January 2010

A Guide to Data Governance for Privacy, Confidentiality, and Compliance

Part 1: The Case for Data Governance

Javier Salido, MSc, MBA, CIPP
Senior Program Manager, Trustworthy Computing Group, Microsoft Corporation

Patrick Voon, CGEIT, CISA, CISSP
Senior Governance, Risk and Compliance, Subject Matter Expert, Edgile Inc.
The information contained in this document represents the current view of Microsoft Corp. on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise), or for any purpose, without the express written permission of Microsoft.

Microsoft may have patents, patent applications, trademarks, copyrights or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights or other intellectual property.

© 2010 Microsoft Corp. All rights reserved.

Microsoft and Windows Live are either registered trademarks or trademarks of Microsoft Corp. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Microsoft Corp. • One Microsoft Way • Redmond, WA 98052-6399 • USA
Contents

Executive Summary........................................................................................................................................1

The Whitepaper Series ..................................................................................................................................2

Introduction......................................................................................................................................................4

The Challenges ..............................................................................................................................................4

Information Security ......................................................................................................................................4

Information Privacy ......................................................................................................................................5

A Complex Regulatory Landscape ............................................................................................................6

Governance, Risk Management, and Compliance (GRC) ........................................................................7

Data Governance .........................................................................................................................................9

Data Governance, IT Governance, and Compliance ..................................................................................10

Data Governance for Privacy, Confidentiality, and Compliance: An Overview ........................................11

Conclusion ......................................................................................................................................................16

Glossary of Terms .......................................................................................................................................18

References ....................................................................................................................................................20
Executive Summary

The past decade has produced an unprecedented accumulation of data. Organizations in general and business models in particular increasingly rely upon confidential data such as intellectual property, market intelligence, and customers’ personal information. Maintaining the privacy and confidentiality of this data, as well as meeting the requirements of a growing list of related compliance obligations, are top concerns for government organizations and the enterprise alike. Addressing these challenges requires a cross-disciplinary effort involving a varied list of players—human resources, information technology, legal, business units, finance and others—to jointly devise solutions that address privacy and confidentiality in a holistic way. Data governance is one such approach that addresses many aspects of data management, including information privacy and security as well as compliance.

This whitepaper is the first in a series that looks at different aspects of data governance. It opens with a brief overview of the entire series. It then outlines the threats and challenges that organizations face in this area and looks at the concepts of governance, risk management, and compliance in general. From there, it examines the concept of data governance for privacy, confidentiality, and compliance (DGPC) in particular. It closes with a brief overview of the objectives and overall process flow for a DGPC initiative.
The Whitepaper Series

This whitepaper series aims to answer some key questions that IT managers, security officers, privacy officers, and risk management officers are asking about how to approach the combined challenges of information security and privacy and the associated regulatory compliance obligations.

In its broadest form, data governance is an approach that public and private entities can use to organize one or more aspects of their data management efforts, including business intelligence (BI), data security and privacy, master data management (MDM), and data quality (DQ) management. This series describes the basic elements of a data governance initiative for data privacy, confidentiality, and compliance and provides practical guidance to help organizations get started down this path.

The series is meant for organizations of all sizes and for those with regional as well as global focus. Some might already have an effective IT governance process and information security management system, as well as successful privacy and risk management efforts in place. Some might just be getting started.

At Microsoft, we believe that in order to deal effectively and efficiently with data confidentiality and privacy challenges, organizations must adopt a proactive stance, one in which they hold themselves accountable for:

- Appropriately protecting the security of customers’ and employees’ personal information, as well as the organization’s intellectual property and trade secrets.
- Respecting, preserving, and enforcing customer choice and consent throughout the information lifecycle, particularly when it comes to deciding how personal information is used and distributed within and outside the organization.

As they approach data privacy and security, organizations should consider the following:

- Taking a holistic approach to data privacy and security needs as well as related regulatory and internal compliance requirements. This approach to the planning and implementation of data privacy and security brings together a range of participants. They could include groups and individuals that:
  - Own business processes that generate, collect, and use data
  - Have specific charters with respect to confidential data, such as the chief privacy officer, the legal department, and the IT department
- Augmenting approaches that focus on mere compliance “with the letter of the law,” by implementing and enforcing data privacy and security measures based on generally accepted principles,¹ state-of-the-art industry best practices, and self-regulation measures that go beyond mere compliance with the letter of regulations and standards.

