risk and reward. So, IT risk should also be viewed in the context of the level of risk that the organisation is comfortable with.

Reducing the risks

At this stage risk management is concerned with planning appropriate responses to risks, assigning owners and actionees and then implementing, monitoring and controlling these responses. Essentially we’re looking to reduce the probability of the risk occurring and limit its impact if it does.

Planning for recovery

Inevitably, despite all of the planning, some risks will actually turn into incidents, leading to various problems with the delivery of IT and web services. In such cases it’s vital to get these services up and running as soon as possible and minimise the disruption and financial impact upon the business. It’s here where risk management morphs into business continuity planning. For further information on how to develop effective plans that will enable your business to bounce back from a disaster with the minimum disruption and get you back to ‘trading as normal’ as quickly as possible.

Adopt

Getting Started

As we’ve mentioned previously, IT risk management is a process containing a number of discrete stages.

Carry out a risk assessment

When assessing the IT risks that your business may face you should focus on the most serious risks, based on the likelihood of the risk happening and the cost or impact if it does so.

So, the risk assessment stage is all about identifying the potential risks to your IT systems and the impact these may have upon your business. Some examples of risks that need to be considered include:

- **Physical threats** – the risk that your IT systems could be rendered inoperable as a result of theft or damage from fire or flood
- **Online threats** – the danger that a hacker might, for example, steal your customer database, infect your IT system with a virus, or cause your website to fall victim to a denial-of-service (DoS) attack which results in the site offering a reduced level of service or, in some cases, causing it to cease operation completely
- **Data confidentiality** - the risk that confidential or sensitive information may be mishandled perhaps because of human error by your staff) or fall into the hands of those who shouldn't have access to it
- **Data integrity** – the risk that the underlying data in your key business systems is unreliable because it is incomplete, inaccurate or otherwise suspect
- **Data availability** - the short term loss of service due to IT systems failure has the potential to have a significant - and potentially long-lasting-impact on the daily operations of your business.
- **Project risk** – the risk that an investment made in IT will fail to provide the expected business value
- **Skills deficiency** – the risk that a member of your staff with key knowledge upon which you are heavily reliant could be head-hunted by competitors
- **Supplier issues** – the risk that a supplier who you are dependent upon for a key service suffers a major system problem, fails to deliver the appropriate levels of maintenance to your systems or simply goes out of business

Quantify the risks

Having identified the risks the next step is to quantify them according to the probability of their occurrence and the likely impact should they occur.

The probability can be assessed as high, medium or low, as can the impact. A simple matrix, such as the one shown below, can help to highlight the high probability and high impact risks.

Control the risks

Once the risks have been quantified, there is then a requirement to decide upon the approach to be taken to control or mitigate against these.

There are a number of approaches that can be taken:

- **Accept the risk**–do nothing
- **Avoid the risk**–do something else, for example opt for a cloud -based solution rather than an in-house one

  Reduce the risk–take mitigating action, such as implementing strong security controls to protect sensitive information
- **Contain the risk**–minimise the impact, perhaps by using more than one supplier
- **Transfer the risk**–outsource the activity or take out some form of insurance

The key to the control stage is to plan appropriate responses to the risks you've identified. It's also worth noting that any countermeasures should be proportional to the risks they are intended to guard against. For example, there is little merit in spending £5,000 to protect your business against a risk that will only cost you £500 if it actually occurs.

Review the effectiveness of the measures

It's important that risk management should be seen as an ongoing process rather than a one-off solution. The risk landscape is constantly changing and new threats are emerging almost daily.
So, you should continuously reassess the threats to your IT systems and actively search for new ones by conducting the risk analysis review on a regular basis.

And, as we've mentioned previously, if the worst actually happens and a risk becomes an incident that damages your systems, then it's vital your business continuity plan is capable of kicking into action and ensuring that you get back to business-as-usual as quickly and seamlessly as possible, minimising the impact upon your customers.

Exploit

What Business Benefits Can I Expect

Effective risk management can deliver a wide range of benefits to an organisation, from both an IT and a wider business perspective.

IT-related benefits

- It ensures that the risks to your IT systems and services are identified in a structured manner, and the implications of these are fully understood.
- It enables you to take account of these risks to your IT systems in your security and business continuity planning, so that most risks are mitigated, and in the event of any still occurring, the business will be up and running with minimum disruption.
- Importantly, you should consider the implications of NOT taking the time to understand the IT-related risks to your business and, as a consequence, doing nothing...

Business benefits

- It is reassuring to your customers and confirms that you take the continuity of your services to them seriously
- It assists in addressing specific regulatory requirements for continuity planning that exist in certain industry sectors such as financial services
- There are fewer sudden shocks and unwelcome surprises to your business
- It can save you money through more efficient controls, more effective architectures and appropriate levels of protection

Top Tips

Take the time to identify the risks posed

The risk assessment stage will underpin all of the subsequent activities undertaken within the risk management process, so it’s worth spending sufficient time to ensure that you get it right.

Quantify any risks you identify

Identify the priority of any threats posed by rating the probability of occurrence and the likely impact on your business, this will ensure that you focus upon the most significant risks.

Understand the risk appetite of your business

Risk plays a critical role in business today, so IT risk (as with all types of business risk) should be viewed in the context of the level of risk that you are comfortable with.

Agree on how best to handle the risks

Develop an action plan for addressing the risks that pose particular concerns, with the aim of reducing them As Low As Reasonably Practical (ALARP).

Integrate your risk management and business continuity plans

Make sure you have a business continuity plan covering any serious IT-related risks that you cannot fully control.

Allocate responsibilities to individual members of staff

Give your staff specific risk management-related activities to undertake and ensure that they are aware of what is expected of them.

It’s not a one-off exercise

Regularly review and update your IT risk assessment and business continuity plan to take account of emerging threats.

Risk management should be cost effective

Ensure that any countermeasures you implement are proportional to the risks you are protecting against.

Is it worth it?

Consider the potentially disastrous implications of not fully understanding the IT–related risks that your business might face.

NEXT STEPS

1. **Register to attend a fully-funded Business Development Workshop.**
   www.business.wales.gov.uk/superfastbusinesswales/events

2. **Make an appointment to see a Business Advisor who will help you create a personal action plan to grow your business.**
   www.business.wales.gov.uk/contact-us

For further information on IT Risk Management take a look at:

See how other businesses in Wales have exploited Superfast Broadband
www.business.wales.gov.uk/superfastbusinesswales/superfast-success-stories

Find out how much your business could save with our
www.business.wales.gov.uk/superfastbusinesswales/savings-calculator

Other business guides that may interest you include:
www.business.wales.gov.uk/superfastbusinesswales/superfast-business-guides

For monthly updates on business development, technology news and events subscribe to the Business Wales Newsletter below.
https://public.govdelivery.com/accounts/UKWALES/subscriber/new

For more information call 03000 6 03000 or visit:
www.business.wales.gov.uk/superfastbusinesswales