Progress® | ipswitch®

A PROGRESS PROFESSIONAL GUIDE

The International Data Privacy and Compliance Handbook

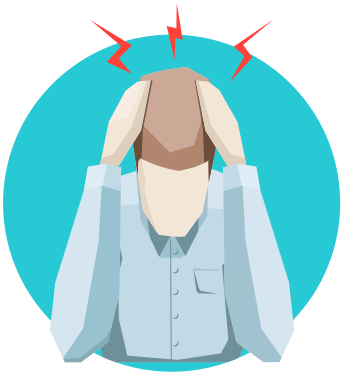
Introduction

We get it, you likely don't have the time to slog through intricate checklists to meet each and every aspect of regulatory compliance, especially considering all the rules and regulations around the world focusing on data privacy.

It seems that today every country has its own compliance standards as

This handbook lists and describes various international standards for data privacy and data protection around the world. Some of these regulations are required by all industries, while other may be more stringent if you work in a regulated industry, like healthcare and finance. This handbook will cover the following:

- International Regulatory Compliance Standards and Legal Requirements
- Preparing for An Audit
- Building an Effective Security Response Team



What's Your Answer?

If you are an IT or security professional ask yourself and your team these questions:

- Is my organization doing everything possible to stay compliant?
- Do our users recognize when they are being phished?
- Do we have a sound plan in place to manage through a data breach?

If you answered "no" or "I don't know" to any of those questions then you're not alone. Most organizations struggle to protect themselves from outside threats. Being compliant and ready for an audit does not mean you are well armed to fend off an attack from a determined hacker or disgruntled employee.

Making sure that your IT infrastructure is routinely patched to protect from the latest vulnerabilities listed is a good start for risk mitigation. We recommend you routinely check out reports from CVSS (Common Vulnerability Scoring System) and Microsoft's "Patch Tuesday" bulletins. Even with this, information security is a perpetual and thankless task. Patches alone can't promise full protection. But it's a start.

It's also important to note which compliance standards effect your business. Depending on where you do business, you may need to make sure that you are compliant with one or maybe even several regulations around the world.

Regulatory Compliance Standards and Legal Requirements

Regulators have long been aware of the risks associated with poorly managed data transfers. Their expectations grow along with the penalties they can impose. Compliance matters everywhere in the world, major corporations and SMBs included. These days, auditors are interpreting standards in more consistent yet more demanding ways, drawing upon a growing set of best practices. Knowing what you will get asked during an audit, before the audit happens, is your best bet.

For instance, many healthcare and financial organizations have their own internal audit teams to prepare for outside auditors. If you are looking to create an internal group, consider staffing with a combination of experienced auditors, legal professionals, and IT managers. (or some possible subset).

At the very least, the internal audit team should have the knowledge and resources available to hold practice audits to identify gaps and potentially weaknesses. They should also know which regulations apply to your business.

General Data Protection Regulation (GDPR)

Companies storing personally identifiable information (PII) must comply with a broad range of existing information security regulations, while newer and more demanding regulations are being introduced in places like the European Union, the United States and China.

The European Commission has unified data protection regulations within the European Union under the General Data Protection Regulation (GDPR). Because GDPR is a regulation rather than a directive, it's immediately applicable to all member states.

If GDPR wasn't enough change to manage, the UK's exit from the EU (aka "Brexit") means businesses moving and storing data in the UK will be responsible for maintaining whatever standards the UK passes, while also complying with the EU's GDPR.

GDPR goes deep, requiring privacy by design, a right to erasure, data breach notification, and data portability when a patient or customer wants a copy of their data, for example medical records. Non-compliance with the GDPR is serious considering penalties can be up to 5% of your company's annual revenue.

Brazil's General Data Protection Law

Inspired by the GDPR, in mid-August of 2018, Brazil passed a new legal framework aimed at governing the use and processing of personal data in Brazil: the General Data Protection Law.

The law replaces approximately 40 or so laws that currently deal with the protection of privacy and personal data, and is aimed at guaranteeing individual rights, and encouraging economic growth by creating clear and transparent rules for data collection.

The Bill was signed into law in mid-August 2018 and is expected to take effect in February 2020.