American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA), “Generally Accepted Privacy Principles,” http://infotech.aicpa.org/Resources/Privacy/Generally+Accepted+Privacy+Principles.
• Augmenting prevailing IT privacy and security paradigms—which address threats by restricting access to data and keeping it from "escaping" well-defined boundaries—by evaluating threats to confidential data at different stages of the information lifecycle. This approach helps organizations identify technical and nontechnical measures that can reduce security and privacy risks to acceptable levels.

In this paper, we analyze the data privacy and security challenges that organizations face today, including an increasingly complex regulatory environment. We then look at the concept of data governance and analyze how it complements ongoing efforts within the organization. Finally, we outline the core process for data governance for privacy, confidentiality, and compliance (DGPC) and discuss the key elements an organization must have in place to get started.

Other papers in the series will:

• Review the DGPC process in greater detail and discuss the organizational elements required to support it.
• Provide tools to help organizations evaluate security and privacy risks in the context of the information lifecycle and select technical and nontechnical measures to manage these risks based on the organization's risk tolerance.
• Discuss how these tools and processes can be extended to mixed environments that include cloud-based data storage and applications.

---

Introduction

The past 30 years have brought significant changes in the way organizations are structured and run. Entirely new business models have emerged, and old ones have been radically transformed. Productivity has soared, fueled by an endless stream of innovations in information and communications technology (ICT). Centuries-old paradigms for data collection, storage, and use have shifted. Until the early 1990s, it was fairly common for individual departments and divisions to collect, store, and use their own data in their own file cabinets or in departmental computers; as a result, information that could not easily be shared with other groups. Rapid advances in the ability of different technologies to interoperate have made it easier for entities of all sizes to exchange information in an almost seamless fashion. Such information exchanges are integral to business efficiency, competitiveness, collaboration, and agility in the 21st century.

The massive and rapid flow of information over the Internet has played a key role in this transformation, by enabling applications that make use of intelligent data analysis, expanded sales and service channels, and other tools. These applications, along with diminishing storage costs, have made it easy for organizations and individuals to accumulate unprecedented amounts of data. A study by the School of Information at the University of California, Berkeley, estimated that the world’s total production of content in 2002 required 5 exabytes (5 thousand million gigabytes) of storage. It also estimated that the volume was growing at an average yearly rate of 30 percent.3 If these trends continue, humans will require 40.8 exabytes of storage space for new data in 2010. That is 2.7 gigabytes for each man, woman, and child on the planet.

This situation has raised awareness of the need to protect confidential data kept by organizations—including intellectual property, trade secrets and market data, and the personal data of customers, employees, and partners—against misuse and unauthorized disclosure or modification.4 In some cases, concerns have led to the enactment of laws and regulations that vary by industry or geography and the creation of specific industry standards.

Organizations, private and public alike, find themselves confronted with challenges that can at times seem overwhelming.

The Challenges

Information Security

Much has been written about the changing nature of IT security threats. From viruses and worms built to satisfy the egos of their creators, threats have expanded and shifted in source and scope. Organizations now worry about criminal enterprises that steal customers’ personal information, small storage media and devices that can hold gigabytes of data and can easily be lost or stolen, and even industrial espionage and warfare. Information security itself is no longer a relatively obscure discipline of IT that is relevant primarily to financial

---


4 Note that the term “confidential data,” used throughout this document, encompasses personal data (under the European Commission definition), personally identifiable information (PII), intellectual property (IP), trade secrets, and all other types of information for which an organization might want to maintain confidentiality, integrity, and availability.
and government institutions. It has become a topic of conversation for C-level executives and is commonly discussed by the mainstream media. The attention is justified: the financial and reputational cost that information security incidents like data breaches can have on an organization is significant. Consider the following:

- According to DataLossDB, a nonprofit organization that tracks data breach incidents, more than 218 million records containing individuals’ personal data were compromised in 436 incidents in 2009.5
- A study by the Ponemon Institute of organizations that suffered one or more data breach incidents in the United States in 20086 found that the average cost incurred by the organizations was US$6.6 million (not including long-term litigation costs and the resulting penalties). The study also found that these organizations lost an average 3.6% of its customer base as a result of the incident(s). For financial institutions, the average loss was 6%.
- In January 2009, U.S.-based payment processor Heartland Payment Systems disclosed what is possibly the largest data breach on record. An identity theft ring stole an estimated 130 million credit and debit card records from the company’s databases.5 The CEO estimated that the company spent close to US$32 million in the first half of 2009 in IT and legal costs related to the breach.7 Heartland’s market value dropped by 75% in the two months following the announcement of the incident.

