Surveying Data Governance Policy Models

Prepared for BCCAT by Plaid Consulting

March 2021

Surveying Data Governance Policy Models

Prepared for BCCAT by Plaid Consulting

BC COUNCIL ON ADMISSIONS & TRANSFER
Web/Email: bccat.ca | bctransferguide.ca | info@bccat.ca
Twitter: @bccat_org | @bctransferguide

Executive Summary

This report focuses on data governance at post-secondary institutions and related organizations. Data governance is the formal execution and enforcement of authority over the management of data and data-related assets (Seiner, 2014). Universities and colleges are increasingly relying "on data and analytics for everything from facilities management to developing and monitoring institutional strategic goals" (Reinitz, 2019). In addition, a growing portfolio of systems outside the traditional enterprise report system, organizational reliance on timely data, and demands from the public to interact digitally while maintaining security and privacy of personal data are creating increased pressure for organizations to review, and perhaps formalize, their data governance policies and processes.

This project consisted of three parts:

1. An overview of data governance at higher education institutions;
2. An overview of data access and privacy legislation in the context of higher education; and
3. A discussion of key considerations and recommendations for higher education institutions.

Part one, *Overview of Data Governance*, reviews the elements of data governance, the goals and motivations of data governance programs, and the implementation of data governance frameworks and maturity models in the context of higher education. Part two, *Overview of Data Access and Privacy Legislation* reviews relevant legislation from British Columbia and nine other provinces or territories. It also reviews Canadian national legislation, legislation in several American states, and Europe's General Data Protection Regulation (GDPR). This review looks primarily at public- and private-sector privacy legislation and public health-related legislation, with some mention of data governance legislation related to educational institutions.

In part three, the discussion section, we discuss the key considerations, insights, and recommendations for higher education organizations and institutions in relation to their data governance programs. Higher education institutions and organizations developing a data governance program should:

- Start small, typically with a pilot program,
- Ensure executive buy-in and leadership,
- Begin by considering how resources can be devoted to people, not software tools, to start,
- Leverage existing institutional structures and governance expertise,
- Consider intersections across various departments who may interact with data in varying ways.

We also discuss areas for future research, given the rapidly changing landscape of data governance in higher education.

Table of Contents

List of Figures

List of Tables

Methodology

This report has been informed by academic literature and articles related to data governance in the professional press, interviews with 14 institutions and organizations, and public-facing materials on institutional and organizational websites. Our research identified a variety of questions that are ultimately addressed in Part 1 of this work: what is data governance, what frameworks support it, how do we measure our effectiveness at it, and what kinds of organizational structures are common within the domain?

The organizational data governance scan consisted of three major pieces: video/telephone interviews with data governance representatives at selected organizations in BC and across North America; an analysis of organizations that posted information about their data governance programs/practices on the public internet; and an online survey. These are described in greater detail below.

Our method for selecting organizations to participate included identifying those with information available online; contacting those who self-identified in the online survey as interested in a follow up interview; and following recommendations from BCCAT staff and our own personal networks. We were not able to select a random sample of participants, and there are more participants from British Columbia (BC) than from other jurisdictions.

Table 1 shows the organizations that were interviewed between October 2019 and August 2020.

Table 1: Participating Institutions

Jurisdiction	Organization
Alberta	Alberta Post-Secondary Application Service (Apply Alberta)
British Columbia	British Columbia Institute of Technology Douglas College EducationPlannerBC Justice Institute of British Columbia Population Data British Columbia University of British Columbia
Ktunaxa Nation	British Columbia First Nations' Data Governance Initiative
Saskatchewan	University of Regina
Maritime Provinces	Maritime Provinces Higher Education Commission
Nova Scotia	Nova Scotia Council on Admissions and Transfer
Ontario	Ontario Universities Application Centre University of Ottawa
Quebec	Concordia University
United States of America	National Student Clearinghouse

Interviews were conversational in nature, rather than following a specific interview scheme. Appendix 2: Data Governance Interview Template presents the questions used to guide the interviews, but some organizations opted to directly share their story or have a conversation about data governance rather than use the template. All participants signed informed consent forms.

We reviewed data governance programs, frameworks, and practices that were posted on organization and institution websites. We identified organizational websites to review through web searches for data governance materials, with a focus on North American educational, government, and health organizations. This review was to ensure that we included perspectives from organizations that we may not have been able to interview.

The organizational policy and framework scan originally included a high-level online survey of data governance maturity for educational, governmental, and health organizations, which was launched on October 17, 2019. Promotions included through various trade organizations such as the Canadian Institutional Research and Planning Association (CIRPA), Canadian University and College Chief Information Officers (CUCCIO), the Pan-Canadian Consortium on Admissions and Transfer (PCCAT) data governance groups on LinkedIn and Twitter, through Plaid's various social channels, and shares by BCCAT.

