Trustworthy Computing

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

Part 2: People and Process

January 2010

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.
## Contents

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

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

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

People ....................................................................................................................................... 5

Executive Management ............................................................................................................ 6

The Data Governance Organization .......................................................................................... 7

Process ....................................................................................................................................... 10

Guiding Principles for DGPC Core Processes .......................................................................... 12

Manage DGPC Organization ...................................................................................................... 12

Manage DGPC Requirements .................................................................................................... 14

Manage DGPC Strategy and Policies ......................................................................................... 15

Manage DGPC Control Environment ......................................................................................... 19

Conclusion .................................................................................................................................. 21

Glossary of Terms ....................................................................................................................... 22

References .................................................................................................................................. 24
Executive Summary

The past decade has produced an unprecedented accumulation of data. Organizations in general and business models in particular increasingly rely on 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 enterprises 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 is the second whitepaper in the series titled “A Guide to Data Governance for Privacy, Confidentiality, and Compliance.” In it, we examine the core capabilities related to people and process that are required to enable data governance for privacy, confidentiality, and compliance (DGPC). For the people component, we conclude that effective governance requires an appropriate DGPC framework with clearly defined roles and responsibilities, sufficient resources to perform assigned duties, and clear guidance on the overall goals and objectives of the program. For the process component, we look at the four core processes and associated key activities, inputs, outputs, and responsible participants in 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 in place, as well as successful privacy and risk management efforts. 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

In approaching 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, state-of-the-art industry best practices, and self-regulation measures that go beyond mere compliance with the letter of regulations and standards.

---

1 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); 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](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.

The first paper in the series analyzes the data privacy and security challenges that organizations face today, including an increasingly complex regulatory environment. It also looks at the concept of data governance and how it can complement ongoing efforts within the organization.

In this paper, we look at capabilities that an organization must develop as part of a data governance for privacy, confidentiality and compliance (DGPC) initiative. We then analyze two of these areas, People and Process, in detail and discuss how they interact with each other to enable DGPC.

Other papers in the series will:

• 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 those 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

In the first paper in this series, “A Guide to Data Governance for Privacy, Confidentiality and Compliance. Part 1: The Case for Data Governance,” we advocate a DGPC approach for organizations to meet today’s data security and privacy challenges. We now begin to look at what we call the DGPC framework, or simply “the framework,” as a vehicle to implement this approach.

Figure 1 shows the three main elements, or core capability areas, of the DGPC framework: People, Process, and Technology. Each area comprises specific capabilities that, when implemented successfully, contribute to the desired outcomes.

**Figure 1. Data Governance for Privacy, Confidentiality and Compliance (DGPC) core capability areas and outcomes.**

- **People:** The organization and roles and responsibilities involved in an effective DGPC effort.
- **Process:** How the different roles in the DGPC effort come together to manage risk related to data privacy and confidentiality and define appropriate policies.
- **Technology:** Analysis tools for evaluating risks and the technical and manual controls and technologies for mitigating those risks. This area is addressed in detail in the third paper in the series, “A Guide to Data Governance for Privacy, Confidentiality, and Compliance. Part 3: Managing Technological Risk.”
The fourth paper in the series examines how to evaluate an organization’s maturity and progress in these core capability areas.

**People**

The most important core capability area is People. Processes and technology can only be as effective as the people who use and manage them. Effective governance requires an appropriate organizational structure with clearly defined roles and responsibilities, enough resources to perform required duties, and clear guidance on the overall goals and objectives for DGPC.

The DGPC framework we propose must be tailored to each organization’s unique circumstances—including its size, industry, and location—but the following statements should hold true in most cases:

- The People core capability area does not constitute an entirely new DGPC organization. Rather, it brings together existing capabilities and new capabilities. The DGPC effort should function as a virtual team within the existing organization.
- In a virtual DGPC team, very few people should be needed to manage the overall process, and only in large organizations will anyone need to be dedicated to the effort full time.