**Information Privacy**

Not surprisingly, the highly sensitive nature of some of the information involved in data breach incidents, the large number of records lost, and the potential for an increase in identity theft cases has attracted the attention of consumers and policymakers alike. Concerns about personal privacy as well potentially abusive or careless use of technology by organizations are causing a significant shift on how consumers think about their personal information when held by an organization.

A June 2009 report by the School of Information at UC Berkeley shows that consumers want control over how their personal information is collected, with whom it is shared, and how it is used by the parties involved.8 This represents a significant departure from the way many organizations have viewed customer data—as something the organization “owns” and can therefore exploit as they see fit. Enlightened organizations now appreciate that certain personal data is placed in their trust by customers, and that such trust has significant business value.

The UC Berkeley study suggests that the top privacy concerns of U.S. consumers are:

- The perception that some organizations employ deceptive practices to collect personal information from consumers

---

A Guide to Data Governance for Privacy, Confidentiality, and Compliance

- The perception that some business practices contradict the collecting organization’s stated privacy policies

Such perceptions seem to be driven by the aforementioned concerns about ID theft and misuse of personal information, as well as by concerns about how and when organizations share personal information with third parties. The burden that is currently placed on individuals when it comes to making privacy related decisions does not help, either. Consumers are expected to read and understand every privacy policy from every website they interact with, and to make choices and provide consent based on that understanding. This is simply too much to ask of many people, and something organizations should consider if they want to maintain customer trust.

A Complex Regulatory Landscape

Motivated by security threats and by the need to protect consumers’ personal information from abuse, legislative bodies and government institutions have moved to regulate processing and transfer of personal information. Standards bodies and industry associations have followed suit by promoting or requiring the adoption of key security and privacy standards. These actions serve two key objectives: to spread awareness and use of best practices and to promote levels of self-regulation that might forestall the enactment of increasingly restrictive laws that could harm industries or commerce in general.

Here is a sampling of these laws, regulations, and industry standards:

- In most European nations, the right to privacy is considered a basic human right. European Union member nations are required to enact laws that comply with the Data Protection Directive (DPD) 95/46/EC. The directive’s guidelines are considered a baseline for national laws, and local legislative bodies in member nations may include provisions that go beyond it. Implementation of 95/46/EC is not limited to EU members; Iceland, Norway, and Lichtenstein are among the non-EU nations that have enacted privacy laws that comply with the directive.

- Many other nations have also enacted comprehensive privacy legislation. Examples include Australia’s Privacy Act, Argentina’s Personal Data Protection Law, and Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA).

- In the United States, privacy legislation has taken more of a sector-based approach. Different laws regulate how organizations collect, use, and protect the confidentiality of personally identifiable information (PII) in different sectors. Examples include the Health Insurance Portability and Accountability Act (HIPAA) for health-related PII and the Gramm-Leach-Bliley Act (GLBA) for credit-related PII. Concerns about data breaches that could lead to an increase in identity theft have led most states to enact data breach notification laws. Federal legislation on this matter is being considered in the U.S. Congress. Prompted by the same concerns, states such as Massachusetts and Nevada have also enacted laws that require adoption of encryption technologies to protect the sensitive personal information of state residents in different scenarios.

---

9 Exactly 45 states, in addition to the District of Columbia, Puerto Rico and the U.S. Virgin Islands, at the time of writing.
• The payment card industry (PCI) has taken steps to prevent credit card fraud and protect cardholders against identity theft. The PCI Security Standards Council (PCI SSC) requires all entities that want to hold, process, or transfer cardholder information to comply with the PCI Data Security Standard (PCI DSS). Among other provisions, the standard requires that an organization’s compliance be assessed every year by an independent Qualified Security Assessor (QSA).

