Defending Your Data

GDPR Readiness for CIOs and IT Managers

INNOVATION™
VALUE
INSTITUTE

As a CIO, one of your most important tasks is ensuring the integrity and security of your company's data.

It's a **serious and bottom-line-critical responsibility**--especially when you consider the legal and regulatory implications of personal data protection.

Most jurisdictions have laws requiring companies to keep customer data safe, secure and private.

The most comprehensive of such laws affecting businesses operating in Europe--the **EU General Data Protection Regulation (GDPR)**--is set to become law at the latest May 25th, 2018. Countries may adopt GDPR into law before this date, making compliance an urgent priority for businesses operating within them.

The consequences for non-compliance with these and other regulations can be disastrous.

Article 83 of GDPR outlines the **fines** for companies that lose or mishandle customer data; in brief, these could amount to up to **€20m or 4% of total global turnover** (whichever is higher) each year.

Clearly, data protection is a growing concern.

As a CIO (or equivalent), you are the executive most directly responsible for data management.

While many day-to-day details of data management are handled by technical staff, often it is **the CIO who ultimately bears the responsibility** for overseeing data policies.

If you implement a strong data policy, heeding regulations and using the most advanced security technologies, you can **save your company from potential revenue loss--as much as 4% of global turnover** under the new EU regulations.

In this report, we will address some of the common fears and concerns surrounding data protection.

- We will introduce you to a framework and assessment system for **evaluating data protection at your company.**
- We will show how you can **complete a full data protection assessment**--covering all relevant departments and locations at your company--in 6-8 weeks.
- Finally, we will show how you can **take the first steps** to improve the data protection situation at your organization today.

With the framework outlined in this report, you will be able to answer pressing questions pertaining to data security at your company. These include:

What processes do I have in place to prevent or limit security breaches?

What costs could my company face for not implementing proper data security procedures?

What is our organization's maturity when acquiring, processing, storing, transmitting, and ultimately destroying data?

Am I vulnerable to a data breach?

How well is my organization currently handling and managing data? And what are the **areas for improvement?**

Can I measure the effectiveness of and adherence to these processes?

How often do I audit these processes, and are they still viable in light of GDPR and other legal guidelines?

Are my people aware of their roles and legal responsibilities under the law, and do I have a process in place to ensure their continual development?

Can I detect a **data breach?**

With the EU GDPR regulations going into effect shortly, there has never been a better time to critically examine data security and privacy at your company.

Not only will it **protect you from the consequences of non-compliance,** it will also create **a number of direct benefits** for your company--not the least of which being greater efficiency in handling and managing data.

In the end, the result can be **significant.** We'll show how you can understand and improve your company's data protection gains for your organization.

First, let's take a broad look at the subject--and why it matters to you and your company.

Why prioritise EU GDPR Readiness?

EU GDPR is set to become law by May 25th 2018 making compliance an urgent priority for organizations

There is an **extensive body of law** governing how companies handle such data.

Personal data includes any factual information pertaining to an identifiable person; for example, **demographic data, health statistics, and financial information.**

Non-compliance with these laws can result in **fines and other penalties.**

Personal data protection is a **major concern** for virtually all companies that handle consumer data.

.

Further, poor data management can result in **security breaches**--in extreme cases resulting in theft and direct revenue loss.

If knowledge of data loss becomes public, it can become a **major brand and reputation liability.**

Let’s look at a few of these concerns in more detail.

Compliance – it’s the law

*You are **legally required to follow data security** best practices in many countries--and throughout the EU when new regulations come into effect starting May 25, 2018.*

Most OECD nations have data security regulations of some form. The U.S., for instance, has regulations like the the Health Insurance Portability and Accountability Act (HIPAA), the Children's Online Privacy Protection Act (COPPA), and the Fair and Accurate Credit Transactions Act (FACTA).

Security breaches

*Fines and penalties resulting from non-compliance are just one potential consequence of neglecting data management. There’s also the threat of lost revenue from cybercrime, which **costs businesses upwards of $500 billion annually.***

Legal consequences for non-compliance.

*There are **severe penalties** for companies and officers found not complying with data security regulations. Most noteworthy are the new EU regulations, which can charge up to €20 million or 4% of a company’s global turnover for non-compliance.*

Potential for damage to your brand and reputation.

*Finally, being exposed to a data breach can harm your company's reputation. This can result in **lost revenue through fewer leads**, lower engagement with existing customers and, as mentioned above, even customer attrition.*

Clearly, data protection is a major concern for any company or organization.