The new law governs processing of personal data in Brazil, and it takes a broad understanding of data processing in doing so. Basically, if you touch the data of a citizen at all, you are processing it. That includes collecting the data, storing it, and transferring it.

So, if you, or your organization, perform any of these activities in Brazil, then you are subject to the law. With a few small exceptions for national security organizations, artistic, and journalistic pursuits, private and public sector organizations are both equally accountable to the law.

Australia's Federal Privacy Act 1988

Essentially, the Privacy Act 1988 is an Australian federal law that regulates how personal information is handled. Australia considers any data or opinion of an individual that can be traced back to that individual as personal information. A few examples of personally identifiable information (PII) in Australia are email, a signature, or phone number.

There are a total of 13 privacy principles under the Federal Privacy Act 1988 with the sole purpose of making sure businesses are transparent about how they handle and process personal data. If you have already prepared for the GDPR, much of GDPR compliance will apply in Australia. There are a few caveats, but the idea is the same. Citizens have the right to know what a company is doing with their data.

China's Cyber Security Law

China's first comprehensive regulation for digital privacy and security, Cybersecurity Law (CSL) was passed on November 7th, 2016, and first came into effect on June 1st of 2017. Since then, there has been sporadic enforcement of certain sections of the law, while others are being dealt with less consistently.

Whatever the enforcement, the CSL imposes massive new requirements on a broad range of companies, both domestic and foreign, operating in China, and sets major penalties for failure to comply, such as fines or even jail time.

As China's central internet regulator, the Cyberspace Administration of China (CAC) is the main authority tasked with supervising and enforcing the CSL.

In the years since the law was first put in place, the CAC has been primarily focused on the user-content monitoring outlined above.

The CAC has already imposed fines on several large technology companies, including Alibaba Cloud and Taobao, for "failure to implement measures to prevent the dissemination of prohibited information."

Health Insurance Portability and Accountability Act (HIPAA)

Healthcare organizations comply with the Health Insurance Portability and Accountability Act (HIPAA) for a bunch of reasons, like avoiding persecution from the U.S. Federal government or civil lawsuits filed by patients. HIPAA notoriously demands a wide range of administrative, physical and technical safeguards. These include formal procedures, responsibilities, training, contingency plans and internal audits to safeguard electronic protected health information (EPHI). Protected health information (PHI) is any information about health status, provision of health care, or payment for health care that can be linked to a specific individual.

Failure to comply with HIPAA can result in civil fines of up to USD 1.5 Million per year.

PSD2 Directive

The EU's PSD2 directive (a revised payment service directive) aims to regulate electronic payments in EU member countries. It has no impact on traditional paper-based transactions. The aim is to allow open banking, where cross-border transactions are easily performed, cheaper and involving any number of fintech providers (think digital wallets, payment gateways, and online shopping). Any organization engaged in the process, from the banks themselves to payment providers and account information services (credit checks and data processing) must incorporate strict security, transparency and protect users' rights.

ISO/IEC 27001/2

Organizations are increasingly taking a closer look at the ISO/IEC 27001 international standard, widely recognized across all government and business sectors.

Section A.13.2 of ISO/IEC 27001 is dedicated to the subject of information transfer, with a stated objective of maintaining the security of data transferred within an organization and/or outside with external parties.

This standard is a best practice rather than a specification, and can be interpreted to suit the specific needs and risk environment of each business. Underpinning this interpretation however is a requirement to reference the more comprehensive companion standard ISO/IEC 27002.

ISO 20022

Many years since the initial publication of ISO 20022, more and more financial firms are beginning to leverage the standard. For instance, SWIFT—the global member-owned cooperative and a leading provider of secure financial messaging services—recently announced the creation of a common end-to-end implementation to increase the move of cross-border transactions to the ISO 20022 standard.

SWIFT hopes to increase efficiencies, support straight-through-processing, facilitate improved regulatory compliance, improve the party-identification process, and provide the opportunity for financial institutions to conduct new business. According to SWIFT, the move to ISO 20022 is being driven by the payments community and will require engagement and dialogue between SWIFT users on a

regular basis. SWIFT said it will invite the community to review and comment on the guidelines as they are crafted.