The People component of the DGPC framework is depicted in Figure 2. The layers of the pyramid are as follows:

- **Executive Management.** The role of executive management is *strategic* in nature. Some organizations have a governance, risk management, and compliance (GRC) council that oversees organization-wide GRC issues and whose support and involvement are essential to the success of DGPC activities. They provide the vision and top leadership for DGPC. If a large organization does not have a GRC council, it might want to create one. Smaller organizations might want to merge the top and middle layers of the pyramid.

- **Data Governance Organization.** The data governance organization—steering committees and working groups—provides oversight for DGPC. It assumes the *tactical* role of data stewardship and is responsible for creating and managing the DGPC principles, policies, standards, and procedures.

- **Workforce and Trusted Business Partners.** At the *operational* level, principles, policies, standards, and procedures are communicated to the organization’s workforce and trusted business partners. As data collectors and consumers, employees and partners are accountable for adhering to those principles, policies, standards, and procedures. Trusted business partners are external entities that maintain a contractual working relationship with the organization and are entrusted with access to the organization’s data assets.
Note that the DGPC structure does not replace existing mechanisms, groups, or officers with responsibilities for security (CISO/CSO), privacy (CPO or Privacy Office), or risk management (CRMO or RM Office). Instead, these should be represented in the DGPC structure, as should other relevant groups such as Legal, HR, and business units. Further discussion of the roles and responsibilities at each layer of the pyramid follows.

**Executive Management**

Senior leadership should designate an executive-level leader for GRC. This leader could be the executive who is currently responsible for enterprise risk management or corporate compliance (e.g., a risk officer or compliance officer). It is important to choose someone who has more of a business than an IT focus because compliance programs typically need business-directed funding to be successful. Designation of a lead with this level of authority for GRC demonstrates executive management’s concern about, and commitment to, the effort. This communicates a positive “tone at the top” message to the rest of the organization—a critical first step for acceptance of upcoming changes.

The executive GRC leader should serve as the chair of the GRC council and guide the council through definition of a charter and objectives that are aligned with the organization’s business strategy. The GRC leader also leads the council in the execution of its assigned duties and ensures that the senior leadership of the organization remains engaged in overall GRC efforts.

One of the main goals of the council is to ensure that all GRC-related matters are addressed in a timely and effective fashion. Thus, the council is responsible for communicating the list of relevant authority documents.
and the initial list of integrated (high-level) DGPC requirements to the steering committee (discussed later in this section).

The GRC council should include leaders from a cross-section of business units and other groups that have knowledge relevant to, and whose businesses will be affected by, the council’s decisions. It might include leaders from law and corporate affairs, human resources, corporate compliance, corporate risk management, finance, sales, operations, IT, security, privacy, and business units. GRC council members must clearly understand GRC-applicable authority documents (company policies and objectives, laws and regulations, and so on) in their respective business areas. They are also responsible for ensuring that those authority documents become part of the integrated GRC requirements and that their requirements are addressed by the DGPC strategy. Finally, council members are responsible for assigning data stewards\(^3\) from their respective groups to serve as members of a DGPC steering committee.

**The Data Governance Organization**

The data governance organization consists of steering committees and focused working groups. Figure 3 depicts examples of such an organization in a large and mid-size company.

**Steering Committees**

DGPC steering committees set the plans, objectives, and performance measures for the DGPC effort and prioritize urgent business needs.

\(^3\) Data stewards will be discussed later in this paper.
Larger organizations will tend to have multiple steering committees that are involved in activities related to information security and privacy:

- DGPC
- Privacy
- Information Security
- Compliance

A large organization with a comprehensive enterprise data governance (EDG) program might create a DGPC steering committee as a branch of the EDG steering committee. In smaller organizations or those that are just getting started on the road to data governance, the EDG and DGPC steering committees might be one and the same. Alternatively, these organizations might choose to assimilate the DGPC steering committee function into existing privacy and information security committees.

