FORDWAY

fordway.com

Fordway Whitepaper

April 2022

Managing Information Security Risk in a digital world

Fordway Whitepaper
April 2022

Executive Summary

Contents

As many organisations now adopt a hybrid work model, they have also opened themselves up to new information security risks.

With these systems increasingly integrated into routine working, now is the time for organisations to review whether they have appropriate governance and compliance in place for the long term.

They need policies and processes that will provide assurance that data is secure, maintain customer trust and protect the organisation's reputation. These need to be integrated across all channels to ensure nothing slips through the gaps.

Getting this right means first understanding that information security issues are not just IT risks but business risks. Tackling them requires the support and commitment of the board and senior management.

Organisations first need to classify and prioritise the risks they face, then implement systems and processes to actively manage them without restricting innovation and collaboration. Being too averse to risk can be extremely costly, but too few controls can put an organisation's reputation, and potentially its very future, in jeopardy.

In this document we explain how an organisation can assess the potential impact of the information security (and other) risks it faces by understanding its Risk Appetite; how to incorporate appropriate, tailored risk management into governance and compliance; how to align with best practice and international standards; and how to use compliance to increase credibility and provide reassurance, thus extracting maximum value. We then provide some practical tips for mitigating information security risk.

Introduction

Why information security risks are not just IT risks but business risks

As organisations have rapidly adapted to new ways of working since the beginning of the pandemic, they have opened themselves up to new information security risks. Some of these risks made headlines but were quickly resolved, such as concerns around unsecured video calls. Others have resulted from criminals incorporating COVID-related issues in 'traditional' scams, from spam calls and social engineering to phishing emails and ransomware. However, some of these risks have not yet manifested themselves, and may not become clear until much later.

Do systems and processes rolled out in haste have the appropriate safeguards in place for long-term use? As the novelty of working remotely fades, are employees becoming relaxed about security and exposing their organisation to attack? Plus, information security risks are continually evolving. For example, Brexit brings new requirements in terms of data governance and security.

IT is fundamental to almost every organisation's continuing operations, and digital transformation increases organisations' dependence on IT. Business leaders need to understand that data and information security risks are not just IT risks but business risks; tackling them requires the support and commitment of the board and senior management in order to build them into the organisation's risk and governance framework, and they must be reviewed regularly. This means:

a. Assessing the impact of these new risks, in order to explain to senior management and obtain the support and commitment needed. Senior management will also have to ensure that they adhere to the policies and processes put in place, so obtaining their buy-in will ultimately help to ensure their compliance.

b. Developing an appropriate risk strategy to protect their organisation's information without stifling operational performance.

c. Embedding this strategy in governance and compliance policies which can be used for reporting and can be adapted as technology and the associated threats change.

IT departments need to achieve a delicate balance between mitigation and agility. Being too averse to risk can be extremely costly, but too few controls can put an organisation's very future in jeopardy, so the importance of effective information security risk management cannot be overstated. In this document, we look at what organisations need to consider addressing the risks of new ways of working. We discuss:

- How to assess Risk Appetite as a basis for policy and process
- How to incorporate this into governance and compliance to achieve the required balance between security and flexibility
- Using compliance to increase credibility and provide reassurance, thus extracting maximum value
- Practical tips on steps to mitigate information security risk while maintaining adaptability.

01 Assessing risk appetite as a basis for policy and process

1.1 Perimeter security is increasingly irrelevant to information security

The growth in flexible and cloud-based working, use of a range of endpoint devices and reliance on external organisations such as cloud providers, accelerated by the pandemic, has made every organisation's attack surface significantly larger. Perimeter security has become increasingly irrelevant; it is no longer enough to secure the perimeter of corporate offices and data centres, meaning the traditional castle and moat (or hub/spoke) security architecture needs to be re-examined, along with the relevance of MPLS connectivity and perimeter firewalls. The PC in your user's home, connected through a consumer broadband service, is now your network perimeter and needs to be secured and monitored as such.