Organizations are left with the daunting and increasingly expensive task of determining which rules—including geographically based and industry-specific ones—apply to their national or globally dispersed activities. In some instances, they are forced to decide what constitutes a conflict between multiple compliance obligations and to determine how to address it. The issues are complex and depend on the type of data involved, the type of industry, where and how the data is collected, how it is used, and the residence of the individuals whose PII is collected.

**Governance, Risk Management, and Compliance (GRC)**

The combination of business and technology-related challenges and the requirement to meet regulatory compliance obligations is not unique to the area of information security and privacy. Such combinations are common in areas such as enterprise risk management, finance, operational risk management, and IT in general. An approach commonly known as governance, risk management, and compliance (GRC) has evolved to analyze risks and manage mitigation in alignment with business and compliance objectives.

• **Governance** ensures that the business focuses on core activities, clarifies who in the organization has the authority to make decisions, determines accountability for actions and responsibility for outcomes, and addresses how expected performance will be evaluated. All of this happens within a clearly defined context that might span a division, the entire organization, or a specific set of cross-discipline functions.

• **Risk management** is a systematic process for identifying, analyzing, evaluating, remedying, and monitoring risk. As a result of this process, an organization or group might decide to mitigate a risk, transfer it to another party, or assume the risk along with its potential consequences.

• **Compliance** generally refers to actions that ensure behavior that complies with established rules as well as the provision of tools to verify that compliance. It encompasses compliance with laws as well the enterprise’s own policies, which in turn can be based on best practices. Compliance requirements are not static, and compliance efforts should not be either.

GRC goes beyond merely implementing these three elements separately and finds ways to integrate them to increase effectiveness and efficiency and decrease complexity. GRC ensures than an organization acts in accordance with self-imposed rules, acceptable risk levels, and external regulations, as illustrated in Figure 1. Each circle in the figure represents one component of the GRC approach; each rectangle includes the
description of that component’s main objective. Each arrow shows the information exchanges among the three elements.\textsuperscript{10}

\begin{figure}
\centering
\includegraphics[width=\textwidth]{grc_overview.png}
\caption{Governance, Risk Management and Compliance (GRC) overview}
\end{figure}

Organizations typically find it easier to focus on compliance first, and then gradually expand efforts to include risk management and governance. It is important to note, however, that governance activities will happen, whether planned or not, and that lack of planned governance and rigorous risk management can have serious consequences for the business.

By its very nature, GRC is broad in scope. Furthermore, in today’s organization, no single group or entity holds all the relevant knowledge and expertise necessary to achieve the desired objectives. This required knowledge might encompass organizational practices and processes, financial and legal aspects of the business, company policies, and market trends. Organizations need an integrated, focused approach. They need a form of GRC.

that specifically focuses on data privacy, confidentiality and compliance; that can provide the appropriate context for multi-disciplinary discussions; and through which appropriate solutions can be defined. This approach is data governance.

**Data Governance**

Data Management International (DAMA, [www.dama.org](http://www.dama.org)), a nonprofit organization for data management professionals, defines data governance as follows:

> The exercise of authority and control over the management of data assets. It is the planning, supervision and control over data management and use.\(^\text{11}\)

Enterprise Data Governance (EDG) focuses on high-level planning and control of the entire data management function, which DAMA describes as “the business function of planning for, controlling and delivering data and information assets to the organization.” Throughout this whitepaper series, the term EDG refers to an organization-wide data governance effort that encompasses two or more of the data management functions listed above; as opposed to the simpler DG, which refers to a specific function.

DAMA’s guide to the data management body of knowledge identifies the following core data management functions that are overseen by EDG:

- Data Security management (which comprises data security and privacy, as well as related regulatory compliance requirements)
- Data Architecture management
- Data Base Operations management
- Master Data and Meta Data management
- Data Quality management
- Data Warehousing and Business Intelligence management
- Data Development
- Document and Content management

EDG is comprehensive in scope. Most organizations that implement a data governance initiative start with a much narrower focus—typically only one or two of the data management functions listed above. For instance, in the case of this discussion, the scope would be only data privacy and confidentiality. Of course, once the organization has gained experience governing the selected function, it can expand the program to include others. In that case, the EDG effort can provide a common vision, principles, and guidelines that support all functions, including data security and privacy.