In general, data governance steering committees are composed of data stewards. Data Management International (DAMA), an independent industry association, defines the role of data steward as follows:

Data stewardship is the formal accountability for business responsibilities that ensure effective control and use of data. A data steward is a business leader or subject matter expert (SME)
A Guide to Data Governance for Privacy, Confidentiality, and Compliance

designated as accountable for these responsibilities. Data stewards are responsible for protecting, managing, and leveraging the data for which they are entrusted.\(^4\)

In the normal course of the DGPC process, data stewards are needed to make decisions on their respective access control profiles (who can access what), disaster recovery requirements (how quickly their data and system need to be recovered after a disaster), policy-compliant use of data, and other tasks related to data management.

In most cases, these responsibilities will already be assumed by one or more people within the organization, but not formally. It is natural, and in most cases desirable, to enlist these people as formal data stewards since they already perform these duties. Formalizing their role also recognizes their competence in managing data assets in the best interests of the organization. Care should be taken, however, to ensure that these key people are not overwhelmed with multiple competing roles. More information about the role of data steward can be found in *The DAMA Guide to the Data Management Body of Knowledge* (www.dama.org/i4a/pages/index.cfm?pageid=3364) and on the Web sites of the Data Administration Newsletter (www.tdan.com) and the Data Governance Institute (www.datagovernance.com).

The CIO should designate members of the IT leadership team to participate in the DGPC steering committee so appropriate technology solutions can be developed and implemented. At the same time, IT leaders—from information security, architecture, engineering, application development, operations, or service management areas—should identify and address technological constraints that might affect solution development and implementation. IT can also help identify data steward candidates by examining their portfolio of application systems and databases.

The DGPC steering committee supports the GRC council by developing policies, standards, and procedures that address GRC requirements and follow DGPC strategy. These are presented to the GRC council for review and approval.

**Focused Working Groups**

The DGPC steering committee is also responsible for forming focused working groups, which consist of subject matter experts from different areas of the organization. These experts collaborate to develop a comprehensive set of process and technical controls in support of approved policies, standards, and procedures. For example, to address PCI-DSS compliance requirements, the steering committee might assemble a focused working group consisting of subject matter experts from legal, finance, IT, and internal audit departments, as well as appropriate data stewards. Working group responsibilities also include transition plans and ensuring that affected workforce and business partners are informed about impending changes.

**Workforce and Trusted Business Partners**

The organization’s workforce and trusted business partners operate under the implemented process and technical controls. As collectors and consumers of the data, they are responsible for using and handling it in

---

accordance with DGPC policies, standards, and procedures. They are also responsible for reporting any issues or violations to the DGPC steering committee.

Internally and with partners, effective communication and education are essential. Success cannot be achieved if participants are not aware of their role and responsibilities within the DGPC effort. Affected individuals should, at the very least, receive training that helps them understand the rationale behind the changes and their individual obligations, as defined by the DGPC organization.

Process

The Process area addresses the type and flow of activities involved in the DGPC effort. Figure 4 expands on the DGPC process diagram introduced in the first paper in this series and illustrates the four core processes within this area, along with the corresponding inputs and outputs.

- **Manage DGPC Organization.** This process ensures that the appropriate DGPC organizational structure is in place to support the other core processes.

- **Manage DGPC Requirements.** This process examines various GRC authority documents to rationalize business data requirements (including data quality metrics and business rules) and data compliance requirements and to create integrated GRC guidance. Integrated GRC requirements feed into the next process—managing strategy and policies.

- **Manage DGPC Strategy and Policies.** This process develops DGPC strategy, principles, and policies that align with the integrated GRC requirements and authority documents. Resulting output serves as input to the final process—managing the DGPC control environment.