The widespread change in working practices has created new ways for those with malicious intent to try and infiltrate an organisation, from malware to phishing attacks and social engineering. As a result, it is more important than ever to provide assurance that data is secure, maintain customer trust and protect an organisation's reputation – all while continuing to drive business growth, increase customer satisfaction, improve productivity and keep costs down. These changes mean IT leaders need to rethink their approach to information security, using tactics such as behavioural and pattern-based security and zero trust networks. However, before turning to this technology they must first understand the risks they face and put in place appropriate policies and processes to address them. This means:

a. Understanding how information security risks arise

b. Assessing the organisation's Risk Appetite

c. Developing an appropriate strategy to protect their organisation without stifling innovation and operational performance

d. Embedding this in governance and compliance policies

1.2 Understanding Risk Appetite makes decision making simpler

Assessing Risk Appetite begins with understanding the organisation's Risk Profile – the risks it faces, both internal and external, how vulnerable it is to those risks (i.e. how likely they are to be realised), and the impact on the organisation if this were to happen. This includes understanding the potential information security risks arising from the cloud, remote working, mobile devices, the IoT etc., and then considering the impact on the organisation's activities if the risk was realised e.g. an unprotected mobile device was lost, or ransomware attack successful. The next step is to assess the organisation's Risk Appetite. This means considering three factors:

- The organisation's ethical stance and culture
- The legal, regulatory and potentially moral frameworks in which it operates, which vary greatly across jurisdictions and even within 'standardised' trading blocs such as the EU
- Its security requirements, which will depend to some extent on the sector in which it operates.

Risk Appetite is largely qualitative, although it has quantitative elements. A measure of an organisation's Risk Appetite could be the threshold value above which it treats each of the risks identified in its Risk Profile as a potential disruptor to its operations.

01

The impact of getting information security risk management wrong include:

• Damage to reputation – how the outside world and its staff view the organisation

• Loss of trust, resulting in loss of market and customer confidence

• Financial loss: both a primary commercial impact through fines and penalties and a secondary impact due to loss of reputation after a compliance breach. There may also be contractual penalties and the cost of insurance to transfer risk

• Loss of competitiveness, due to restricted access to markets and potentially loss of business

• Loss of productivity, if the operating environment is barred or services are suspended.

When organisations understand their Risk Appetite, decision-making becomes simpler because their leaders understand the parameters within which they operate. This enables them to make informed choices about where to invest to protect against the most critical risks to their business. Each organisation needs to ask itself a range of questions.

The answers will depend on its Risk Appetite and which threats it has identified as the most critical to its business. For example:

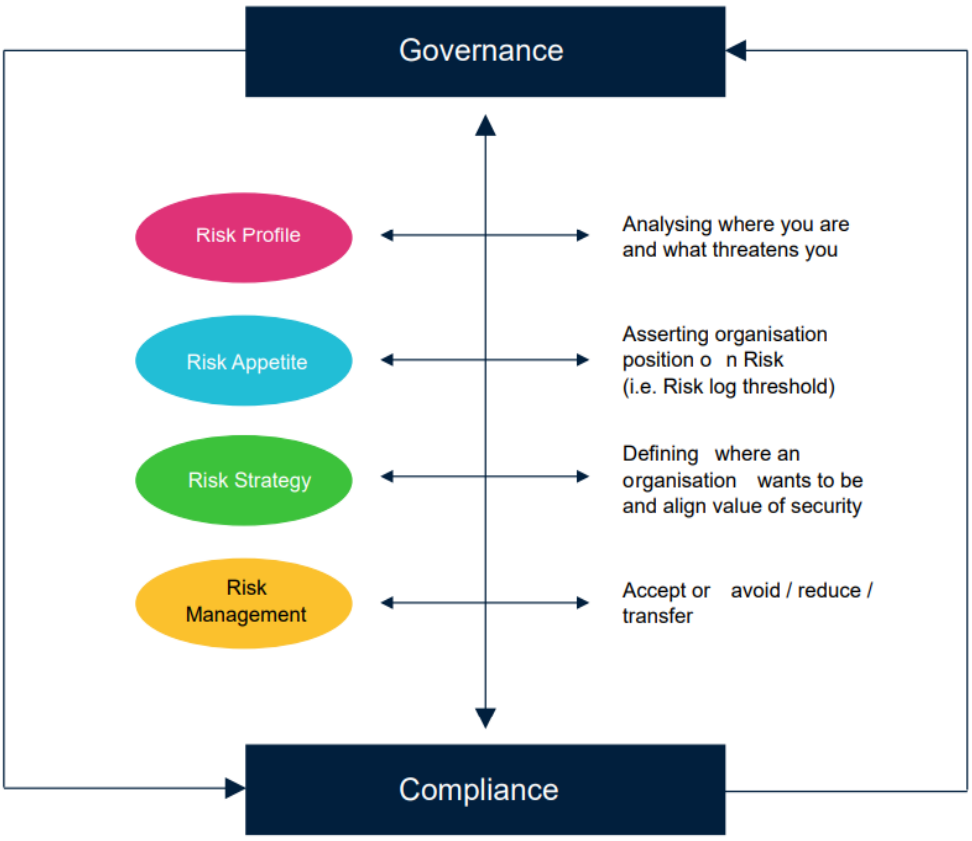
• Device, operating system and application patching is a key aspect of protecting against cyber risk, but is a time-consuming process for those doing it, has a risk of service impact and can be disruptive to the service users. Should it be done weekly, or is monthly sufficient? Does a weekly process provide significantly greater benefit for the additional cost and time required? Does the organisation's patching service ensure that every device is patched as part of the standard process, every time, and can they prove it?