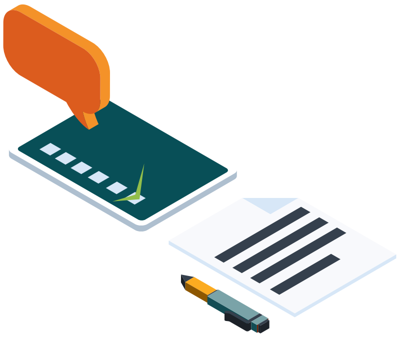
Having robust data protection measures in place **can protect you from legal action, cyber crime, and brand/reputation damage**. Unfortunately, the majority of companies do not have adequate data protection measures in place.

The good news is, **with the right framework and assessment tools, you can ensure that your company keeps apace of the changing data security landscape.**

The GDPR Readiness Assessment:

What it does, and how it benefits your business

Developed by IVI, the GDPR Readiness Assessment is a comprehensive evaluation of your company's data protection. It provides a comprehensive look at:



where you stand with data protection & actionable recommendations to improve your security.

The GDPR Readiness Assessment consists of team meetings, online surveys, interviews and data analysis procedures. By the end, you'll have a clear picture of **what your data protection needs are, how to set targets, and how to move toward them.**

The GDPR Readiness Assessment provides a **high-level comprehensive view of current and target state with respect to data**, at every level of your organization. It examines how data is handled, where it is stored, the policies used to manage it, and more.

The GDPR Readiness Assessment focuses on **Capability as well as Compliance.** The focus on compliance helps identify predictable risks, as well as business processes that can mitigate or eliminate them--satisfying or even exceeding today's legislative requirements.

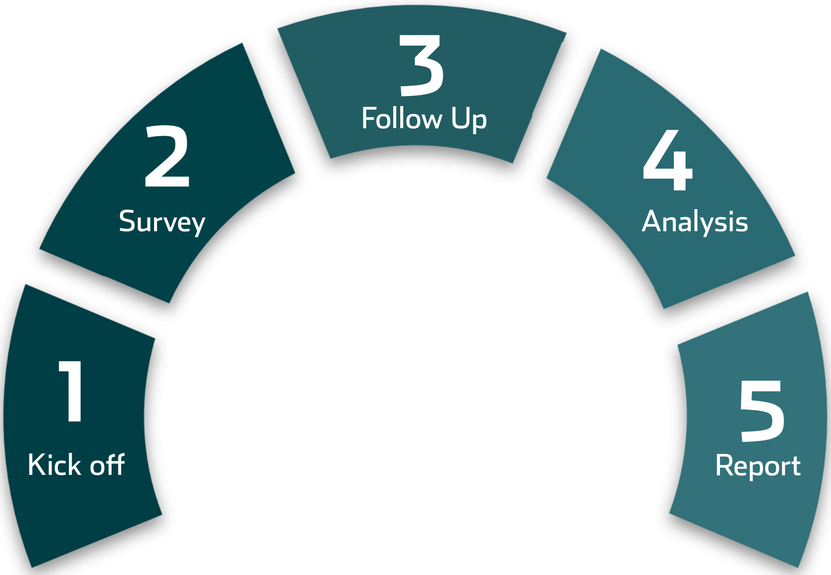
The focus on compliance helps with:

- Anticipating and responding properly to future events
- Measuring adherence to processes
- Audits
- Process improvements
- Limiting and reversing damage when it does occur.

What The Assessment Includes:

The GDPR Readiness Assessment consists of team meetings, online surveys, interviews and data analysis procedures, designed to give you a clear picture of your company's data protection needs.

The assessment includes 5 phases.



1. Survey kick-off meeting. In this phase, your managers and staff are coached on how to complete the survey.

2. The online survey After receiving initial coaching, participants answer questions pertaining to the company's data security and procedures. This will provide valuable feedback to the CIO and IT team.

3. Follow-up participant interviews. Once surveys are complete, individual participants will be interviewed to validate survey results, providing robust qualitative input that the initial survey may have missed.

4. Analysis of quantitative and qualitative results. After all surveys and interviews are complete, results are interpreted using advanced statistical methods, to yield the most insightful and actionable results.