- **Manage DGPC Control Environment.** This process applies the DGPC tools and techniques (described in the third paper in this series) to identify appropriate controls and technologies for implementation. It includes a feedback loop to adjust DGPC strategy and policies based on how well the controls are performing.
As mentioned earlier, the core processes must be adapted to each organization’s unique circumstances and needs.
Guiding Principles for DGPC Core Processes

To design, develop, and implement efficient and effective DGPC practices, organizations must define a set of guiding principles that can be applied in each core process. These principles include, but are not limited to, the data privacy and confidentiality principles discussed in the first paper in this series.5

- **Adhere to the Data Privacy and Confidentiality Principles:**
  - Honor policies throughout the confidential data lifespan.
  - Minimize risk of unauthorized access or misuse of confidential data.
  - Minimize impact of confidential data loss.
  - Document applicable controls and demonstrate their effectiveness.

- **Apply continuous process improvement methodologies.** DGPC processes should always be viewed from a lifecycle management perspective. The typical lifecycle of a process involves planning, designing, testing, implementing, monitoring, measuring, and refining. Continuous process improvement ensures that a process operates efficiently and effectively and does not become a burden to the organization. Some examples of continuous process improvement methodologies include the Deming PDCA Cycle (Plan-Do-Check-Act), Six Sigma, and Lean. These methodologies help identify deficiencies in a process and evaluate the effectiveness of corrective measures.6

- **Keep each process structured, manageable, and repeatable.**
  - Complex processes are difficult to manage. Typically, a complex process attempts to address too many functions. As a result, it requires significant coordination of participants, activities, inputs, outputs, and resources. Simplifying and breaking it down into smaller, more focused processes and functions will make things more manageable.
  - A process comprising activities that are not clearly defined will create confusion to those involved. Processes should be structured and defined so that involved parties can follow it easily.
  - A process should be designed to be easily repeatable so it can produce consistent results every time it is executed.

Manage DGPC Organization

As mentioned earlier, a DGPC structure might consist of the GRC council, DGPC steering committees, and multiple focused working groups. An overall process is needed to manage the formation of these committees and the definition of their purposes, objectives, and relationships to one another. For example, the GRC council’s charter might be simply this: “To provide assurance that governance, risk, and compliance matters are being managed to meet a standard of due care.” The goals and objectives of committees and working groups must align with and support that charter.

---

Key activities for managing the DGPC effort are listed in Table 1. This is not a definitive or exhaustive list; organizations should adjust it based on their unique culture, structure, and resource constraints. In any case, at the end of the cycle, activities should be repeated in support of a lifecycle process.

**Table 1. Manage DGPC Organization: Key Activities**

<table>
<thead>
<tr>
<th>No.</th>
<th>Activity</th>
<th>Input</th>
<th>Output</th>
<th>Responsible Party</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Appoint executive leader to GRC council and define role and responsibilities</td>
<td>List of executive leader candidates</td>
<td>GRC council executive leader’s role and responsibilities</td>
<td>Enterprise senior leadership team</td>
</tr>
<tr>
<td>2.</td>
<td>Define GRC council charter</td>
<td>Business strategy</td>
<td>GRC council charter</td>
<td>Enterprise senior leadership team</td>
</tr>
<tr>
<td>3.</td>
<td>Appoint GRC council members and define role and responsibilities</td>
<td>List of GRC council member candidates</td>
<td>GRC council members’ role and responsibilities</td>
<td>Enterprise senior leadership team</td>
</tr>
<tr>
<td>4.</td>
<td>Define GRC council goals and objectives</td>
<td>GRC council charter</td>
<td>GRC council goals and objectives</td>
<td>GRC council</td>
</tr>
<tr>
<td>5.</td>
<td>Appoint DGPC steering committee members</td>
<td>List of steering committee member candidates (data stewards)</td>
<td>DGPC steering Committee members’ role and responsibilities</td>
<td>GRC council</td>
</tr>
<tr>
<td>6.</td>
<td>Define DGPC steering committee goals and objectives</td>
<td>GRC council goals and objectives</td>
<td>DGPC steering committee goals and objectives</td>
<td>DGPC steering committee</td>
</tr>
<tr>
<td>7.</td>
<td>Create focused working groups</td>
<td>DGPC steering committee goals and objectives</td>
<td>Focused working groups</td>
<td>DGPC steering committee</td>
</tr>
<tr>
<td>8.</td>
<td>Appoint focused working group members</td>
<td>List of focused working group member candidates</td>
<td>Focused working group members’ role and responsibilities</td>
<td>DGPC steering committee</td>
</tr>
<tr>
<td>9.</td>
<td>Define focused working group goals and objectives</td>
<td>DGPC steering committee goals and objectives</td>
<td>Focused working group goals and objectives</td>
<td>Focused working groups</td>
</tr>
<tr>
<td>10.</td>
<td>Report focused working group performance to DGPC steering committee</td>
<td>Performance status of focused working group and</td>
<td>Focused working group status report</td>
<td>Focused working groups</td>
</tr>
</tbody>
</table>
Manage DGPC Requirements

