GOVERNANCE

ENFORCING DATA PRIVACY IN THE DIGITAL WORLD

CONTENTS

4 **Privacy and Security Controls in the Data Life Cycle**
5 **Evolution of Global Data Privacy Laws**
6 **Top Data Compliance Challenges and Solutions**
8 **Impact of Incorrect and/or Missing Data Privacy Controls**
9 **Building a Strong Data Governance Program**
9 / Build Your Team
10 / Identify Specific Threats and Controls
10 / Continually Assess Effectiveness of Existing Controls
11 **Managing Enterprise Data Life Cycle Compliance Needs**
11 / Perform Asset Inventory
11 / Identify Key Risks
11 / Perform an Impact Analysis
12 / Monitor Regulations
12 / Compare GRC or Commercial-Off-the-shelf Solutions
13 **How Enterprises Can Improve Privacy Risk**
13 / Case Study 1
14 / Case Study 2
14 **Conclusion**
15 **Acknowledgments**

© 2019 ISACA. All Rights Reserved.

ABSTRACT

Emerging technologies such as robotic process automation, Internet of Things (IoT) and artificial intelligence (AI) are increasing the sources of personal data available to enterprises. This, in turn, is increasing data protection risk to enterprises.

While enterprises try to reduce this risk, they are also faced with evolving laws and regulations. Designed to protect data privacy, these laws and regulations affect enterprises globally and present numerous data privacy and compliance challenges.

Building a strong regulatory data governance and protection model is essential for compliance. This white paper provides you with solutions to some of the top enterprise data privacy compliance challenges. You will gain a stronger understanding of:

- The impact of privacy regulations throughout the data system
- The impact of an enterprise failing to implement regulatory data privacy controls
- The adoption of frameworks and standards to help your enterprise stay in regulatory compliance
- The automation of privacy law monitoring and compliance reporting to help address the governance, risk and compliance (GRC) needs of your enterprise

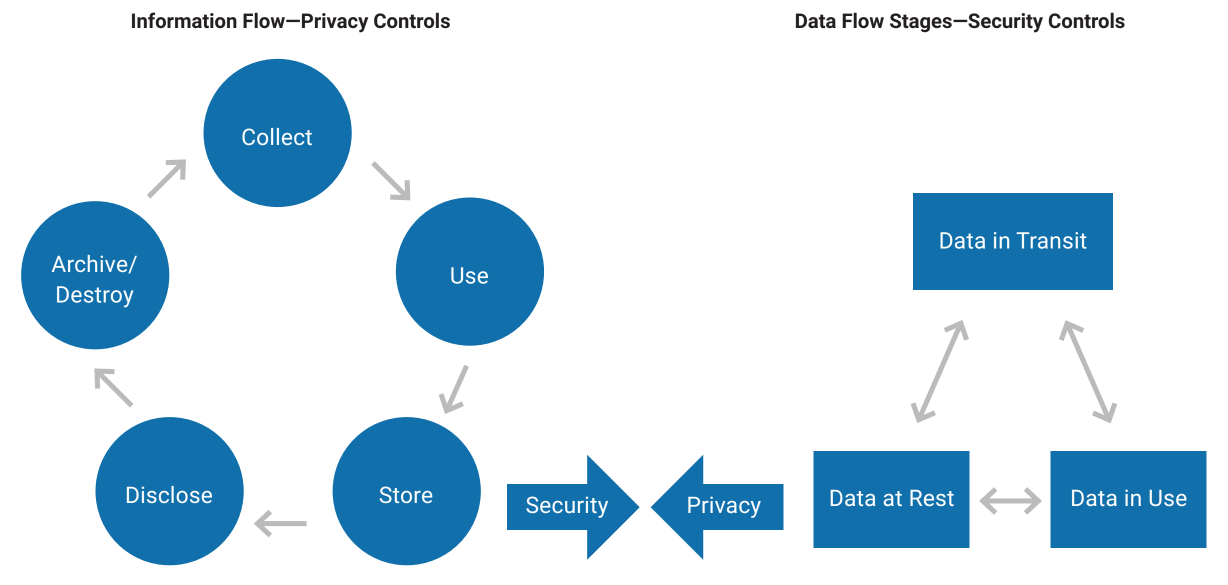
© 2019 ISACA. All Rights Reserved.

Privacy and Security Controls in the Data Life Cycle

Emerging technologies, such as robotic process automation, the Internet of Things (IoT), artificial intelligence (AI) and machine and deep learning, introduce more ways for sensitive information to be collected, used, stored, disclosed and destroyed, and increase data privacy risk. Data privacy laws are designed to protect sensitive customer data collected through these means.

A comprehensive data analysis is a critical step in assessing privacy risk. **Figure 1** shows the information flow, which is where privacy controls are applied, and the data flow stages, which is where security controls are applied. Privacy and security controls should coexist for effective data protection.

FIGURE 1: Information Flow and Data Flow Stages in the Data Life Cycle



As information flows through the data life cycle (**figure 1**), privacy and security controls must be reevaluated constantly because technological advancements continue to introduce more data protection risk to enterprises.