• Do the cloud services the organisation uses provide appropriate business continuity for its needs?

• Should an organisation take out cyber insurance or choose to self-insure?

Being averse to risk can be extremely costly, as overbearing restrictions mean slower responses to changing situations. Some risk can be a positive thing: organisations need to innovate, so may actively incur calculated risks as they grow their business into new areas. However, taking this too far can be even more costly, as too few restrictions can put an organisation's future in jeopardy.

01



Key takeaways

- To understand the parameters in which they operate, each organisation needs to understand its Risk Profile (threats and vulnerabilities) and Risk Appetite (the threshold value above which it treats each of the risks as a potential disruptor to operations).

- Being averse to risk can be extremely expensive, but too few controls can put an organisation's future in jeopardy, so finding the right balance is crucial.

02 Using governance and compliance to manage risk

2.1 Developing policies around how users work

With the potential risks identified and classified, and organisational Risk Appetite agreed, the next step is to develop appropriate policies to manage the highest rated risks. These might include both corporate values and behaviours, which frame how staff operate, and the processes required to carry out day-to-day operations. In developing them, organisations need to assess how their users work and how new ways of working can be aligned to organisational strategy without compromising security.

For digital risks the ITIL framework for service management can assist; the recently released version 4 has been updated to better address digital transformation and will help organisations make the change at pace while maintaining integrity.

Having defined their policies and procedures, organisations should apply governance to review their compliance with these policies. This is not a one-off activity but requires continual monitoring, reporting and service improvement to steer the organisation in the right direction. Governance is not about ticking boxes but means actively understanding and managing risk through reviewing how the organisation operates, thinking about the impact of actions, and establishing and following appropriate policies for those actions.

Compliance then sets out how the organisations show that it is following the policies it has defined. To address and mitigate digital risks it is vital to obtain commitment and buy-in from the board and senior management, as an investment will be needed to implement and operate the required systems and policies. They need to understand the importance of implementing strong governance and what this means in operating a profitable and secure business.

Put simply, it is to align business strategy, objectives and values with operational and IT functions through management systems, whilst complying with industry standards and best practices. It is important to explain that risk management is part of business as usual (BAU), not a one-off activity each time a new risk is identified or new legislation such as GDPR comes around, and that risk management and compliance should be extended to customers and suppliers (section 3.2).

2.2 Making the business case: how good governance and compliance increase credibility

Governance and compliance are often seen as an organisational burden – a means of ensuring that an organisation meets the regulatory and legislative standards of the environment it operates in. However, they should be considered as a statement of organisational values and an investment in future growth, as well as an integral part of risk management strategy. They are a vital part of ensuring that an organisation moves in the desired direction.

02

Proof of effective governance and compliance can be used to increase an organisation's credibility and enable it to respond to changing markets while providing assurance to its customers – particularly if the organisation demonstrates compliance to external, audited standards.

The key points to make to the board for investing in governance and compliance include:

• Done properly, good governance will assure customers and partners that the organisation's systems and values are visible, secure and viable, building confidence and trust and thus supporting sales and driving revenue.

• Increasing or enhancing compliance and achieving new industry standards can help increase revenue by opening new and potentially lucrative markets and revenue streams.

• Good compliance will reduce costly mistakes as well as making lack of performance visible to senior management.