Unfortunately, the online survey was unable to attract a large enough sample of respondents for the data to be included in subsequent analysis; therefore, the survey was closed on November 18, 2019. We thank those who took the time to fill in the survey and apologize that we were unable to include those data. The low number of responses may be due to:

1) data governance is often a shared responsibility, meaning that one individual may be uncomfortable completing the survey on behalf of their organization;

2) an online survey format may not lend itself well to understanding the nuances of data governance maturity; and,

3) the survey used a specific methodology (from the Data Management Body of Knowledge (DMBOK)) to assess the maturity of an organization's data governance structure. Our research suggests that most data governance maturity models are based on similar frameworks, but it is possible that our audience felt the survey wasn't ideally targeted. We feel that the survey instrument itself could be useful in furthering conversations about data governance within organizations. The instrument is presented in Appendix 3: Online Survey Instrument for this purpose.

While we included an array of academic literature, we did not conduct a full literature review, which may have provided further insight and analysis. We note that we have minimized the distinction between data management frameworks and data governance frameworks: most literature views data management as the set of architecture or tools needed to achieve data governance (Data Republic, 2019), which is the formal execution of authority over the management of data and data-related assets (Seiner, 2014). We felt delving into this nuance would render the report inaccessible for individuals just beginning their data governance journeys.

The second part of the project consisted of an in-depth review of data governance legislation, policy, and practices in British Columbia, and other Canadian and North American jurisdictions. The primary pieces of legislation and regulation that apply to data governance in higher education institutions are privacy and freedom of information acts, and higher education-related acts. We provide an overview of these pieces of legislation and their implications for post-secondary institutions (PSIs) in building their data governance programs. We reviewed publicly available legislation and regulations, and excluded any judicial precedents, except in cases where precedent is identified in the acts themselves or identified by a third party, such as the Office of the Privacy Commissioner of Canada. The pieces of legislation that were reviewed are presented in **Table 2**[1]:

[1] This legislative review was conducted in late 2019, prior to the impacts of COVID-19 becoming known. Several jurisdictions have since amended their legislation to enable additional remote work and cloud services on a temporary basis. These amendments are not reflected here.

Table 2: Legislation reviewed by type and jurisdiction

Province	Public Sector Act	Private Sector Act	Health Act
British Columbia	Freedom of Information and Protection of Privacy Act (1995)	Personal Information Protection Act (2003)	E-Health (Personal Health Information Access and Protection of Privacy) Act (2008)
Alberta	Freedom of Information and Protection of Privacy Act (2000)	Personal Information Protection Act (2003)	Health Information Act (2000)
Manitoba	The Freedom of Information and Protection of Privacy Act (1997)	Personal Information Protection and Electronic Documents Act (2000)	The Personal Health Information Act (1997)
New Brunswick	Right to Information and Protection of Privacy Act (2009)	Personal Information Protection and Electronic Documents Act (2000)	Personal Health Information Privacy Access Act (2009)
Newfoundland and Labrador	Access to Information and Protection of Privacy Act (2015)	Personal Information Protection and Electronic Documents Act (2000)	Personal Health Information Act (2008)
Nova Scotia	Freedom of Information and Protection of Privacy (1993)	Personal Information Protection and Electronic Documents Act (2000)	Personal Health Information Act (2010)
Northwest Territories & Nunavut	Access to Information and Protection of Privacy Act (1994)	Personal Information Protection and Electronic Documents Act (2000)	
Ontario	Freedom of Information and Protection of Privacy Act (1990)	Personal Information Protection and Electronic Documents Act (2000)	Personal Health Information Protection Act (2004)
Prince Edward Island	Freedom of Information and Protection of Privacy Act (1998)	Personal Information Protection and Electronic Documents Act (2000)	
Quebec	Act respecting access to documents held by public bodies and the protection of personal information (2019)	Act respecting the protection of personal information in the private sector (2019)	Act respecting the sharing of certain health information (2019)
Saskatchewan	The Freedom of Information and Protection of Privacy Act (1990-91)	Personal Information Protection and Electronic Documents Act (2000)	
Yukon	Access to Information and Protection of Privacy Act (2002)	Personal Information Protection and Electronic Documents Act (2000)	

Data Governance at Post-Secondary Institutions

Data governance has been increasing in prevalence in many sectors. Within higher education, data governance initiatives are relatively new, gaining traction over the last decade (Reeves & Pearlman, 2017). As post-secondary institutions find themselves dealing with larger pools of increasingly complex data, as well as greater data security and privacy concerns, data governance emerges as a more urgent topic. For this report, we have adopted the definition of data governance provided by Seiner (2014):

> Data governance is the formal execution and enforcement of authority over the management of data and data-related assets.