Enterprises in every industry process millions of transactions and handle massive amounts of data every second. Each transaction, which is likely to involve some personal data, increases the risk for data corruption, error or leakage. Numerous laws and regulations, which are being enacted across the globe, require enterprises to reduce the risk to data privacy. Enterprise privacy compliance efforts must address all applicable privacy laws/regulations. Privacy risk reduction requires that enterprises implement a comprehensive regulatory data privacy compliance program.

© 2019 ISACA. All Rights Reserved.

Evolution of Global Data Privacy Laws

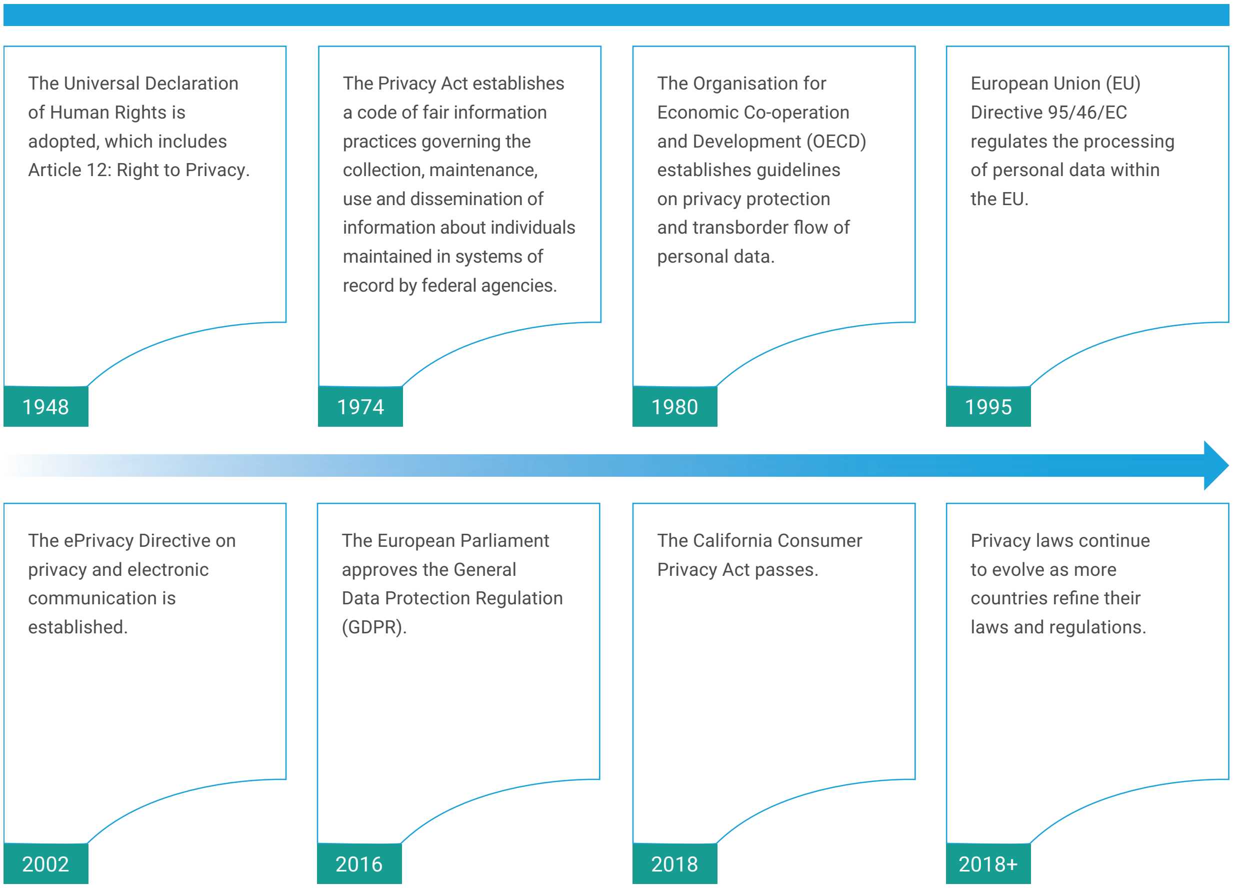
Data privacy laws originated at the country level more than a century ago and propagated worldwide. Global privacy laws now exist in many forms and vary by country and region. A data privacy law can be categorized as one of the following types, depending on its scope:

- Sectoral or industry-specific law
- Comprehensive law
- Co-regulatory, federal, state or local country law

Figure 2 shows that lawmakers have been creating and amending laws for decades.[1] When technological advancements were introduced, laws were either created or updated to address new weaknesses and vulnerabilities in information handling. Technological advancements create various challenges and vulnerabilities within enterprises that can result in minor or major data breaches, affecting increasing numbers of individuals. The European Union General Data Protection Regulation (GDPR) is a recent privacy regulation that has a major global impact on enterprises and their data protection policies and practices.[2]

It is critical for enterprises to understand the challenges created by the evolving data privacy landscape and to implement effective solutions.

FIGURE 2: The Evolution of Key Privacy Laws



1948 — The Universal Declaration of Human Rights is adopted, which includes Article 12: Right to Privacy.

1974 — The Privacy Act establishes a code of fair information practices governing the collection, maintenance, use and dissemination of information about individuals maintained in systems of record by federal agencies.

1980 — The Organisation for Economic Co-operation and Development (OECD) establishes guidelines on privacy protection and transborder flow of personal data.

1995 — European Union (EU) Directive 95/46/EC regulates the processing of personal data within the EU.