Data Governance, IT Governance, and Compliance

Many organizations wonder whether they truly need DGPC if they already have successful IT governance, a well-established control framework, and an effective information security management system (ISMS) and are currently meeting their compliance obligations. The answer to this question is directly related to the discussion in the previous section:

- Compliance is commonly and narrowly understood to be about meeting requirements—checking boxes, so to speak. Good data governance enables compliance in a changing regulatory landscape and takes into account changes in the organization’s own business goals and objectives.
- Data governance does not replace IT governance but complements it. To borrow an analogy commonly used by the data management community, IT governance focuses on the pipelines—the organization’s IT infrastructure. Data governance focuses on the water—the data that flows through those pipelines. IT governance focuses on defining a portfolio of IT investments, setting performance objectives, and evaluating and managing risk for the IT infrastructure. It ensures alignment of those IT investments with the organization’s mission and business goals, and it evaluates and manages organization-wide risks to the IT infrastructure. Data governance, on the other hand, focuses on creating a context that enables the organization to align data management efforts with business objectives, support regulatory compliance, and manage risks that are specific to the data itself.
- DGPC does not replace essential IT management and control tools, such as control frameworks like COBIT, the Microsoft Operations Framework (MOF), or security standards such as ISO/IEC 27001/27002 and PCI DSS. To use another analogy, security standards and control frameworks focus on the “forest” of information protection—managing the risks related to the protection of the IT infrastructure and the information it contains. DGPC, on the other hand, focuses on the “trees” of information protection—managing risks related to the specific data elements that the organization wants to protect, including personal information, intellectual property, trade secrets, and market data.

Figure 2 illustrates how the concepts of IT governance, data governance, and compliance relate to one another and to data security and privacy controls. Note that the information security management system is considered a component of the IT governance domain.

---

12 Our use of the term “information protection” focuses on protection of all confidential data in the organization, and is different from the term “data protection” used in the EU Data Protection Directive, which refers to the protection of personal data only.
The main objectives of DGPC are:

- To protect the organization’s data against internal and external threats to privacy and confidentiality
- To ensure that the organization complies with applicable laws, regulations, and standards
- To ensure that proof of compliance is generated and documented within the process

At a practical level, this means the organization needs to understand the myriad business and legal requirements it has to comply with and define a set of common controls and activities that meet those requirements and that can be effectively monitored and documented. To make this possible, organizations must follow an activity flow similar to that shown in Figure 3.
Figure 3. Data Governance for Privacy, Confidentiality and Compliance activity flow

Here is a brief overview of each of the activities (ovals) shown in the activity flow, and the corresponding inputs/outputs (rectangles). Note that in both Figure 3 and the description that follows, the letter indicator A.x refers to activity x, and the indicators O.y and I.z refer respectively to output y and input z. A more detailed look at this process, and the organization that supports it, is provided in the second whitepaper in this series: “A Guide to Data Governance for Privacy, Confidentiality, and Compliance. Part 2: People and Process.”

A.1: Examine relevant authority documents

- The first input in the process (I.1), labeled “Authority Documents,” refers to laws, regulations, and industry standards that are applicable to the organization. It also refers to the organization’s own approved policies, business plans, and objectives.
- If the organization has an enterprise data governance (EDG) program along the lines described earlier, its guidelines and best practices (I.2) need to be taken into account. For DGPC purposes, relevant
parts of these EDG guidelines include guidance from key DAMA data management functions, such as Document and Content management, Business Intelligence, and Master Data management.

- In activity A.1, the relevant authority documents are selected and examined to produce an initial list of high-level integrated DGPC requirements. Authority documents listed in I.1 in Figure 3 are examples and do not constitute an exhaustive list. Note that if the organization has an EDG program in place, the selection of appropriate authority documents may take place in the context of EDG efforts, in which case the DGPC activity flow will start in activity A.2.

A.2: Refine Requirements

- The authority documents selected in A.1 will serve as input to A.2, the activity in which data compliance and business data requirements are defined and refined to produce a list of final requirements (O.1/I.4).
- Note that the inputs from A.1 affect the organization as a whole. Other relevant authority documents that are more limited in scope but nevertheless relevant to privacy, confidentiality, and compliance efforts might exist. Examples of these “GRC sources” (I.3) are control frameworks (COBIT, MOF) and security and privacy standards (such as ISO/IEC 27001 and PCI DSS); these must also be provided as inputs to A.2 if they are in use within the organization.
- The outcome of this process is a unique, harmonized set of compliance requirements that make it possible to eliminate redundant controls, reduce costs, and increase operational efficiency and effectiveness (O.1/I.4).  