In this section, we discuss the current state of data governance in higher education, the elements of data governance, the goals and motivations for implementing data governance programs, and formal data governance programs and implementation.

Our research and interviews showed most BC post-secondary institutions are at least beginning to discuss data governance within their organizations. While most higher education organizations are in the early stages of developing data governance programs and initiatives, we have identified the University of British Columbia[2] and the University of Regina[3] as leaders in this area, based on the scope of their initiatives relative to their institutional size, and their willingness to share information on their websites, and through interviews.

Data governance consists of several elements, most of which are already embedded in the operations of higher education organizations and institutions (Seiner, 2014). In this section, we discuss the central elements involved in working with data, and the benefits of formalizing and defining processes, roles, responsibilities, and standards within these elements.

Roles and Responsibilities

Defining the roles and responsibilities of those working with data within an organization is a central consideration in the creation of data governance programs (Patil, 2015; Seiner, 2014). Commonly, these include data trustees, data stewards, data architects, data custodians, chief data officers, and end-users, each of which are described in the following section.

In most of our interviews, we found this was often one of the first steps an organization will take when establishing a formalized process. We found that while all participating institutions with a data governance program in place had defined roles for those working with organizational data, only one of the institutions *without* a data governance program had such definitions. We note that the definitions and titles of data roles vary across organizations, further emphasizing the need for clear, institution-wide definitions. One example of data governance roles at a Canadian post-secondary institution is from the University of Saskatchewan (n.d.a.), where the institution groups roles into the following:

---

2 The University of British Columbia data governance website (https://cio.ubc.ca/data-governance) is set to update in the Fall of 2020, after the completion of this report.

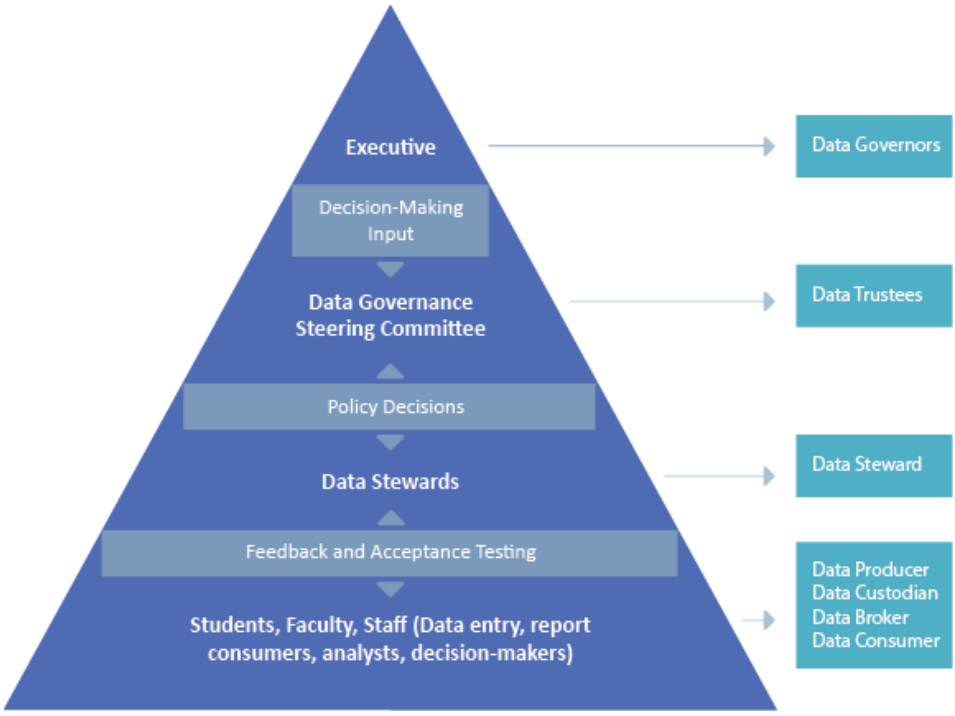
3 https://www.uregina.ca/orp/d-g/index.html

- Data Trustees - Highest-ranking individuals accountable for what happens with and to university (e.g. institutional, research, etc.) data.
- Data Stewards - Individuals who are responsible for promoting appropriate data use through planning, policy, and protocols at the university.
- Data Custodians - Individuals responsible for ensuring that policies are followed within a specific area and that local processes are consistent with university policies and procedures.
- Data Guardians - Individuals in IT who have operational level responsibility for data management activities related to the creation, storage, maintenance, cataloguing, use, dissemination, and disposal of data.
- Data Users - Individuals who access and use university data.

(University of Saskatchewan, n.d.a.)

A similar framework is used at the University of British Columbia, as shown in **Figure 1**.