2002 — The ePrivacy Directive on privacy and electronic communication is established.

2016 — The European Parliament approves the General Data Protection Regulation (GDPR).

2018 — The California Consumer Privacy Act passes.

2018+ — Privacy laws continue to evolve as more countries refine their laws and regulations.

[1] Many resources are available to learn about the evolution of data privacy. See, for example, International Association of Privacy Professionals, Inc., "Decode the GDPR's DPIA Requirements," www.iapp.org.

[2] European Commission, "2018 reform of EU data protection rules," https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

© 2019 ISACA. All Rights Reserved.

Top Data Compliance Challenges and Solutions

The continuous evolution and refinement of data privacy laws can create serious challenges for enterprises. Some key challenges are:

- Ongoing changes to data privacy laws in the jurisdictions in which the enterprise operates or houses customer personal data
- Requirements to conduct and show proper due diligence when adopting new technological advancements to better serve customers
- The need to continuously monitor and audit controls to ensure they work effectively according to accepted standards

Whether all of these challenges apply to an enterprise across countries and/or across industries depends on the enterprise's risk exposure to threats posed by external or internal groups or individuals. The risk exposures that enterprises encounter now and into the future are addressed in "The Global Risks Report 2018,"[3] published by The World Economic Forum.

The report defines global risk as, "an uncertain event or condition that, if it occurs, can cause significant negative impact for several countries or industries within the next 10 years."[4] The report also emphasizes the importance of analyzing various risk conditions (e.g., economic, environmental and geopolitical).

Failure to assess technological risk is more likely to have an adverse impact on information privacy, specifically:

- Adverse consequences, intended or unintended, of technological advances such as artificial intelligence, geoengineering, and synthetic biology, causing human, environmental and economic damage
- Increasing vulnerability to the outage of a critical information infrastructure (e.g., Internet and satellites) and networks, causing widespread disruption
- Large-scale cyberattacks causing extensive economic damage, geopolitical tensions or widespread loss of trust in the Internet
- Massive incident of data fraud/ theft, resulting in exploitation of private or official data that takes place on an unprecedented scale[5]

These challenges and the associated technological risk can be addressed using various frameworks and standards, ranging from generic templates that provide blanket coverage, to very specific point solutions per individual data privacy law.

Organizations such as ISACA, the International Organization for Standardization (ISO) and the Payment Card Industry (PCI) Security Standards Council maintain these frameworks and standards. These organizations are constantly researching, evaluating and reacting to changes made by data privacy regulators, to understand the exact impact and determine the updates that are needed.

A few examples of responses from these organizations to the evolving regulatory landscape include:

- ISACA *Data Protection Impact Assessment*,[6] which highlighted the changes that enterprises could expect with GDPR.
- PCI *Data Security Standard (DSS)* version 3.2.1,[7] which added requirements to migrate from Secure Sockets Layer (SSL) to Transport Layer Security (TLS) higher version, and from two-factor to multi-factor authentication to better protect regulatory data.
- PCI *Data Security Standard (DSS)* version 3.2.1 also introduced sub-requirement 11.3.4.1, which contains additional compliance

[3] World Economic Forum, "The Global Risks Report 2018," 13th Edition, http://wef.ch/risks2018

[4] *Ibid.*

[5] *Ibid.*

[6] ISACA, *GDPR Data Protection Impact Assessments*, September 2017, http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/GDPR-Data-Protection-Impact-Assessments.aspx

[7] PCI Security Standards, "PCI Data Security Standard (PCI DSS)", www.pcisecuritystandards.org

© 2019 ISACA. All Rights Reserved.

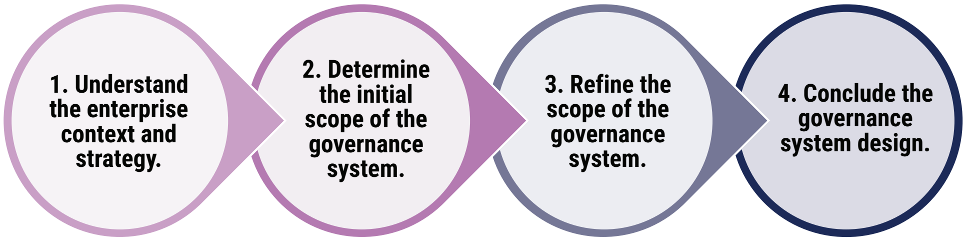
requirements for service providers only. It dictates penetration testing when segmentation is used, to confirm PCI DSS at least every six months and/or after any changes to segmentation controls/methods. PCI DSS not only applies to all entities involved in payment card processing, but also applies to all other entities that store, process or transmit cardholder data and/or sensitive authentication data. Penetration testing is a very useful tool to determine weaknesses in the critical information infrastructure and networks of any entity processing customer personal information and sensitive data.[8]

To address these new challenges, standards organizations and various industries are joining forces to interpret the data privacy laws, and reformulate and adapt existing frameworks and standards.