Each level of the DGPC structure has a role and responsibility for managing various aspects of the DGPC requirements. Table 2 lists key management activities.

Table 2. Manage DGPC Requirements: Key Activities

<table>
<thead>
<tr>
<th>No.</th>
<th>Activity</th>
<th>Input</th>
<th>Output</th>
<th>Responsible Party</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Translate business strategy into general DGPC requirements</td>
<td>• Business strategy</td>
<td>Combined general DGPC requirements</td>
<td>GRC council</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• External laws, regulations, and standards</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Translate combined general DGPC requirements into business data and compliance requirements</td>
<td>General DGPC requirements</td>
<td>Business data (quality) and compliance requirements</td>
<td>DGPC steering committee</td>
</tr>
<tr>
<td>3.</td>
<td>Identify and assemble GRC authority documents</td>
<td>• Business data (quality) and</td>
<td>Compilation of GRC authority documents</td>
<td>Focused working groups</td>
</tr>
</tbody>
</table>
Perhaps the most critical step in managing DGPC requirements is the integration of relevant GRC authority documents into a single, coherent set of requirements. In addition to business data requirements (including data quality metrics and business rules), this step looks at control frameworks, standards, and legal compliance authority documents (e.g., SOX, HIPAA, PCI-DSS, CA SB1386, MA 201, EUDPD 95/46/EC compliant country laws, Val IT, COBIT, and ISO/IEC 27001) to ensure that redundant or duplicate compliance requirements are consolidated and rationalized. The result is a unified, or “harmonized,” set of integrated GRC requirements.

One helpful tool for this rationalization and consolidation process is the Unified Compliance Framework (UCF). The UCF maps numerous authority documents (regulations, control frameworks, and standards) into a set of common control objectives, which can then be combined with business requirements to form harmonized GRC guidance for the organization. An example of harmonization is described in the “Microsoft Compliance Framework for Online Services,” which offers an overview of how compliance requirements for Microsoft’s online services infrastructure are harmonized.

Organizations should implement a routine review cycle of the activities in the Manage DGPC Requirements process to address changes in regulations and business strategy demands. In other words, all of the activities must be performed repeatedly, on a scheduled basis or as changing business needs demand.

### Manage DGPC Strategy and Policies

This process develops and maintains the DGPC strategy and policies that are based on the harmonized GRC requirements developed in the previous process. The key activities in this process are listed in Table 3.

---

7 Unified Compliance Framework (UCF), [www.unifiedcompliance.com](http://www.unifiedcompliance.com).

DGPC Strategy

The GRC council is responsible for drafting the DGPC strategy based on the requirements derived from GRC authority documents with corresponding business strategy inputs. The DGPC strategy should have the following elements:

- DGPC goals, objectives, and benefits. For example, one DGPC goal might be to ensure that policies are in place to support the integrated GRC requirements. The objectives would be to define the policies and the associated management processes. The benefits would be policies that are relevant, effective, and enforceable.
- The four DGPC principles (described earlier in this section).
- A short- to long-term roadmap of the people, processes, technologies, and activities required to achieve the DGPC goals, objectives, and benefits.
- An estimate of resources (time, people, and technologies) required to develop and support the activities and capabilities.
- Metrics to measure the status of strategy execution, such as tracking of actual versus estimated time and costs to achieve the stated objectives.