• Effective, streamlined processes will promote security and minimise mistakes; good compliance will demonstrate organisational commitment and avoid unplanned expenditure remediating problems later. Organisations should consider consolidating various standards into single policies where possible, as this will save money through reduced internal and external audit costs.

There are also internal benefits. Operating best practice policies and processes that are externally audited will generate internal confidence, improving morale and increasing staff retention. External certification will reduce cyber insurance costs, in the same way that business continuity reduces insurance costs in the event of a disaster. However, done badly, compliance frameworks can inhibit agility. They should be constantly reviewed to ensure that they meet changing organisational needs.

Key takeaways

- Governance and compliance enable an organisation to incorporate risk management into both corporate values and behaviours and operational functions
- Implementing effective governance and compliance requires board investment and ongoing commitment
- Good compliance can increase credibility and reassure customers, thus supporting sales
- Increased compliance can open new markets
- Defining clear processes and areas of responsibility and training staff appropriately will increase productivity, reduce costly mistakes and increase accountability.

03 Developing effective compliance

There are three types of compliance:

1. Standards, or external compliance

Mandatory regulations and standards that organisations have to comply with to effectively operate their business, such as PSN, PCI, HSCN, ISO27001 and Cyber Essentials Plus.

2. Organisational compliance

Internal compliance to corporate standards, business objectives and business values. It can be defined as 'here's a list of the things we do as an organisation and the proof that we actually do them'.

3. Supplier compliance

Supplier compliance i.e. trust in the supply chain.

3.1 Making the business case: how good governance and compliance increase credibility

Compliance to external standards ensures that an organisation has implemented what is universally seen to be best practice. It can enable processes to be simplified and, if audited regularly, is likely to be more enforceable and applied more consistently. However, while these external standards provide a basic framework, the policies and processes that support them must be streamlined and tailored to the organisation's specific needs and strategic direction to extract value (point 2).

It is important to be aware that achieving and maintaining industry standards is a costly undertaking. Once an organisation has met the standard, its customers will expect this to be maintained, which will require regular audits and updates, with all the associated costs.

However, achieving specific standards may open new business opportunities and hence revenue streams. For example, Cyber Essentials is increasingly required when pitching for public sector contracts, but the base Cyber Essentials assessment is self-certified. Certification to Cyber Essentials Plus, which is externally audited by approved assessors, provides independent assurance and gives certification customers can rely on.

Implementing a system to comply with one standard or regulation will also create interfaces to other standards. For example, if the organisation has to create an access control policy for Cyber Essentials Plus, this could be written and implemented in a way that conforms to ISO27001 in case this standard is required in the future. Similarly, when creating an incident management policy for compliance with ISO20000, it would be useful include workflows to manage security incidents that align with ISO27001.

An approach that well-managed organisations have used to streamline governance and compliance is to consolidate security, quality, environmental and service management systems (ISO27000, ISO9001, ISO14001, and ISO20000). This means that they now, in certain areas, have single policies to manage instead of multiple policies across different systems. A streamlined environment with no or minimal non-conformance means less spend on remediation.

03

Key takeaways

- The organisation's Risk Appetite needs to be reflected in tailored management systems which align with corporate strategy and goals
- These systems should be aligned with industry standards to comply with best practice
- Consolidating systems simplifies management and hence reduces costs.

3.2 Extend compliance to customers and the supply chain

Governance, risk and compliance need to extend beyond an organisation's stakeholders to both its customers and its increasingly complex supply chain. Compliance can be used to increase customer trust by bringing them into the compliance regime and encouraging their tailored adoption. However, it is important to ensure that trust can be validated. This means working with customers to understand their business and providing additional, add-on solutions to support the new digital landscape.

Aligning an organisation with its customers with an environment of mutual trust and understanding creates an open and trusted relationship that shares the risk. The behaviour of an organisation's suppliers can have a critical impact on its customers, and it needs to work closely with its major technology suppliers so that together they can design long term security and stewardship of its strategic assets. It is vital to ensure that all suppliers in an organisation's supply chain, including cloud providers, align with its risk standing. Security in the supply chain is only as strong as its weakest link.

Suppliers should be categorised depending on the organisation's reliance on them, with critical suppliers having, at a minimum, the same security governance and compliance. The result should be a cost-effective partnership on agreed standards and the joint operation of governance, risk and compliance. For example, a large IT supplier will typically have a long and well-established compliance process which is extremely secure but comes at a high cost. An SME will be more agile and can potentially use its technical expertise on the specific area of work to reach the same goal more quickly. The buyer has to assess whether the resulting risk is acceptableand find the right balance between risk and restriction, which is where it obtains the best value services.