To effectively address the challenges associated with evolving data privacy laws, new technological advancements, and continuous monitoring, an enterprise should:

- Assess the latest versions of frameworks, standards and industry best practices.
- Implement a strong governance framework. The *COBIT 2019 Design Guide*[9] proposes a flow for designing a tailored governance system (see **figure 3**).
- Deploy the right software tools to identify the usage of general and sensitive personally identifiable information (PII) handled during each stage of the data life cycle.
- Obtain the latest information on new and critical vulnerabilities on various frequencies (daily, weekly and monthly) from objective sources, such as US Computer Emergency Readiness Team (US-CERT)[10] or the Computer Emergency Response Team (CERT-EU) for the EU institutions, bodies and agencies.[11]
- Establish and update an adequate internal controls framework that considers data privacy and its related controls, and includes continuous monitoring and auditing of controls surrounding the data life cycle.

FIGURE 3: Governance System Design Workflow


1. Understand the enterprise context and strategy.
2. Determine the initial scope of the governance system.
3. Refine the scope of the governance system.
4. Conclude the governance system design.

- 1.1 Understand enterprise strategy.
- 1.2 Understand enterprise goals.
- 1.3 Understand the risk profile.
- 1.4 Understand current I&T-related issues.

- 2.1 Consider enterprise strategy.
- 2.2 Consider enterprise goals and apply the COBIT goals cascade.
- 2.3 Consider the risk profile of the enterprise.
- 2.4 Consider current I&T-related issues.

- 3.1 Consider the threat landscape.
- 3.2 Consider compliance requirements.
- 3.3 Consider the role of IT.
- 3.4 Consider the sourcing model.
- 3.5 Consider IT implementation methods.
- 3.6 Consider the IT adoption strategy.
- 3.7 Consider enterprise size.

- 4.1 Resolve inherent priority conflicts.
- 4.2 Conclude the governance system design.

Source: ISACA, *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*, USA, 2018, www.isaca.org/COBIT/Pages/COBIT-2019-Design-Guide.aspx

Addressing these challenges may not be part of an enterprise's core business, but it is vital to protect the enterprise's critical resources and to achieve compliance or remain compliant. Addressing these challenges also provides the added benefit of gaining or maintaining customers' confidence and trust that their information is

[8] *Ibid.*

[9] ISACA, *COBIT® 2019 Design Guide*, USA, 2018, http://www.isaca.org/COBIT/Pages/COBIT-2019-Design-Guide.aspx

[10] US-CERT, United States Computer Emergency Readiness Team, www.us-cert.gov

[11] CERT-EU, Computer Emergency Response Team for the EU Institutions, bodies and agencies, https://cert.europa.eu/

© 2019 ISACA. All Rights Reserved.

well protected. These functions can be managed by using GRC software that can support the requirements of evolving data privacy laws, new technological advancements and continuous monitoring.[12]

GRC software can change the way an enterprise works by streamlining processes and tasks. Some of the steps to achieve IT audit readiness are:[13]

- Identify, assess and classify IT risk
- Identify controls
- Map controls to a master framework library
- Plan, scope and stress test micro risk with controls
- Assess effectiveness of existing controls
- Capture, track and report deficiencies
- Monitor and automate tests of controls
- Flag exceptions, review, investigate and remediate
- Conduct ongoing improvement of control and monitoring processes
- Perform predictive IT risk trending
- Integrate IT risk management processes into overall enterprise risk management

Data governance must be viewed as the responsibility of everyone in the enterprise. It requires an understanding of how the data is collected, maintained and interpreted, what users are doing with the data and why the data is important and valuable. Successful data governance may require a broad transformation of the enterprise and culture. Software tools can help support the transformation of impacted processes and the mindset of the people supporting those processes.[14]

Because there are many GRC software vendors in the market, it is important to conduct a thorough feasibility study that maps the enterprise GRC requirements with the software solution.

Impact of Incorrect and/or Missing Data Privacy Controls

Although many enterprises focus on data privacy from a compliance standpoint, data breaches can also cause irreparable monetary and reputational damage. A data breach is a significant threat that can disrupt operations as the enterprise scrambles to perform damage control, and it can result in lost business opportunities, productivity and customer trust. Additionally, penalties, compensation and refunds from a data breach can ultimately impact the bottom line.

Recently, a group of Iranian hackers infiltrated nearly 140 US universities and enterprises across the world through targeted phishing emails. These hackers captured over 31TB of data. This infiltration was uncovered because the universities and enterprises had data privacy officers, data protection managers, IT compliance managers or other data security specialists. Other recent enterprises to suffer major data breaches are Facebook, British Airways, Uber, Verizon and Marriott.[15]

If these global enterprises can experience major data breaches, then it is only a matter of time before other enterprises either disclose a data breach or become aware of a data breach. It is vital for every enterprise to properly monitor its environment and implement proper defense-in-depth strategies to maintain the right privacy and security posture that is in sync with other risk.

Lawsuits are a major issue that can cause public humiliation, reputational damage and large monetary hits. Examples include:[16]

[12] For an example, see ACL, "Getting started with IT governance software," https://www.acl.com/it/it-governance-software/.

[13] ACL, "What is IT readiness and why should IT managers pursue it?," https://www.acl.com/it/it-audit-ready/

[14] For examples, see ACL, "Information technology governance: best practices to prevent data breaches," www.acl.com/it/information-technology-governance/.