The GRC council presents a draft of the DGPC strategy to the enterprise senior leadership team for review and approval. If necessary, adjustments to the strategy are made based on the feedback received. The DGPC strategy is subsequently communicated to the DGPC steering committee for execution.

Table 3. Manage DGPC Strategy and Policies: Key Activities

<table>
<thead>
<tr>
<th>No.</th>
<th>Activity</th>
<th>Input</th>
<th>Output</th>
<th>Responsible Party</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Develop/refine DGPC strategy</td>
<td>Integrated GRC authority documents</td>
<td>DGPC strategy draft</td>
<td>GRC council</td>
</tr>
<tr>
<td>2.</td>
<td>Review and approve DGPC strategy</td>
<td>DGPC strategy draft</td>
<td>Approved DGPC strategy</td>
<td>Enterprise senior leadership team</td>
</tr>
</tbody>
</table>
| 3.  | Develop/refine DGPC policies          | • Approved DGPC strategy
                                           • Integrated GRC authority documents    | Draft of relevant DGPC policies  | • DGPC steering committee
                                           • Focused working groups                |                                  |
<p>| 4.  | Review and approve DGPC policies      | Draft of relevant DGPC policies            | Approved DGPC policies        | GRC council                              |
| 5.  | Implement approved DGPC policies      | Approved DGPC policies                     | Published DGPC policies       | DGPC steering committee                   |
| 6.  | Monitor and report on DGPC            | DGPC policy                                | DGPC policy                   | Focused working groups                   |</p>
<table>
<thead>
<tr>
<th>No.</th>
<th>Activity</th>
<th>Input</th>
<th>Output</th>
<th>Responsible Party</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>policy compliance</td>
<td>compliance metrics</td>
<td>compliance scorecard</td>
<td>groups</td>
</tr>
<tr>
<td>7.</td>
<td>Review and respond to DGPC policy compliance scorecard</td>
<td>DGPC policy compliance scorecard</td>
<td>DGPC policy compliance action plan</td>
<td>DGPC steering committee</td>
</tr>
</tbody>
</table>
| 8.  | Implement DGPC policy compliance action plan | DGPC policy compliance action plan | Corrective actions | • DGPC steering committee  
• Focused working groups |

**DGPC Policies**

The DGPC steering committee can work in partnership with the focused working groups to identify, develop, or refine the DGPC policies that directly support the DGPC strategy. The main policies are:

- **Data Stewardship.** This policy documents the role and responsibilities of data stewards, who are responsible for ensuring effective control and use of data assets according to data security and privacy requirements. As such, the policy should also address how to measure the data stewards’ performance.

- **Data Classification.** This policy establishes an enterprise-wide classification scheme that defines appropriate security levels and protection controls, data retention policies, and criticality and sensitivity of enterprise data (e.g., public, confidential, top secret). Tagging confidential information covered by statutes and regulations with the associated authority document is also a good idea. The classification scheme should apply to both structured and unstructured data.

The key to an effective classification policy is to keep the classification scheme simple. For most organizations, the following three levels of classification will suffice:

- **Public:** Information generally made available to the public. This is information that has a low impact on the business.

- **Internal Use Only:** Information intended for use within the organization and not for public distribution. This information might be shared with external entities that have a contractual working relationship with the organization. This category of information has a moderate impact on the business. It is intended for limited use under the terms of a business arrangement (e.g., consent from the asset owner for limited disclosure to specified groups of employees and/or approved non-employee agents).

- **Restricted/Confidential:** Information that is intended only for a subset of groups, departments, or divisions within an organization. This information has a high impact on the business. Examples include information subject to specific regulatory or industry requirements (such as GLBA, HIPAA, CA SB1386, PCI DSS, and laws that comply with the EU Data Protection Directive).
In addition to using this classification scheme, it is good practice to associate confidential data with specific laws and regulations that govern it. That is, some data might be classified as Restricted/Confidential as well as “PII/GLBA,” or “sensitive data/EUDPD.”