A.3: Define Strategy & Policies

- Requirements and guidance in O.1/I.4 will shape the definition, in A.3, of DGPC strategy, principles, and policies, all of which are documented in O2/I.5. These outputs are described later in this section.

A.4: Define Control Environment

- The principles, policies, and strategy (O.2/I.5) serve as input to define the DGPC control environment (A.4). The resulting list of manual and technical controls (O.3) represents the solution that the DGPC process proposes in order to meet the privacy, confidentiality, and compliance requirements identified in A.2. These include control activities that support control objectives that were derived from policies, standards, procedures, and guidance. For instance, a user access management policy may require that designated data stewards review and approve user access requests using the following controls:
  o A manual control, which may be implemented in the form of an access request workflow procedure that supports this policy.

---

13 The study “IT GRC: Managing Risk, Improving Visibility, and Reducing Operating Costs” by Aberdeen Group, 2009, revealed that the top two pressures driving investments in IT GRC are “Address New/Changing Regulatory Compliance” (88%) and “Improve Operational Efficiencies” (80%).

14 The term “data steward” is discussed further in Part 2 of this whitepaper series and is used throughout the remaining whitepapers. DAMA’s definition of the term is included in the glossary of this paper.
A technical control, which is implemented by automating the routing of the request to the designated data steward for approval prior to granting access to the user.

We now provide additional details and comments on some of the key inputs/outputs from activity A.3.

**DGPC Strategy (O.2/I.5)**

A successful DGPC program starts with the definition of a clear, concise, measurable, and executable strategy. The strategy states the goals and objectives of the program and provides a roadmap with the necessary short- and long-term activities. By establishing this roadmap, the organization sets the stage for identifying and assigning necessary resources to support strategic activities.

**Data Privacy and Confidentiality Principles (O.2/I.5)**

These principles play a key role in the risk management process and the selection of the activities and technologies that will protect confidential data assets such as intellectual property, trade secrets, or personal information. The principles start out as high-level statements that can be followed by more detailed guidance. Specifically, this detailed guidance should take the form of clear and concise statements that “translate” the high-level principles into information security and privacy language that can be used to guide the risk management and decision-making processes.

Below we identify four general principles that can be applied in most organizations. Examples of actionable guidance are also provided; these are loosely based on the Organisation for Economic Co-operation and Development’s information privacy guidelines. The four principles play an important role in the selection of technical and manual controls and in the process of risk management (a topic discussed in the third paper of this series). Note that the use and enforcement of a data classification taxonomy and an associated use policy are prerequisites for the proper adoption of any of the four principles and the success of the DGPC effort. Both the taxonomy and the policy must be clearly communicated to all individuals involved in the generation, collection, and use of data. Enforcement of the policy throughout the organization will be more effective if tools can be used to automate it.

**Principle 1: Honor policies throughout the confidential data lifespan**

- Process all data in accordance with applicable statutes and regulations.
- Preserve privacy and respect individuals’ choice and consent in the collection, use, sharing, and disclosure of customer, partner, and employee personal information.
  - Systems should provide notice of data collection, use, disclosure, and redress policies.

---

15 Organisation for Economic Co-operation and Development, “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,” [www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html](http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html).


18 Policies may comprise various requirements derived from laws, standards, promises, individual customer or employee choices, commercial obligations, and other sources.
Confidential data should be tagged when collected, generated, or modified, in accordance with organizational policy.

Machine-readable data privacy policies must be available in digital form.\(^\text{19}\)

- Systems should provide individuals with access and capabilities to correct information as applicable.
- All confidential data types should have a clearly associated retention policy and disposal procedures.
- Confidential information will be transferred to and stored in facilities/geographies that meet applicable laws and regulations.

**Principle 2: Minimize risk of unauthorized access or misuse of confidential data**

- Information protection: The system provides reasonable administrative, technical, and physical safeguards to ensure confidentiality, integrity and availability of data. This includes the ability to detect and prevent unauthorized or inappropriate access to data.
- Data quality: The system should maintain accurate, timely, and relevant data, and this capability should be verifiable.