[15] Hay Newman, Lily; "The Worst Cybersecurity Breaches of 2018 So Far," *Wired,* 9 July 2018, www.wired.com/story/2018-worst-hacks-so-far/

[16] Marr, Bernard; "GDPR: The Biggest Data Breaches and the Shocking Fines (That Would Have Been)," *Forbes,* www.forbes.com/sites/bernardmarr/2018/06/11/gdpr-the-biggest-data-breaches-and-the-shocking-fines-that-would-have-been/#5a3c6d2a6c10

© 2019 ISACA. All Rights Reserved.

- Marriott International, Inc. recently announced a data breach of 500 million guest accounts and was sued by Rochon Genova LLP on 3 December 2018 in a proposed national class action in Montreal, Quebec.
- Yahoo paid out US $85 million in free credit monitoring to 200 million users as part of a settlement for a data breach in 2013 and 2014 that was not disclosed until 2016.
- Uber agreed to pay US $148 million to settle a data breach that affected some 57 million customers in 2016.
- Target suffered an embarrassing data breach in 2013 in which 40 million customer credit cards were compromised. The retailer agreed to pay up to a US $10 million settlement.

In addition to lawsuits, substantial regulatory fines and remediation requirements can result from a data breach. For example, GDPR has mandated fines and penalties for noncompliance. There are two tiers of fines:

- Up to €10 million or two percent of annual global turnover (revenue) of the previous year, whichever is greater
- And up to €20 million or four percent of annual global turnover, whichever is greater

It is expected that breaches of data subjects' rights will result in the higher-level fine. Many factors will determine the actual fine, including the duration and gravity of the infringement and the types of personal data affected. The level of cooperation and behavior of the enterprise will also play a role in influencing the final fines.[17]

Colorado Consumer Data Protection Laws mandate that any commercial entity (whether for-profit or nonprofit) that experiences a data breach must investigate the likelihood that personal information has been or will be misused. The enterprise is legally required to notify affected Colorado residents as soon as possible by mail, telephone or electronic means.[18]

An enterprise may be unaware of a breach that is occurring or has occurred. Therefore, it is critical for every enterprise to constantly monitor its environment and to implement defense-in-depth strategies to maintain the appropriate data privacy and security posture.

Handling a data breach notification for enterprises varies from jurisdiction to jurisdiction. For example, every US state has its own data breach requirements, on top of the federal data breach notification requirement. Assuming that the enterprise operates nationally in the US, it must adhere to 50 different data breach notification requirements. And, if an enterprise is doing business globally, it must comply with numerous other privacy and data laws and regulations (e.g., GDPR). Therefore, it is essential to have effective and efficient tools and processes to respond when a data breach occurs.

Building a Strong Data Governance Program

To control risk, an enterprise should take foundational steps to build a strong GRC program.

Build Your Team

Governance starts by putting together a cross-functional or multidisciplinary team to help design and drive the process. Because IT connects with so many aspects of an enterprise, expertise is gathered with representation from functional areas, including financial controls, core business operations, human resources, marketing, sales, risk, internal audit and roles within IT itself (e.g., IT security and data specialists). The enterprise should ensure proper and visible leadership support for data protection readiness, including a leader who can overcome obstacles that might arise.

[17] *Op cit* European Commission

[18] The Office of the Attorney General, "Colorado's Consumer Data Protection Laws: FAQ's for Businesses," State of Colorado, https://coag.gov/resources/data-privacy-laws

© 2019 ISACA. All Rights Reserved.

Identify Specific Threats and Controls

An enterprise should implement the following IT governance best practices to ensure proper access and stop personal and sensitive data from being accessed by unauthorized individuals.

- Keep systems and network devices up to date. Monitor potentially vulnerable software that is end of support/end of life or software that may be installed by staff who are unaware of the related threats. Monitor inappropriate manual intervention that can cause unauthorized changes to programs and allow easy access.
- Ensure system software patches and upgrades to all systems and network devices are applied in a controlled manner and an expedient time frame. Employ an information assurance (IA) concept in which multiple layers of defensive security controls are placed throughout critical systems to help prevent known threats and vulnerabilities (e.g., anti-malware, antivirus, encryption, data loss protection, firewall, VPN, etc.).
- Authenticate the identity of end users and ensure the proper maintenance of these user profiles so new hires, external workers, terminations and role changes are always handled within appropriate deadlines and remain up to date.
- Identify potential threats, implement the necessary controls and continuously monitor risk; add new controls as identified. Test controls to ensure that they are operating effectively and are mitigating identified threats. Use traditional methods, because the process of monitoring can be very time- and resource-consuming and prone to error. Developing analytical techniques for automated testing improves the overall coverage and allows for regression and new testing effectively and efficiently with large volumes of data.
- Report regularly on specific new threats and request decisions on adding new controls.

Controls are designed to address the risk at various levels and can become increasingly detailed to help combat specific threats and vulnerabilities. Effective risk management is knowing when it is cost justified to accept a particular risk, and how far to go in implementing a control measure. At some point, the costs of reducing risk can outweigh the likely extent of damage for the enterprise. A control may be so unwieldy that it may cause a severe loss of staff productivity, resulting in deadline challenges and a serious impact on the bottom line.

To manage risk effectively, management needs to consistently assess the extent of risk relative to the controls that are designed. Effective risk management also includes the ability to communicate the overall impact of accepted risk and control failures to senior management. It remains the prerogative of executive management to decide on the appropriate controls for addressing risk.