Keeping the classification scheme simple also allows for simple treatment requirements and controls at each classification level. This enables IT to more easily translate and implement the controls in the technology infrastructure—for instance, to automate the data classification policy controls.

Some control frameworks and industry standards provide alternative information classification schemes:

- **Information Security**: Typically a high-level policy that describes the purpose of information security—to maintain the confidentiality, integrity, and availability of confidential information. This policy is supported by a series of supplemental policies that focus on areas such as acceptable use, access control, change management, data integrity, and backup/disaster recovery. A standard reference model to use for developing information security policies is the ISO/IEC 27002 Code of Practice for Information Security.

- **Privacy**: A policy containing practices to ensure that personal data is collected and used according to applicable privacy laws. It also describes specific rights of data subjects (individuals and other entities) afforded by law or by decision of the GRC council, the DGPC steering committee, or the business itself.

Most organizations already have these policies in some form or another. As a result, the process generally requires identifying, collecting, and updating these policies as necessary and aligning them with the DGPC strategy. Each policy should clarify the following basic elements:

- Purpose of the policy.
- Policy statement.
- Whom the policy affects and their associated role and responsibilities.
- How the policy will be monitored for compliance (metrics and related key performance indicators).
- What enforcement actions will be taken against policy violators.

To measure the effectiveness of a policy, compliance metrics should be collected and reported in the form of a scorecard. Significant noncompliance indicates that the policy might need to be adjusted. The DGPC steering committee is responsible for reviewing scorecards and creating compliance action plans to correct the root causes of issues. Finally, as part of the implementation of these policies, the DGPC steering committee should develop a communication plan to prepare all affected parties.

---


Manage DGPC Control Environment

This process formulates DGPC process and technical controls according to the DGPC strategy and policies. These controls generally consist of standards and procedures that directly support each policy, as well as the associated control objectives from the harmonized GRC requirements.
Table 4 lists the key activities involved.

In this process, the focused working groups formulate the necessary control standards and procedures. The result is a controls matrix that maps standards and procedures to the control objectives—aided by DGPC tools and techniques to help define auditing and reporting mechanisms. The third paper in this series offers further details on these tools and techniques.

The DGPC steering committee reviews and approves the proposed control standards and procedures and the controls matrix. The focused working groups make any recommended adjustments and create a controls implementation plan that outlines the activities, schedule, and resources required. Larger organizations might enlist their project management office to assist in developing this plan. The proposed plan is presented to the DGPC steering committee for review and approval. After making any recommended adjustments, the focused working group executes the plan.

Once the controls have been implemented successfully and transitioned to a business-as-usual state, monitoring and reporting activities begin. These include testing and validating infrastructure security as well as measuring and monitoring data quality. A controls effectiveness scorecard is generated periodically to report on controls compliance, enforcement, and effectiveness. The DGPC steering committee reviews the scorecard and develops a plan to correct any deficient controls. The affected focused working group is responsible for implementing the corrective actions. In terms of data quality, procedures should be in place to clean and correct data quality defects.

Whenever changes are made to the DGPC strategy, integrated GRC requirements, or DGPC policies, the activities in this process should be repeated from the start.
### Table 4. Manage DGPC Control Environment: Key Activities