**Principle 3: Minimize impact of confidential data loss**

- Information protection: Systems should provide reasonable safeguards (i.e., encryption) to ensure confidentiality of data if it is lost or stolen.
- Accountability: Appropriate data breach response plans and escalation paths should be in place and documented for all relevant data. All organization employees likely to be involved in breach response should be trained appropriately in these plans and the use of the escalation paths. Appropriate breach notification plans should be in place for all relevant data.

**Principle 4: Document applicable controls and demonstrate their effectiveness**

- Accountability: Adherence to data privacy and confidentiality principles should be verified through appropriate monitoring, auditing, and use of controls. Plans and controls should be properly documented.
- Compliance should be verifiable through logs, reports, and controls. The organization should have a process for reporting non-compliance as well as a clearly defined escalation path.

Appropriate data privacy and confidentiality principles are essential to the success of DGPC. Organizations should carefully consider the selection of both the principles and the related guidance statements. DGPC team members would benefit from considering other sources as well, such as the Generally Accepted

---

\(^{19}\) In 2007, the World Wide Web Consortium (W3C) published the Platform for Privacy Preferences (P3P), a framework that requires privacy policies to be prepared in a standardized, machine-readable format. Information can be found at the W3C Web site: [www.w3.org/P3P](http://www.w3.org/P3P).
Privacy Principles (GAPP),\textsuperscript{20} the privacy principles of the European Data Protection Directive (EUDPD),\textsuperscript{21} and the ISO/IEC 27001/27002 security standards.\textsuperscript{22}

**DGPC Policies (O.2/I.5)**

DGPC policies should be based on business and compliance requirements, the DGPC strategy, and the Data Privacy and Confidentiality Principles. Basic DGPC policies include:

**Data Classification**

This policy establishes a classification scheme that applies throughout the enterprise to define the criticality and sensitivity of enterprise data (e.g., public, confidential, top secret). This scheme should define the security levels and appropriate protection controls and should address data retention and destruction requirements. Many organizations find it useful to associate confidential data types to the laws and regulations that govern them, as part of the classification.\textsuperscript{23}

**Information Security**

This is typically a high-level policy that describes the purpose of information security efforts: to maintain confidentiality, integrity, and availability of data. This is the core policy of an information security management system (ISMS) and is typically supported by a series of supplemental policies that focus on specific areas, such as acceptable use, access control, change management, and disaster recovery.

**Privacy**

This policy describes the practices followed by the organization when it comes to managing the lifecycle of customer data as it relates to privacy—that is, the retention, processing, disclosing, and deleting of customers’ personal data. The content of the policy will vary depending on the applicable legal framework, which in turn will vary depending on factors such as industry and geography.

**Data Stewardship**

This policy documents the role and responsibilities of personnel designated as data stewards. Data stewards are responsible for ensuring effective control and use of data assets and exercising a series of functions assigned to them by the data governance organization. Additional details on the data steward’s role and responsibilities are provided in the second paper in this series.

**Conclusion**

Public and private entities must contend with multiple information security and privacy threats. Citizen and consumer perception of what organizations should do to protect their personal information is evolving. Threats

\begin{itemize}
\item \textsuperscript{20} GAPP: [http://infotech.aicpa.org/Resources/Privacy/Generally+Accepted+Privacy+Principles](http://infotech.aicpa.org/Resources/Privacy/Generally+Accepted+Privacy+Principles).
\item \textsuperscript{22} ISO/IEC 27001/27002: [www.27000.org](http://www.27000.org).
\item \textsuperscript{23} See suggestions for data classification in part 2 of this whitepaper series.
\end{itemize}
against, and concerns about, the consequences of data breaches and general loss of confidential information are driving the enactment of new laws, regulations, and, in some cases, compulsory industry standards.

Enlightened organizations are adopting a holistic approach to meet these threats and challenges, one that involves the participation of multiple groups such as legal, HR, finance, IT, and others to do the following:

- Define policies, roles, and responsibilities for the management, use, and protection of confidential data
- Adopt measures that simultaneously address or otherwise consider privacy and security threats as well as compliance requirements
- Implement rigorous risk management processes for the use and protection of confidential data
- Ensure compliance with appropriate laws, regulations, standards, and organizational policies and generate proof of that compliance

DGPC can offer organizations the means to create the appropriate organizational context for implementing these processes.