This does not mean SMEs should reduce their governance and compliance standards. However, they can adapt more easily to the scope of governance to work in a tailored way with each supplier. Both parties need to agree on how they grade each risk so that the right amount of resources are assigned, and then audit the process to ensure governance. The result should provide the best value for the buyer.

Key takeaways

- Extending compliance to customers and suppliers will increase trust – provided you can validate it.
- It should be tailored to each supplier, depending on their importance, to obtain the best value.

03

3.3 Implement processes for addressing changing regulations

The recent implementation of GDPR forced organisations to think more widely about the implications of their business processes and to understand that they need to have controls in place to ensure that not only are they acting correctly, in line with regulations, industry standards and best practice, but they can prove that they are doing so.

It could of course be argued that these should have been best practice anyway! While this is primarily a legal issue, much of the burden of compliance is likely to fall on the IT department. Now that GDPR has been implemented, the way organisations use data is rapidly evolving and changing. Now, they have the capability to gather even more data, which makes GDPR a moving target for organisations to manage.

A key lesson from GDPR is that regulations do not stand still but are frequently changing. For example, just because GDPR policies are now in place, organisations cannot sit back and put a tick in the compliance box for handling Personally Identifiable Information (PII). Data management will change as organisations change, along with their ever-expanding range of customers and suppliers. Similarly, technology and cyber threats do not stand still, nor does company strategy, so governance, risk and compliance need to keep pace.

To address this, organisations should have processes and procedures in place for understanding existing regulations, translating them into policy and practice, and for ensuring constant adherence to those regulations. They also require a process for capturing new regulations well in advance in order to incorporate them into their existing governance. Additionally, organisations need to ensure that they fully understand their specific operating landscape in respect of assets, threats and vulnerabilities, from changes in government policy to cyber security risks, and ensure that these are addressed in their compliance policies and processes.

Key takeaways

- Implement processes to capture changing regulations so they can quickly be incorporated into policy and practice.

3.4 Ensure policies are understood and followed through training

Strong governance, supported by appropriate training to ensure policies are understood and followed, will ensure that everyone in the organisation understands their roles and responsibilities, cementing accountability and improving productivity.

This means ensuring it is included in employee job roles as a core activity, not a series of tasks that are carried out when needed to show compliance, without any focus on their real value to the organisation. All staff should be trained so that they are fully aware of their responsibilities, the threats that exist and the importance of complying with the correct processes to reduce risks. This means putting place cyber security training and awareness, with acceptable use policies that are linked to HR policies.

Key takeaways

- Implement training to ensure staff understand the importance of governance and their own responsibilities.

04 Practical tips for mitigating information security risk

While implementing effective risk management supported by appropriate governance and compliance is a strategic activity that requires considerable time, effort and resource, there are several tactical steps organisations can implement immediately to mitigate information security risk.

1. Ensure your IT security policies address the identified risks

Whilst it should be obvious, we have audited several organisations where the stated policies of the organisation did not address the most likely or highest impact risks. In our view, this can either be because of infrequent review, updating and communication of policies or due to poor co-ordination between teams responsible, where risk analysis, policy management and compliance are seen as separate functions that are not coordinated.

2. Implement suitable policy enforcement and monitoring capability

Another issue we have seen, thankfully less frequently recently, is where there are stated policies in place but we can find no capability to implement and enforce the policy or report adherence to it.

3. Manage access to company resources

IT teams should incorporate data protection into system design. The mapping and storage of personal data needs to be considered carefully, in the light of GDPR, and zero trust (see point 4 below) can be built into systems in such a way as to restrict or prevent any data loss.

It is vital to securely manage access to company resources from mobile and other devices, especially where staff are permitted to use personal devices (i.e. BYOD, BYOT and the IoT).

Multi-factor authentication should be implemented, along with mobile device management (MDM), Mobile Application Management (MAM) and Mobile Identity Management (MIM) where data security is important.

4. Implement least trust access management

Access management – the aligning of rights and privileges – is an area that requires continual monitoring. Many organisations have in the past been too lax in handing out administrator access. A more effective solution is to assign all users the least privilege access rights to individual systems, with clear processes to elevate rights on approval.