<table>
<thead>
<tr>
<th>No.</th>
<th>Activity</th>
<th>Input</th>
<th>Output</th>
<th>Responsible Party</th>
</tr>
</thead>
</table>
| 1.  | Formulate process controls and technical controls | • Approved DGPC strategy  
• Integrated GRC authority documents  
• Published DGPC policies  
• Gap analysis matrix | Control standards and procedures (controls matrix) | Focused working groups           |
| 2.  | Review and approve proposed control standards and procedures | Control standards and procedures (controls matrix) | Approved control standards and procedures (controls matrix) | DGPC steering committee     |
| 3.  | Develop controls implementation plan          | • Approved DGPC strategy  
• Approved control standards and procedures (controls matrix) | Controls implementation plan | Focused working groups      |
| 4.  | Review and approve controls implementation plan | Controls implementation plan | Approved controls implementation plan | DGPC steering committee     |
| 5.  | Implement approved control standards and procedures | • Approved controls implementation plan  
• Approved control standards and procedures (controls matrix) | Implemented control standards and procedures | Focused working groups      |
| 6.  | Monitor and report on effectiveness of controls | Control standards and procedures metrics | Controls effectiveness scorecard | Focused working groups      |
| 7.  | Review and respond to controls effectiveness Scorecard | Controls effectiveness Scorecard | Controls effectiveness action plan | DGPC steering committee     |
| 8.  | Implement controls effectiveness action plan  | Controls effectiveness action plan | Corrective actions | Focused working groups      |
Conclusion

In the DGPC framework, the People core capability area helps organizations understand the capabilities needed to determine how best to implement the DGPC effort. It should not be necessary to create a new group within the organization to carry out DGPC objectives—a virtual team within the larger organization should be enough.

Organizations can successfully implement and manage the Process capabilities by adapting the four core processes of the framework to fit into their environment:

- **Manage DGPC Organization**: Ensuring that the appropriate DGPC structure is in place to support the remaining core processes

- **Manage DGPC Requirements**: Examining the various GRC authority documents to rationalize business data requirements and data compliance requirements and to create harmonized GRC guidance

- **Manage DGPC Strategy and Policies**: Ensuring that the DGPC strategy, principles, and policies are developed in alignment with the GRC requirements and authority documents.

- **Manage DGPC Control Environment**: Using DGPC tools and techniques to define appropriate controls and select relevant technologies

From the outset, DGPC efforts must be aligned with and linked to the organization’s business strategy and initiatives. This will demonstrate the value of the effort and justify the need for funding. Further, given that business needs and regulatory demands are dynamic, the DGPC strategy should be flexible enough to adapt to change. Organizations should therefore review and refine the DGPC strategy and principles on an ongoing basis.
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 a manual assertion/signoff or an automated validation using 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.\footnote{The DAMA Dictionary of Data Management, 1\textsuperscript{st} Edition, 2008.}

data protection The management of personal information. In the United States, “privacy” is the term used in policies, laws and regulations. In the European Union and other countries, the term “data protection” is often used in reference to privacy-related laws and regulations.\footnote{IAPP Information Privacy Certification: Glossary of Common Privacy Terminology, International Association of Privacy Professionals (IAPP), 2006.}

data steward A business leader or subject matter expert who is accountable for 1) identifying 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.\footnote{The DAMA Dictionary of Data Management, 1\textsuperscript{st} Edition, 2008.}

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 as 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. \(^{14}\)

**personally identifiable information (PII)** Any information that can be traced to a particular individual. Usually a set of identifiable information is identified through a 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. \(^{15}\)

**personal information** Any information that relates to an individual and identifies, or can be used to identify, the individual. Such information might include an individual’s name, postal address, e-mail address, telephone number, Social Security number, or other unique identifier. \(^{15}\)

**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. \(^{15}\)

**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 than that of ordinary personal data. \(^{26}\)
References

COBIT 4.1 – PO2.3 Data Classification Scheme,
www.isaca.org/Content/NavigationMenu/Members_and_Leaders1/COBIT6/Obtain_COBIT/Obtain_COBIT.htm

Continuous process improvement methodologies:


DAMA Dictionary of Data Management, 1st Edition, 2008,
www.dama.org/i4a/pages/index.cfm?pageid=3345

www.dama.org/i4a/pages/index.cfm?pageid=3345

Data Administration Newsletter (TDAN), www.tdan.com

Data Governance Institute (DGI), www.datagovernance.com

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


Microsoft Compliance Framework for Online Services,

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

Unified Compliance Framework (UCF), www.unifiedcompliance.com