ISO 20022 focuses on international, cross-border communications among financial institutions, clients, and market infrastructures involved in the processing of financial transactions. There is, however, a strong opportunity to also use ISO 20022 for the development of new domestic financial messages, which will streamline all communications for financial institutions.

The standard can be used across various business domains, communication networks, and the infrastructures of financial institutions, clients and suppliers. This flexibility provides many benefits for financial institutions to improve transaction efficiency while reducing costs and exposure to risk:

- Creates a common language for financial business process communications.
- Facilitates interoperability with other protocols.
- Generates financial messaging standard encompassing complete transaction sequences.
- Includes a complete selection of data sets and messages for investment funds.
- Provides support for non-Latin alphabets.
- Offers improved remittance and permitting for extensions.
- Harmonizes formats not previously allowed for cross-operation.

Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) is an international mandatory compliance requirement for all organizations processing, storing, transmitting, or accessing cardholder information for any of the major payment card brands.

The PCI DSS demands very strict security controls to be applied to protect cardholder information, including the establishment of a secure Cardholder Data Environment (CDE). The standard is enforced contractually through frequent audits and tests by approved security consultancies and vendors.

If your organization stores financial data like a credit card number, you need to be PCI compliant.

MiFID II

Issued by the European Union, MiFID II is an updated version of the Markets in Financial Instruments Directive, which went into effect in 2007. MiFID II broadens the scope of MiFID to include increased transparency at every stage of a transaction—from when orders are first placed until they are reconciled. Every trade must be closely monitored at every phase.

One key area of MiFID II on which IT and compliance teams need to focus is automated trading. Algorithms must be registered, tested and have circuit breakers. Brokers also have to provide more detailed reporting on their trades, including price and volume information, and they need to store all communications—including phone conversations.

Another key area is data management. Here's a quick rundown of what IT should zero in on:

- Ensure data feeds support micro-second time-stamping.
- Source pre- and post-trade data only from systematic internalizers, approved publication arrangements, and trading venues.
- Set alerts to determine if systematic internalizer thresholds are breached
- Publish all asset classes.
- Report transactions by the close of the following business day.
- Document who distributes financial products.
- List transaction fees and research charges separately
- Apply benchmarking to best-execution and transaction-cost analysis

Financial firms must also be able to compile data from multiple systems and transform the data into a coherent format that clearly depicts the entire journey of each transaction at any step in its process.

Given the data management requirements of MiFID II, IT teams will have to build and integrate new functions with their IT systems. This is particularly challenging in environments where technology solutions have been developed independently and have changed frequently on top of legacy infrastructures.

Sarbanes-Oxley Act (SOX)

In a post-Enron world, transparency is key for businesses in the finance sector, but moving parts are plentiful. An important aspect of regulatory compliance, such as Sarbanes-Oxley (SOX) is knowing where your critical business data is at all times: at rest and in transit.

In a fictitious example of insider trading, say a rogue employee sends earnings data showing negative profitability to a friend on Wall Street two days before the earnings call. What controls does your IT team have in place to identify and mitigate security risks like this? How do you implement these controls without creating bottlenecks that become a manual labor time suck?

Companies that report to the Securities and Exchange Commission (SEC) must comply with the Sarbanes-Oxley Act (SOX). The legislation is intended to protect investors by improving the accuracy and reliability of corporate disclosures. The Act makes the CEO and CFO personally responsible for assessing the effectiveness of internal controls governing financial reporting.

The consequences for non-compliance can be steep fines and imprisonment. This assessment must be reviewed by an independent auditing firm. Although there is no prescribed list of controls, the security and integrity of financial reporting systems is an essential component of a SOX assessment. This encompasses all controls that ensure that applications function correctly. There are similar laws in many other countries, including Australia, Canada, France, Germany, Italy, Netherlands, South Africa, Turkey, and Japan.

Basel II and III

The Basel Framework is the international framework for banking and financial institutions. Amongst other things it requires banks to mitigate operational risks, such as fraud, system failure and unauthorized intrusions, and to establish formal information management policies, procedures and controls.

Basel III introduces enhanced evaluation and measurement of risk, as well as updated rules on corporate governance and reporting standards.