5. Final report with improvement recommendations. Includes actionable tips that you can start to implement immediately.

The Benefits: to you and your organization

The GDPR Readiness Assessment provides accurate insights across all areas of data security and privacy:

Management and Oversight of Personal Data Protection

- ☑ Strategy and Governance of personal data protection processes
- ☑ Supplier Management
- ☑ Monitoring, Reporting and Enforcement of personal data protection processes

People

- ☑ Stakeholder awareness
- ☑ Data Subject Rights Management
- ☑ Enforcement of roles, responsibilities, and accountabilities

Processing of Personal Data

- ☑ Security, access rights and risk management
- ☑ Personal data acquisition and purpose
- ☑ Compatibility, adequacy and accuracy
- ☑ Information life cycles
- ☑ Data retention and destruction.

More broadly, The GDPR Readiness Assessment delivers significant benefits in terms of your ability to meet regulatory requirements and protect your business from revenue loss.

Specific benefits include:

- EU GDPR readiness. **Help you become fully compliant** before the new laws come into effect May 25th 2018.

- Security threat awareness. **Understand your current data risks**--and how to mitigate or eliminate them.

- Consumer data protection compliance. Find out if you'll be compliant under the new laws.

- Data protection policy consistency. Gain **a crystal-clear understanding** of how your data protection policy is being followed internally, and how it could be improved.

- **Skills preparedness.** Assess your current skills and identify areas for improvement.

- Impeccable **data security processes.**

- **Better resource management.** Gain a better understanding of where limited resources should be allocated, and in what amounts.

- **Robust data integrity.** Assess where you stand now, and how to improve for the future.

- **Better customer data management.** Develop better policies for protecting customer data, and handling data requests.

Powered By The IT-CMF Framework

The GDPR Readiness Assessment is based on the IT Capability Maturity Framework (IT-CMF), a proven methodology for aligning IT and business decisions.

The IT-CMF encompasses 36 management disciplines, from accounting and budgeting to Security and UX design.

Managing IT like a Business

- AA Accounting and Allocation
- BP Business Planning
- BPM Business Process Management
- CFP Capacity Forecasting and Planning
- DSM Demand and Supply Management
- EIM Enterprise Information Management
- GIT Green IT
- IM Innovation Management
- ITG IT Leadership and Governance
- ODP Organization Design and Planning
- RM Risk Management
- SAI Service Analytics and Intelligence
- SRC Sourcing
- SP Strategic Planning

Managing the IT Budget

- BGM Budget Management
- BOP Budget Oversight and Performance Analysis
- FF Funding and Financing
- PPP Portfolio Planning and Prioritization

Managing the IT Capability

- CAM Capability Assessment Management
- EAM Enterprise Architecture Management
- ISM Information Security Management
- KAM Knowledge Asset Management
- PAM People Asset Management
- PDP Personal Data Protection
- PPM Programme and Project Management
- REM Relationship Management
- RDE Research, Development and Engineering
- SRP Service Provisioning
- SD Solutions Delivery
- SUM Supplier Management
- TIM Technical Infrastructure Management
- UED User Experience Design
- UTM User Training Management

Managing IT for Business Value

- BAR Benefits Assessment and Realization
- PM Portfolio Management
- TCO Total Cost of Ownership

IT-CMF forms the basis of all of IVI's assessments, with **proven benefits to CIOs and IT managers** across broad areas like:

- ☑ Individual Critical Capabilities
- ☑ Holistic IT Effectiveness
- ☑ Data Protection
- ☑ Digital Business Readiness.

The core of the IT-CMF framework is **36 critical capabilities, or disciplines that are necessary for comprehensive management of technology across the organization.**

These 36 capabilities span both IT and non-technical disciplines, and are evaluated according to maturity; in other words, how well developed a particular capability is at an organization.

How is data protection impacting your entire organization?

The GDPR Readiness Assessment draws on IT-CMF capabilities to provide a broad look at how data protection is impacting your entire organization.

The assessment is holistic, gauging your data management effectiveness in terms of compliance, security and even marketing.

It is analytical, using advanced statistical methods to provide dependable metrics. And most importantly, it is actionable, providing recommendations for improvement that you can implement quickly.

Want to learn more? Get in touch

If you'd like to learn more about the **GDPR Readiness Assessment**, or just want to learn more about IVI's offerings, we'd love to speak with you.

FIND OUT MORE

Or get in touch with us directly at:

Web: https://ivi.ie | **Email:** info@ivi.nuim.ie | **Phone:** +353 1 708 6931

IVI INNOVATION™
VALUE
INSTITUTE