Figure 1: Data Governance Roles at UBC



Source: University of British Columbia. "[Data Governance] Roles and Responsibilities" by University of British Columbia. n.d.b. (https://cio.ubc.ca/data-governance/people). Copyright n.d. by University of British Columbia. Reprinted with permission.

Data stewards define, implement, and enforce the accountability and responsibility of the organization's data stakeholders, and typically support regulatory compliance, internal policies, business goals, and the strategy and structure of the data governance program. Data stewards are "individuals who are responsible for promoting appropriate data use through planning, policy, and protocols at [an] institution" (Backscheider et al., 2015).

> *Data stewards provide university-level knowledge and understanding for a specific data area (e.g., student data, financial data, HR data, or alumni development data). Data stewards are responsible for data quality and data integrity, including consistent data definitions and their application throughout connected systems. They collaborate with other stewards to ensure that overlap areas (e.g., student employees and employees who are students) work across the board and that system updates are scheduled reasonably and tested appropriately. Data stewards work with security, privacy, and compliance officers to ensure that data are classified appropriately and that appropriate training is provided to users who will interact with data. Example stewards are the registrar and HR director.* (Backscheider et al., 2015, p3).

Data stewards can be identified by "the kinds of questions they might ask in a meeting, such as 'Why are those data important to the institution?' or 'How long do you think we should keep that record', or 'What can we do to improve the quality of this analysis?'..." (Backscheider et al., 2015, p.1). Those working with data, such as employees in institutional research or information technology, often operate informally as data stewards before the development of data governance frameworks, and usually inherit the role once data governance becomes formalized at their organization. Seiner (2014) remarks that "being a data steward describes a relationship to data and is not a position...[T]hose who define data as part of their jobs should have formal accountability for making certain that data are produced following the business rules" (p. 69-70).

Just as there are different roles working with data, there are often multiple data stewardship roles within organizations. These can include stewards for specific departments and faculties, stewards for different aspects of the data management process (collection, usage, access, security, etc.), or combinations of both. Further to this, data stewardship "supports the base for the continuance of the program beyond the initial implementation and ensures proper representation across the organization" (Patil, 2015, p. 9).

At Simon Fraser University, there are separate data stewardship committees for oversight of data related to administrative systems, educational systems, and research systems. A fourth umbrella committee facilitates the discussion of key emerging issues from all three areas. Data stewards at the University of British Columbia are operationally responsible for data quality, data governance activity, and issue resolution within their business area, and collaboration with other business areas.

Data governance literature suggests that the term 'data owner' typically refers to those whose roles include the authority to make decisions regarding internal data practices and policies. According to DAMA International's *Data Management Body of Knowledge*, "[a] Data Owner is a business Data Steward, who has approval authority for decisions about data within their domain" (p. 77).

Our research shows that while this term is commonly used in the private sector, it is not typically used in higher education. Instead, post-secondary institutions tend to use terms like 'data trustees' and 'data stewards'. Interviewees noted that their institutions have avoided using the term 'data owner' to avoid the suggestion that data is 'owned' by those in authority roles or by institutional departments. One interviewee suggested that the use of this term may promote the formation of data silos. The terms 'data trustees' and 'data stewards' were cited by interviewees as better representing the relationship between those with responsibility over data and those charged with data informed

decision-making. Data trustees are "the highest-ranking individuals accountable for what happens with and to data" (Backscheider et al., 2015, p.10), and "provide a broad, university-wide view of data, approve policies, resolve questions of procedure, and ensure that data plans are consistent with and in support of university strategic plans".

Another role commonly seen in data governance structures at post-secondary institutions is the Data Architect or Data Custodian. Staff with these responsibilities often hold IT roles and are responsible for the technical elements of data governance. They are "system administrators responsible for the operation and management of systems and servers that collect, manage and provide access to institutional data" (University of British Columbia, n.d.b.). As part of their role, data custodians should

> *document data definitions, configure tools to monitor data quality and integrity, promote consistency of data management goals, policy, procedures, tools, and techniques, perform impact analysis for changes and ensure appropriate security* (Fraser Health Authority, 2015).

Executive buy-in and communication are important to the implementation of data governance programs (Patil, 2015). The interviewees from institutions with existing data governance initiatives felt that they had executive support or sponsorship, often in the form of a data governance steering committee or similar with senior leadership to set direction and resolve conflicts. Many interviewees noted that buy-in at the executive level was critical to the development of their data governance program, citing the need for resources in the creation, maintenance, and adherence to data governance frameworks.

The structure of executive leadership varied, in the data governance processes described by interviewees. It might include designated executive level committees, executive representation on existing committees, or data governance being included in the mandate of an existing executive committee or committee with executive representation.