Penalties for non-compliance can include fines of up to 10% of turnover and withdrawal of the banking license.

Preparing for an Audit

The best way to become and remain prepared for an audit is a full-on dress rehearsal. You might want to conduct your own internal audit through a certified auditor. This will help IT teams to become fully prepared as it reveals issues that need resolving. Internal audits are typically managed by members of a compliance team, including executives like your Chief Compliance Officer (CCO), Chief Security Officer (CSO), or even your CEO if it's a small businesses. Your compliance and security officers are often the gatekeepers for all documentation that proves your company's earnest efforts to meet compliance.

What's important to note is that in all cases of an audit, a member of the IT team will need to be present to answer any questions. This is why it is crucial to hire an internal auditor to check to see that IT has all its tracks covered before a real audit takes place. You may even want to hire a third party vendor to audit your business.

Become Ready for Anything with a Security Response Team

As regulations become more dense, data security can't be the sole responsibility of a single individual person or team. Multiple areas of the business have a stake in meeting compliance. Composing a security response team of designated compliance, security and technology practitioners including managers from all departments is a good practice. This team composition will be the most qualified to help educate users to avoid being the source of a data breach.

A WHO'S WHO LIST FOR SECURITY RESPONSE

Here is a list of people within your own organization who you should consider to take part in the formation of a security response team:

Everyone in the C-suite

All executives should be part of a security response team. A security response process can often be carved out of an existing crisis communications document. And if anyone is going to get prosecuted, it's likely it'll be your CEO. Most senior executives are highly sought after spearphishing targets. Simply put, becoming prepared should start from the top down.

The IT Team

No surprise here that this group is very computer literate and needs to be on top of all the latest online attacks and vulnerabilities. As mentioned before, staying current with reports like CSVV, along with end user security training to teach them how to recognize social engineering tactics.

Pick someone on your IT team who knows how to communicate effectively with those who are far less technical. Have that person provide a crisp and accurate representation of policy, procedures, and decisions. Much like the CEO, the CIO could be in the hot seat if there are ever legal ramifications due to a data breach.

Compliance and Security Officers

Your CCO or CSO is responsible for creating all company protocols relating to regulatory compliance. This puts them on the security response team whether or not it's what they'd chosen. They also are the gatekeepers of documentation that proves that your business has done everything necessary to stay compliant even if cybercriminals get inside your network.

Product

If you are a B2B, you most likely have a product team since you are selling products/services. The product team will have hands on experience with the technology used within an organization. Product and IT should partner up when an issue arises considering today's DevOps culture. Depending on the source of a breach or compliance point of failure, either IT or the product teams will most likely be implementing a fix.

Marketing

Every security response team needs to have a seasoned corporate communications person on it. These PR experts are professional corporate crisis managers and need to control any information flow to the outside world. Many standards including HIPAA require a company that has suffered a data breach announce it via a press release if more than 500 people are affected. Smaller breaches will at the very least require some kind of notification to those affected by it.

Security and Compliance is Everyone's Responsibility

Every individual on a security response team should understand their role and responsibilities as it pertains to any given standard. Your business should have a plan in place for when an audit takes place or in the unfortunate event of a data breach.

Knowing how to respond quickly and effectively can make a world of difference on your company's balance sheet. This is why twice-yearly internal audits and practice drills are critical. Preparation is absolutely critical. There's simply no time to learn-as-you-go after you've been breached.

About Progress

Progress NASDAQ: PRGS) offers the leading platform for developing and deploying strategic business applications. We enable customers and partners to deliver modern, high-impact digital experiences with a fraction of the effort, time and cost. Progress offers powerful tools for easily building adaptive user experiences across any type of device or touchpoint, award-winning machine learning that enables cognitive capabilities to be a part of any application, the flexibility of a serverless cloud to deploy modern apps, business rules, web content management, plus leading data connectivity technology. Over 1,700 independent software vendors, 100,000 enterprise customers, and 2 million developers rely on Progress to power their applications.

Learn about Progress at www.progress.com or +1-800-477-6473.

Progress® MOVEit®

Download your FREE TRIAL of MOVEit ›

RITM0047162