Implementing this – termed zero trust or restricted trust – begins with a full understanding of access management and the aligning of rights, privileges and behavioural patterns that are built into policies. It means implementing least privilege and default-deny policies for each user and each system, with clear processes to elevate rights on approval. This restricts unrequired and unwanted lateral movement of traffic between systems and in user access. It should be accompanied by the ability to monitor and log access and failed access (see point 3 above).

5. Be alert for abnormal user behaviour

User management is closely linked to access management. Systems need to be in place to detect and create alerts for abnormal user behaviour, with everyone fully aware of threats and threat vectors. This requires robust cyber security training and awareness and acceptable use policies linked to HR policies. Training needs to be ongoing to ensure all new cyber-threat vectors are understood by users and mitigated. Logging user behaviour in this way will help organisations understand what is 'normal' in their network and for their users. This information can also be used for compliance analytics, which involves gathering and storing relevant data and mining it for patterns, discrepancies, and behavioural abnormalities. Compliance analytics helps companies proactively identify issues and provide appropriate remediation actions.

04

6. Keep up to date with patching

Despite continued high profile issues, many organisations let their patching regime slide. It is important not to simply assume that patching is being carried out but to monitor it effectively. If there is a problem with patching, for whatever reason, the associated risks need to be communicated up the management chain.

Organisations shou ld consider automating patching, using tools which can provide reporting and auditing as well as patching. The time and resources required to set systems up can be quickly repaid by removing constant manual activities. Patching can also be provided by a third party as part of a managed service and is also available through cloud-based services (patching as a service).

7. Review the major incident process

Organisations need to understand their priorities if a breach occurs and what the appropriate actions are to ensure a rapid response. For GDPR, this is set out by the ICO and should already have been incorporated into appropriate policies and processes.

This requires a major incident process for both security breaches and data protection breaches, with inbuilt levels of communication to ensure that users, customers and governing authorities are informed and managed within the required legis lative timescales and with the required scope of information. Should the worst occur, corrective and preventive actions need to be identified and adopted, with continual service improvement embedded to make sure that lessons are learnt and actioned.

Key takeaways

- Implement least trust access management and user management to restrict unrequired traffic and detect abnormal behaviour quickly.
- Monitor the patching regime and consider automation, for which tools may already exist within the organisation.
- Review and update the major incident process.

Summary

The key steps in implementing effective information security risk management are:

- Set out company objectives
- Agree on the level of risk the organisation is willing to tolerate
- Define policies to align with those objectives
- Ensure suitable tools and processes are implemented to measure and report on policy adherence
- Implement streamlined systems to comply with mandatory regulations and legislation
- Tailor these systems with the organisation's corporate policies and align with best practice
- Allow bridges for future compliance to other industry standards
- Set up a governance structure, with auditing, to provide assurance that all policies are being operated and meeting their design goals to achieve company objectives
- Continuously improve
- Bridge to new industry standards when there is a clear business case and the organisation is mature enough to comply and gain advantage
- Market the organisation's compliance to extract maximum value.

Implementing effective governance and compliance to embed effective risk management requires support and buy-in throughout an organisation. It requires a team comprising different levels of capabilities to plan, design, build, operate, monitor, react and improve. Some of these skills may not be available in-house, particularly in SMEs, so it may mean engaging external organisations to supplement internal knowledge. This could include an initial audit to assess the current situation; support for implementing specific systems where the organisation does not have existing in-house expertise and working with experts on specific standards and regulations which the organisation would like to achieve.

Fordway Whitepaper
April 2022

About Fordway

Doing IT differently

We take time to get to know your business, understand your strategy and the context of operations. Our solutions succeed as a result of a relationship founded on strong communication, appreciation and understanding.

Simplifying Complexitiy

We make IT manageable. We resolve your immediate priorities and enable transformation step-by-step at a pace to suit you.

Experience and Expertise

Our consultants solve issues for customers, where others have failed. We pinpoint the root cause quickly and fix the issue so you can move on.

Getting IT right

If it isn't an effective solution for your needs, we won't recommend it and we'll tell you why. It doesn't matter whose logo is on the box.

Bridging the gaps

We'd rather keep you working than hide behind a contract. Our end to-end service ensures nothing falls through the gaps..

Get in touch

For more information
visit: **www.fordway.com**
or call: **08448 700 100**