Data governance initiatives often begin with the formation of a steering committee. At UBC, the Data Governance Steering Committee (University of British Columbia, n.d.b.) is responsible for:

- *Approving policies, procedures and guidelines to ensure data consistency, data standardization, data security and data use,*
- *Creating a formal decision-making structure for data standardization,*
- *Providing a two-way mechanism for communicating (e.g., a reporting structure and/or communication plan) about data initiatives across the University,*
- *Creating formal procedures for liaising with data consumers and technical groups for data governance projects,*
- *Promoting best practices around data standardization.*

(https://cio.ubc.ca/data-governance/people)

Several interviewees noted that data governance steering committees at post-secondary institutions often experience challenges with engagement, and that data governance matters were better handled within existing committee structures.

Particularly in larger institutions, the role of chief data (or data and analytics) officer has a broad range of responsibilities relating to data quality, security, and use. Since higher education deals both with large quantities of varied data, and heavy regulation, designating a chief data officer is recommended (Pomerantz, 2017). However, a 2017 survey of 29 employees in higher education institutions found that while the title of chief data officer is prevalent in many other industries, few higher education organizations employed this title, with many executive leads for data governance instead holding the role of Director: for example, Director of Institutional Research (Pomerantz, 2017).

One of the early steps in the development of UBC's data governance program was the hiring of a full-time Chief Data Officer to coordinate the project. The role, established in 2016, involves overseeing the implementation of data governance tools (such as data warehouses and data glossaries), organizing training and resources, communicating with and liaising across the institution's business areas, assembling documentation, and facilitating strategic planning. Pan-institutional buy-in and effectiveness for UBC's data governance programs has been supported by working collaboratively with the business units, and developing a portfolio that is seen both as being distinct from information technology or institutional research, and as a collaboration that helps the entire university achieve success.

End users of data "include the people, organizational units, and information systems that are granted access to data for specific uses" (Backscheider et al., 2015, p.8). Data users play an important role in the data governance process. For example, at the Fraser Health Authority in British Columbia, data users

> *identify issues with data quality and escalate, work with data owners to determine and validate data usage, comply with policies, and ensure quality and availability of data for analysis and reporting meets business requirements* (Fraser Health Authority, 2015).

Communication Structures

In addition to defined roles and responsibilities, data governance programs should include a structure for communication between those in various roles. When defining the roles and responsibilities of those working with data, it is important to consider the communication that will take place within and between these roles (Patil, 2015).

Much of the communication around data governance within higher education institutions takes place in committees. While some institutions have standing data governance committees, others will imbed data governance into the mandate of existing standing committees. These committees will often already have relevant stakeholder representation, including executive leadership.

Higher education institutions often have departments that work with different kinds of data, and each will have its own varied goals and regulations regarding that data. Alumni associations at public institutions, for example, may need to comply with private sector legislation when collecting data related to donor events. UBC, for example, defines a number of *data communities* to support collaboration across business areas and interests, including: learners, human resources, advancement, finance, geospatial, services, research, and teaching and learning.

Data-Driven Culture

Building a data-driven culture is a requirement for the effective implementation of a data governance program.

> *Effective and long-lasting data governance programs require a cultural shift in organizational thinking and behavior about data, as well as an ongoing program of change management to support the new thinking, behaviors, policies, and processes to achieve the desired future state of behavior around data. No matter how precise or exotic the data governance strategy, ignoring culture will diminish chances for success. Focus on managing change must be part of the implementation strategy*. (DAMA International, 2017, p. 93)

The elements, identified by interviewees as central drivers of a data-driven culture were:

- Clearly defined roles and responsibilities;
- Shared responsibilities;
- Clearly defined goals and principles;
- Executive backing and leadership;
- Training and workshops;
- Iterative and flexible implementation; and
- Investing resources in alignment with goals.

Success in data governance is inextricably linked to people, processes, and technology. These elements support a change management approach, helping stakeholders to incrementally move towards both better data governance practices. Additionally, understanding that data governance is a shared responsibility, rather than only the responsibility of IT departments, promotes a data-driven culture.

> *People tend to conflate data and information technology. To become data-centric, organizations need to think differently and recognize that managing data is different from managing IT. This shift is not easy. Existing culture, with its internal politics, ambiguity about ownership, budgetary competition, and legacy systems, can be a huge obstacle to establishing an enterprise vision of data governance and data management* (DAMA International, 2017, p.73).

Business Glossaries

The need for clear definitions to support effective data analysis was a commonly expressed concern from our interviewees. Inconsistent definitions may mean that different people or areas of the institution may be discussing different data. For example, a lack of clarity regarding the types of students that may be included in the number of full-time students enrolled in an institution, may result in different answers to the same question. Creating a business glossary is often recommended as a good first step in developing data governance (Holak, 2019; Firican, 2019). A business glossary is a "metadata repository with clear and consistent definitions about important business and IT information, such as contacts, tools, processes, and who is considered a customer, supplier, business partner and employee" (Holak, 2019). Note how this definition of a glossary differs from a *data dictionary*, which is a term typically used by IT professionals to "(define) the structure and contents of data sets, often for a single database, application, or warehouse" (DAMA International, 2017, p. 429), and is often embedded directly in database tools to assist with operating the system.