Continually Assess Effectiveness of Existing Controls

A major part of data privacy readiness is making sure privacy controls are working as intended. Data analysis is a key component of assessing privacy control effectiveness. The analysis can indicate when the personal or sensitive data were accessed, why data were accessed and if the access was authorized. In general, data analysis confirms whether the controls are operating as expected. After data analysis, the enterprise can determine if any changes are necessary, keeping in mind the cost-effectiveness of the control.

Self-assessment by responsible owners and a certification process by senior management on the implementation of the effectiveness of control systems are basic to the process. These assessments should be performed at least annually. To aid in the process, management should request regular reporting of control deficiencies, actions to correct or improve the control process, and insight into why there may be a delay or an inability to correct.

Monitoring can help identify new privacy risk for which no controls are in place. The enterprise should run data analysis reports on a regular basis—daily, weekly or monthly—as determined by key stakeholders. Activities to monitor include:

© 2019 ISACA. All Rights Reserved.

- Super-user/administrator password access
- Special system access granting and revoking
- Separation/segregation of responsibilities
- Overrides and changes
- Security tool and firewall changes
- Data captures
- Data audits
- Changes, network and physical access, and change logs

Regular privacy monitoring and reporting should uncover true data breaches or potential problems. These problems need to be investigated and resolved by the team that is responsible for the system process. The team can leverage GRC tools with workflow orchestration capabilities, including triggers that create alerts and notify key individuals to investigate. This helps to ensure that exceptions and issues do not remain static, or worse, grow in severity, only to be noticed once a breach occurs. Depending on the severity, this investigation and resolution may take priority over other mission-critical projects and may require an escalation process, properly defined within the governance structure, to be addressed at the senior management or even board level.

As the governance process matures and is continually improved and accepted, there will be fewer exceptions requiring action that may disrupt the day-to-day business of the enterprise. The entire control process becomes commonplace with a continuous cycle of privacy testing, monitoring controls, reporting, and addressing and mitigating exceptions with automated workflows. A critical or high-priority data privacy audit finding becomes less likely.

Managing Enterprise Data Life Cycle Compliance Needs

Although many approaches exist for identifying the right tools to manage a GRC program, one approach is to assess needs based on the complexity of each privacy law and another approach is to adopt an end-to-end methodology like the one below. Specifically:

Perform Asset Inventory

The team should identify all critical systems and data that include customers' personal information. Next, the team should determine the current vulnerabilities and the approach to protect against them. Automated tools are superior to any manual efforts, because they allow timely and complete follow up.

Identify Key Risks

The team should start with the privacy risk that has the most strategic impact, including regulatory, operational and emerging risk. This step is critical and at the core of any risk management process. To identify and build a risk universe that is specific for the enterprise, the level of impact to the enterprise must be taken into account and differs for each enterprise. A basic impact classification can be:

- Critical impact
- Major impact
- Medium impact
- Low impact
- No impact

Perform an Impact Analysis

Next, the team should link the privacy risk to the potential impact the risk has on the enterprise achieving its strategic objectives. Privacy risk should always be quantified in terms of financial or other impact (e.g., people, leadership, reputation, customer delivery or projects) in combination with probability/likelihood, and rated relative to the other risk within the enterprise. Risk assessment of the existence and effectiveness of controls

© 2019 ISACA. All Rights Reserved.

that are intended to mitigate the risk should be an ongoing process during the life cycle of a system (i.e., technology, process or people). A data privacy risk assessment is performed annually or ad hoc when questions arise or a privacy incident occurs (inside the enterprise or within the industry in which the enterprise operates).

Monitor Regulations

To help achieve privacy compliance success in an effective and efficient manner, an enterprise can implement technology that monitors:

- The changing regulatory landscape
- Data access
- Software upgrades to existing systems
- The changing technology in the outside world that may pose a threat

An enterprise can decide to manage its data privacy risk, controls and compliance processes with generic tools and technologies that are not built to manage data privacy governance. If an enterprise chooses to do this, the manpower required will be higher, and the risk of potential data loss will also be higher.

An enterprise is more likely to achieve the greatest success and transform how privacy controls and compliance processes are managed when it implements technologies that are designed and built for this specific purpose. These technologies must be integrated, as much as possible, within the existing technological portfolio to avoid a technological silo. One of the basic requirements is the ability to move data from different sources and to export results to the appropriate organizational (business intelligence) reporting tool to allow efficient integration into the existing management reporting console.

Compare GRC or Commercial-Off-the-shelf Solutions

Another approach to using GRC software for monitoring and integrating various global privacy laws is performing comparisons between different countries or different privacy categories, such as sectoral, comprehensive or co-regulatory/federal/state privacy laws. Good examples are the GDPR and another recently passed bill, the California Consumer Privacy Act (CCPA). Both laws are considered comprehensive but have a few material differences. Some of the requirements worth exploring are:

- Processing of personal data/information (common to both)
- Right of access (common to both)
- Right to erasure/deletion (common to both)
- Right to rectification (GDPR)
- Right to restriction of processing (GDPR)
- Right to data portability (common to both)
- Right to object (GDPR)
- Right to opt-out (CCPA)
- Opt-out notice (CCPA)
- Data protection/privacy policy (common to both)
- Privacy notices (common to both)
- Reuse and disclosure (common to both)

Some of these requirements are very simple because enterprises are doing them already. Other requirements require due diligence involving one or more of the following functional areas:

- Human resources
- Procurement/vendor management
- Legal and compliance
- Quality control
- Information technology and information security
- Marketing, sales, and communications
- Operations
- Customer service

For any of the above departments, the right-to-deletion requirement is a challenge to implement. Proper privacy impact assessments must be undertaken for the legacy application process before an enterprise can create an effective and efficient solution. Part of that assessment includes defining the following roles, inside and outside of the enterprise:

1. **Data subject**—an individual
2. **Controller**—the organization that collects, uses, stores, discloses and destroys the customer's personal information
3. **Processor**—an organization that processes personal information on behalf of the controller

© 2019 ISACA. All Rights Reserved.