In the next paper of the series, “A Guide to Data Governance for Privacy, Confidentiality and Compliance, Part 2: People and Process,” we will review the process component of the framework in greater detail. We will also look at the people component: the virtual team that is required in order to support the process.
**Glossary of Terms**

**assertion**  Statement made by an organization describing a component of the business.

**attestation**  Auditor statement/opinion as to whether the assertion is true.

**authority document**  Any document containing control requirements applicable to an organization, including but not limited to governance, standards, and contractual requirements.

**control objective (CO)**  A goal statement designed to reduce or eliminate risk or meet one or more requirements. It is a breakdown, translation, and harmonization of high-level requirements in the authority documents.

**control activity (CA)**  Any activity that helps with validation if a CO is met and provides guidance on how to achieve that CO. The validation could be manual assertion/signoff or automated using various strategies such as checking to see if a policy exists, if configuration complies with policy, if the audit event stream meets certain requirements, or if a set of properties of some managed entities meets constraints.

**control failure**  The measured failure of a major CO through observation by an auditor, with major repercussions to the organization.

**corrective action**  The recommendation to fix a discovered incident or problem affecting control compliance.

**data governance**  The exercise of authority, control, and shared decision making (planning, monitoring, and enforcement) over the management of data assets.  

**data protection**  The management of personal information. In the United States, “privacy” is the term that is used in policies, laws and regulations. However, in the European Union and other countries, the term “data protection” often identifies privacy-related laws and regulations.

**data steward**  A business leader or subject matter expert who is accountable for 1) the identification of operational and business intelligence data requirements within an assigned subject area, 2) the quality of data names, business definitions, and domain values within an assigned subject area, 3) compliance with regulatory requirements and conformance to internal data policies and data standards, 4) application of appropriate security controls, 5) analyzing and improving data quality, and 6) identifying and resolving data related issues.

**GRC**  Governance, Risk Management, and Compliance.

- **Governance** ensures that the business focuses on core activities, clarifies who in the organization has the authority to make decisions, determines accountability for actions and responsibility for outcomes, and addresses how expected performance will be evaluated. All of this happens within a clearly

---


defined context that might span a division, the entire organization, or a specific set of cross-discipline functions.

- **Risk management** is a systematic process for identifying, analyzing, evaluating,remedying, and monitoring risk. As a result of this process, an organization or group might decide to mitigate a risk, transfer it to another party, or assume the risk along with its potential consequences.

- **Compliance** generally refers to actions that ensure behavior that complies with established rules as well as the provision of tools to verify that compliance. It encompasses compliance with laws as well the enterprise’s own policies, which in turn can be based on best practices. Compliance requirements are not static, and compliance efforts should not be either.

**personal data** Any and all data that relates to an identifiable individual.\textsuperscript{26}

**personally identifiable information (PII)** Any information that can be traced to a particular individual. Usually a set of identifiable information is identified through an identification block of data, such as a name, mailing address, phone number, social security number, or e-mail address. Personal user preferences tracked by a Web site via a cookie are also considered personally identifiable when linked to other personally identifiable information provided by a user online.\textsuperscript{26}

**personal information** Any information that (i) relates to an individual and (ii) identifies or can be used to identify the individual. Such information may include an individual’s name, postal address, e-mail address, telephone number, Social Security number, or other unique identifier.\textsuperscript{26}

**privacy** The appropriate use of personal information under the circumstances. What is appropriate will depend on context, law, and the individual’s expectations. Privacy also refers to the right of an individual to control the collection, use, and disclosure of personal information.\textsuperscript{26}

**sensitive personal information/ sensitive data** The 1998 EU Directive distinguishes between ordinary personal data, such as name, address, and telephone number, and sensitive personal data, such as racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, and criminal convictions. Under the act, the processing of sensitive data is subject to stricter conditions.\textsuperscript{26}

\textsuperscript{26} IAPP Information Privacy Certification: Glossary of Common Privacy Terminology, International Association of Privacy Professionals (IAPP), 2006.
References


Generally Accepted Privacy Principles, American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA), http://infotech.aicpa.org/Resources/Privacy/Generally+Accepted+Privacy+Principles.


OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Organization for Economic Cooperation and Development, www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

Platform for Privacy Preferences (P3P), World Wide Web Consortium (W3C), 2007. www.w3.org/P3P.