Many business glossaries begin as simple efforts, with a few spreadsheets or documents, and advance over time to include enterprise-grade tools. Microsoft, Google, and Apple make popular spreadsheet and document software. Tools built by Alation, Collibra, and the Data Cookbook can facilitate data catalogs, and the latter two were mentioned by our interviewees. Other tools with a wider focus (but that also support creating catalogs) include the data and metadata management tools within Denodo's data virtualization platform, and Tableau's catalog functionality. These tools also enable more automated mapping of data lineage, to show where data comes from, and goes to, throughout its lifecycle. Other features typically include report requests, data governance workflows, and the ability to update and curate data. They aim to facilitate better business practices related to data, allow more time to be spent on analysis, and improve user trust in data.

Accordingly, the creation of a business glossary, as well as the procedures related to updates and maintenance of the glossary, are often a first step in the creation of a data governance program. One method of creating glossaries involves the use of a template that asks those working on the definition to define various elements of a data term, such as "data type". Several of the interviewees noted that a data glossary can be built without expensive tools, and can be started using an intranet, wiki, text document, or spreadsheet. If needs grow over time, the glossary can be ported to more advanced tools.

As part of its data governance program, UBC has built a data glossary, hosted in Collibra, which now governs data definitions across the institution. Employees are able to submit data definitions to the glossary. On its data governance website, UBC states the requirements for a data definition, makes recommendations for data definitions, and provides specific recommendations for polishing data definitions (University of British Columbia, n.d.a.).

At UBC, a data definition shall:

- *Be stated in singular form;*
- *State what the concept is, not just what it is not;*
- *Be stated as a descriptive phrase or sentence(s);*
- *Contain only commonly understood abbreviations/acronyms [define, if required]; and*
- *Be expressed without embedding definitions of other data or underlying concepts.*

UBC also provides examples of definitions. This is shown in **Table 3**.

Table 3: Examples of Term Definition Revision at UBC

Unpolished definition	Revised definition	Comments
FTEs: FTEs are the workload of employees or students converted to a proportion of a full-time work-load.	Full-time Equivalent: The workload of a person converted to a proportion of a full-time work-load during a given period of time.	Start in singular Define acronym separately Exclude the subject term
Reviewer: A senior person, such as a unit manager, can be assigned to review an outcome of a user task.	Reviewer: A user who is assigned to review an outcome of a user task.	Start with noun of broader concept Use of relative clause 'who' Concise Stand alone Exclude example Exclude procedural information
Employee: Person corresponding to the employee identifier.	Employee: A person who is employed for wages or salary.	Avoid circular definition
Baccalaureate Degree: A credential which is awarded at the completion of a baccalaureate program. Master's Degree: The credential awarded upon completion of a Master's program.	Baccalaureate Degree: A credential which is awarded at the completion of a baccalaureate program. Master's Degree: A credential which is awarded at the completion of a Master's program.	Maintain the same terminology and consistent logical structure for related definitions

Source: University of British Columbia (n.d.a.)

Data Storage

In most organizations, data governance includes making decisions on data storage, oversight of storage processes, creation and enforcement of storage and sharing policies, allocation of resources, ensuring compliance with storage regulations, and aligning storage practices within institutional goals (Blair et al., 2014). Data storage affects data security and privacy and can also affect an institution's ability to conduct effective research. Additionally, post-secondary institutions may be subject to legislative provisions regarding data storage. BC's public institutions, for example, must store data within Canada unless they receive permission to store data elsewhere.

Creating structures for storage, as well as clearly identifying guidelines relating to storage, is a central component of data governance. **Figure 2** displays the data handling and storage guidelines created as part of the University of Saskatchewan's data governance initiative.

Figure 2: University of Saskatchewan's Data Handling and Storage Guidelines

Storage Locations & Sharing Options	Institutional Systems	University-provided Department File Storage	University-provided Individual File Storage	University-provided Email and Instant Messaging	University-provided Research Storage	Removable Storage	Personal Devices	Non-university Cloud Services
	Banner, RMS, UnivRS, AIM, UFriend	Jade, SharePoint	Cabinet, OneDrive	@usask.ca accounts, MS Teams	DATASTORE	e.g. USB, External Hard Drive, CD, DVD	e.g mobile phones, computers	e.g Dropbox, Slack, Gmail
RESTRICTED	✓	! 1	! 2	✗ 7	✓ 4	! 5	✗ 8	✗ 9,10
LIMITED	✓	✓	✓	! 3	✓	! 5	✗ 8	✗ 9,10
INTERNAL	✓	✓	✓	✓	✓	✓	! 8	✗ 9,10
PUBLIC	✓	✓	✓	✓	✓	✓	✓	! 6,9

Use with Caution: Contact IT for assistance and recommendations.