4. **Supervisory authority**—the reporting authority that audits the controller/processors to ensure that an enterprise implements a regulation

These roles are explained in more detail in the following right-to-deletion example:

1. A data subject places a request with a controller to delete all of his/her personal information.
2. The controller (or the processor on behalf of the controller) must process this request for deletion within a given time limit that is specified by the regulation or act.
3. The controller or processor must apply proper due diligence to first ensure that the data subject's request is valid. Then, the controller or processor must ensure that the information is properly deleted, independent of where that information might reside (e.g., single systems, multiple systems and paper filing). If the controller is a multinational, operates from the US, and sells products or services to European citizens, then this adds to the complexity of the request for deletion.
4. Now, the controller needs to meet the regulations of the US and the EU. As per US regulations, some of the key information on the data subject must be retained for up to 10 years. An enterprise can solve this by tokenizing the personal information. In this way, the systematic approach of accessing the data subject will not be available anymore and, from the customer service point of view, the data subject is deleted from the system, thus satisfying the European requirement and the US requirement at the same time.

An enterprise must have a strong GRC program to be able to follow all the requirements set by the regulators in countries where the enterprise operates. The guiding principles and requirements of these data privacy laws must be mapped against well-established standards, such as ISO 27001/27002[14] and NIST,[15] and governance frameworks, such as ISACA's COBIT 5 and AICPA's Generally Accepted Privacy Principles (GAPP).[16] A data privacy program can be implemented with one of the following privacy models, selected based on the size and nature of the enterprise:

- **Decentralized**—differing jurisdictions mandate
- **Centralized**—common data privacy laws or approved as adequate with each other's jurisdiction
- **Hybrid**—a combination of the centralized and decentralized models

The requirements and methods in this section are essential to consider in the evaluation of the appropriate GRC solution that will allow an enterprise to meet the complex requirements of the various data privacy laws in the different countries in which it operates.

How Enterprises Can Improve Privacy Risk

Because data-breach processes can be streamlined with GRC software, more software providers are offering their GRC solutions as SaaS (Software as a Service) cloud applications, which brings along its own risk. Enterprises have options to choose the right GRC software based on their needs and risk because many have already migrated, or are in the process of moving, some or many of their applications to a cloud environment.

The following case studies demonstrate an enterprise's adoption of cloud and how it applied proper control measures to protect customers' sensitive PII and special-categories data.

Case Study 1

A major US financial institution decided, as part of a transformation initiative, to move legacy data files to a cloud environment. To ensure proper data migration, they:

1. Conducted a privacy impact assessment (PIA) to identify the people, processes and technology that currently use these data files.

© 2019 ISACA. All Rights Reserved.

2. Analyzed all the data files that needed to be archived in cloud storage and created data classification and label artifacts to identify general and sensitive PII data elements.
3. Used tokenization services to tokenize all the regulatory and PII data.
4. Analyzed many cloud service providers (CSP) and selected two—one as the primary and another for secondary/backup storage. Analyzed the CSPs based on the guidelines provided by the Cloud Security Alliance (CSA).
5. Established secure data transfer connections between the legacy system and identified CSPs.
6. Established virtual private cloud architecture to host the archival data files on the cloud.
7. Successfully moved approximately 500TB of data (critical files used by the credit card issuing modules) and, with some additional steps, began the process of moving their statement images.

This institution demonstrated due diligence in the IT governance process, which helped it migrate from the fixed and variable cost of retaining the archival data files in its legacy data center, to a pay-per-use variable cost model, without incurring any of the fixed cost and the licensing fees.

Case Study 2

In order to implement better collection strategies, a major global financial institution deployed an artificial intelligence machine and deep learning concept to determine the pattern of payment defaults by its customers. To derive the pattern, a very large historical data set needed to be moved to a cloud relational data store. To ensure proper data migration, this institution:

1. Analyzed and identified all regulated and sensitive PII data for tokenization before bringing the large data set into the cloud.
2. Deployed the virtual private cloud to build the custom API to utilize the machine and deep learning services.
3. Successfully identified the required patterns and deployed the new collection strategies from these derived patterns.

This institution demonstrated that it is feasible to employ new technologies without causing data breaches, data loss or data drift.

Both these case studies demonstrate that data privacy can be enforced by adopting appropriate data protection techniques such as tokenization.

Conclusion

Technological advancements will continue to introduce new threats and vulnerabilities, and data privacy laws and regulations will continue to evolve. Therefore, it is essential for an enterprise to build a strong regulatory data governance and protection model. This model will help make customers, partners and suppliers feel comfortable coming to the enterprise, sharing their personal and sensitive information and retaining services for future business.