1. Restrict access permissions appropriately on departmental file storage services.
2. Jade, SharePoint, and DATASTORE are preferred options for storing restricted and limited data outside of institutional systems.
3. Minimize unnecessary copies of limited and restricted data by sharing links instead of data files.
4. Restrict access permissions appropriately on DATASTORE.
5. Encrypt removable storage devices such as external hard drives and USB. Removable storage devices are suitable only for short-term or temporary storage.
6. Do not use non-university cloud services to store or share university data as they lack the contracts or service agreements that safeguard ownership and control of university data.

Not Recommended: Contact IT for assistance and recommendations.

7. Jade, SharePoint, and DATASTORE are preferred options for storing and sharing restricted and limited data outside of institutional systems.
8. Do not store sensitive university data on personal devices. Personal devices require increased security settings when used to access university data.
9. Do not use personal email to store and share university data.
10. Do not use non-university cloud services to store or share university data as they lack the contracts or service agreements that safeguard ownership and control of university data.

Source: University of Saskatchewan. "Data Handling and Storage Guidelines" by University of Saskatchewan, n.d.b. (https://www.usask.ca/avp-ict/documents/data-guidelines.pdf). Copyright n.d. by University of Saskatchewan. Reprinted with permission.

Data Security and Privacy

Effective data security and privacy are central goals of data governance. Data security is described as the "[leveraging of] evolving technology and emerging practices to focus on how to apply the three critical information security imperatives: confidentiality, integrity, and availability" (Fray et al., 2016, p. 1). Fray et al., (2016) describe four domains of data protection.

> *Affirmative Protections: These help define the positive cultural stance an institution has toward data protection, and they indicate the investment that an institution has made in protecting data. They include governance, policy, and procedures that are developed proactively to support data protection.*

Misuse Protections: These focus on ensuring that privacy and security needs are met. Included here are protections that ensure compliance and regulatory requirements are met, as well as actions that need to be taken in case of a breach.

Business Continuity Protections: These protections focus on the continued availability and usability of data.

Data Life-Cycle Protections: These are the procedures and policies specific to all stages of the data life cycle (p. 2).

A central aspect of data security and privacy is knowing who has access to what data, and why (National Student Clearinghouse, EDUCAUSE & REN-ISAC, 2018; Jim & Chang, 2018). Data aggregation is one way of ensuring data privacy while allowing for effective research. Removing any identifying factors from data and conducting research with an anonymized dataset can make data more broadly accessible across and outside of the institution, while maintaining security and privacy.

Data Quality and Reliability

Improving the accuracy and reliability of the data collected and stored at post-secondary institutions is often a primary goal of data governance programs. Many interview participants mentioned that one of the primary motivators for pursuing data governance at their institution was from a risk management perspective. Improving data quality would ensure that the institution's reporting was based on consistent, reliable, and trustworthy data. Improved data quality and reliability also enabled institutions to produce reliable longitudinal data. Others noted a desire to move away from having many "siloed" views of data to having an enterprise view of data, treating data as an asset. The enterprise data approach allows more agility and makes it possible to generate trustworthy data insights or research quickly, consistently, and reliably.

There are a few key concepts of building robust data systems that organizations should consider:

- Single Source of Truth (SSoT): the practice of structuring information models and related schemas so that every data element is stored exactly once. (Grealou, 2016).
- Single Version of Truth (SVoT): the practice of delivering clear and accurate data to decision-makers in the form of answers to strategic questions (Grealou, 2016).
- Multiple Versions of the Truth (MVoTs): the result of business-specific transformation of data into information with relevance and purpose (Dallemulle and Davenport, 2017).

These should not be regarded as mutually exclusive categories – rather, organizations often use these practices in conjunction with one another. Dallemulle and Davenport (2017) suggest that MVoTs are important to allow different business areas of an organization to work with the right nuance for their purposes. For example, in an SSoT view, Bayer would be considered a chemical/pharmaceutical company, and Apple would be considered a consumer electronics company. However, this broad categorization would not be very helpful for all areas in a company. A sales executive would likely prefer to classify Apple as a mobile phone or laptop company, depending on which sales division they were interacting with. Bayer could be seen as either a drug or a pesticide company, depending on the business need. Dallemulle and Davenport suggest that MVoTs supported by SSoTs support superior decision-making.