If an enterprise does not take action and is subject to a major data breach, it will suffer monetary and business losses. Regaining customer trust will be a long and uphill battle.

Automating privacy-law monitoring and compliance reporting is vital for any enterprise to produce data privacy compliance deliverables effectively and efficiently.

The goal is to be better prepared to deal with risk when it occurs, by planning ahead, monitoring and mitigating. This approach allows enterprises to better respond when the inevitable data breach occurs.

© 2019 ISACA. All Rights Reserved.

Acknowledgments

ISACA would like to recognize:

Lead Developers

Balaji Rengamannar
CISM, CIPM, PCI QSA
Chief Executive Officer A1PlusSoft, Inc., USA

Hema Kumaran
Communications Manager, India

Saravanan Rengamannar
SW Architect, India

Stephen B Wheet
Advisor, USA

Lakshman R Yandapalli
Advisor, USA

Expert Reviewers

Mais Borouqa
CISA, CRISC, COBIT 5, GRCP, ISO 27001, ITIL
IT Risk and Assurance Services Assistant Manager, Jordan

Joanna Karczewska
CISA
Poland

Amitav Parida
AWS Certified Solutions Architect
Senior Manager, USA

Phil Shomura
Senior Product Manager, Canada

Jo Stewart-Rattray
CISA, CRISC, CISM, CGEIT, FACS CP (Cyber Security)
Director of Information Security and IT Assurance, Australia

Marc Vael
CISA, CRISC, CISM, CGEIT
Chief Information Security Officer, Belgium

ISACA Board of Directors

Rob Clyde, Chair
CISM
Clyde Consulting LLC, USA

Brennan Baybeck, Vice-Chair
CISA, CRISC, CISM, CISSP
Oracle Corporation, USA

Tracey Dedrick
Former Chief Risk Officer with Hudson City Bancorp, USA

Leonard Ong
CISA, CRISC, CISM, CGEIT, COBIT 5 Implementer and Assessor, CFE, CIPM, CIPT, CISSP, CITBCM, CPP, CSSLP, GCFA, GCIA, GCIH, GSNA, ISSMP-ISSAP, PMP
Merck & Co., Inc., Singapore

R.V. Raghu
CISA, CRISC
Versatilist Consulting India Pvt. Ltd., India

Gabriela Reynaga
CISA, CRISC, COBIT 5 Foundation, GRCP
Holistics GRC, Mexico

Gregory Touhill
CISM, CISSP
Cyxtera Federal Group, USA

Ted Wolff
CISA
Vanguard, Inc., USA

Tichaona Zororo
CISA, CRISC, CISM, CGEIT, COBIT 5 Assessor, CIA, CRMA
EGIT | Enterprise Governance of IT (Pty) Ltd, South Africa

Theresa Grafenstine
ISACA Board Chair, 2017-2018
CISA, CRISC, CGEIT, CGAP, CGMA, CIA, CISSP, CPA
Deloitte & Touche LLP, USA

Chris K. Dimitriadis, Ph.D.
ISACA Board Chair, 2015-2017
CISA, CRISC, CISM
INTRALOT, Greece

© 2019 ISACA. All Rights Reserved.

About ISACA

Now in its 50th anniversary year, ISACA® (isaca.org) is a global association helping individuals and enterprises achieve the positive potential of technology. Today's world is powered by information and technology, and ISACA equips professionals with the knowledge, credentials, education and community to advance their careers and transform their organizations. ISACA leverages the expertise of its 460,000 engaged professionals—including its 140,000 members—in information and cybersecurity, governance, assurance, risk and innovation, as well as its enterprise performance subsidiary, CMMI® Institute, to help advance innovation through technology. ISACA has a presence in more than 188 countries, including more than 220 chapters worldwide and offices in both the United States and China.

About ACL

ACL's purpose-built, cloud-based platform helps IT teams manage governance over cybersecurity, privacy, regulations, risk and compliance. ACL makes it easy to continuously analyze data, enabling robotic automation of governance activities and visualization of patterns. And with over 30 years of experience, built-in best practices and a professional development ecosystem, ACL quickly helps IT managers work more efficiently, identify and mitigate risk, reduce compliance pressures, and ensure audit and regulatory readiness. For more information, please visit www.acl.com.

DISCLAIMER

ISACA has designed and created *Enforcing Data Privacy in the Digital World* (the "Work") primarily as an educational resource for professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

RESERVATION OF RIGHTS

© 2019 ISACA. All rights reserved.

ISACA®

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

Phone: +1.847.660.5505

Fax: +1.847.253.1755

Support: support.isaca.org

Website: www.isaca.org

Provide Feedback:

www.isaca.org/enforcing-data-privacy

Participate in the ISACA Online Forums:
https://engage.isaca.org/onlineforums

Twitter:
www.twitter.com/ISACANews

LinkedIn:
www.linkd.in/ISACAOfficial

Facebook:
www.facebook.com/ISACAHQ

Instagram:
www.instagram.com/isacanews/

© 2019 ISACA. All Rights Reserved.

acl

Achieve greater IT Governance

Essential resources to help you navigate today's IT governance challenges.

Download the IT Governance Success Kit at acl.com/value »