Tools and Technology

Employing tools for the collection, storage, security, sharing, and reporting of data are central elements of data governance. Effective utilization of these tools can optimize workflow, reduce the risk of non-compliance with regulations and legislation, as well as aid in data analysis and institutional research.

As higher education organizations more widely adopt enterprise data warehouses, data lakes, and cloud storage platforms to house data collected from a plethora of systems, better understanding of data fields and better decisions depends in part on having robust tools. According to DAMA *International's Data Management Body of Knowledge*, tools and technologies should be chosen *after* data governance goals have been created. The handbook outlines six common types of tools and technologies used in data governance:

- Online presence / websites;
- Business glossary;
- Workflow tools;
- Document management tools; and
- Data governance scorecards (p. 94, 2017).

Software tools exist for many of these data governance elements, and there are an increasing number of software options which allow institutions to handle multiple data governance needs in one designated space.

Policies, Procedures, and Guidelines

According to DAMA International, in the context of data governance "[d]ata policies are directives that codify principles and management intent into fundamental rules governing creation, acquisition, integrity, security, quality, and use of data information" (2017, p. 77). Institutions may also implement standards, procedures, and guidelines, in addition to policies. Guidelines can help guide users towards a desired course of action, while policies, standards, and procedures state the ways data must be handled.

While post-secondary institutions generally have policies and procedures regarding the collection, storage, security, and use of data, effective data governance includes the strategic creation of policies and procedures that align with other data governance elements, such as data quality goals, data management structures, and the roles of those working with the data.

Though many Canadian higher education institutions and organizations have policies relating to information security, it is less common to find policies explicitly outlining data management. Areas that may need to be considered in policy related to data governance include:

1. Definition of roles and responsibilities
2. Data definition and ownership
3. Data categories/classification
4. Data life-cycle issues
5. Data handling
    a. Classification of ownership of data
    b. Access/availability of data
    c. Transfer of research data
    d. Data destruction

6. Compliance
    a. Interactions with other institutional policies
    b. Relevant laws
    c. Grant rules
    d. Contracts
    e. Violations and sanctions

    (Adapted from Blair et al., 2014, p.4).

For example, the University of Saskatchewan's Data Management Policy, is "responsible for ensuring the availability, confidentiality, and integrity of all information to which it is entrusted" (University of Saskatchewan, 2005). The policy covers data definitions, scope and responsibilities, non-compliance, and principles in working with data. According to the policy,

> *Units and members of the university community must ensure:*
>
> 1. *Compliance with regulatory requirements, as well as third-party and other contractual data obligations.*
> 2. *Data is used for the purposes for which it is collected and any restrictions for its use are observed.*
> 3. *Data is collected, stored, and disposed of in ways appropriate to the risk and impact of unintended disclosure.*
>
> *(University of Saskatchewan, 2005)*

Similarly, UBC has a Data Governance Policy that "establishes who is responsible for information under various circumstances and specifies what procedures should be used to manage it" (University of British Columbia, n.d.a).

Simon Fraser University's Information Systems Data Governance Policy ensures that the highest quality data are delivered throughout the university, facilitating better decision-making through the use of accurate, trusted data. For them, data governance plays a central role to in ensuring that:

- The right people are making decisions about data;
- All users process accurate information;
- Data values are consistent across the institution; and
- Decisions are made based on accurate data.

Formal and Informal Data Governance in Post-Secondary Education

A frequent theme throughout the results of our research was formal versus informal approaches to data governance. When an organization works with data, data governance occurs regardless of the existence of a formal program, and those who work with data absorb data governance responsibilities into their roles. This lack of formal structure, however, often means that data governance is not efficient or consistent. Effective data governance allows institutions to reduce the likelihood of non-compliance with data legislation, policy, or regulation, and to increase the accuracy of data. Conversely, a lack of data governance may mean missed opportunities to align processes, policies, and procedures with institutional data goals, as well as in terms of effective institutional reporting and research.

Data governance is an emerging topic particularly within higher education, where formal data governance programs are still uncommon. Our research found that most higher education institutions did not have a formal data governance program. Programs that were established were either recently created, or are still being developed or implemented

Goals and Motivations of Data Governance Programs in Higher Education

As part of the creation of a data governance program, institutions and organizations should establish and clearly define the goals and motivations of their program. Our interviewees indicated that organizations and institutions with data governance programs were more likely to have clearly defined data governance goals and motivations.

Organizations may have differing motivations and goals for their data governance programs. The US-based National Association of State Chief Information Officers describes the most common goals and motivators across sectors:

- Enable better decision-making
- Reduce operational friction
- Meet stakeholder needs
- Establish common approaches
- Establish standard repeatable processes
- Reduce costs
- Increase effectiveness
- Ensure transparency (2009b, p.10).

The goals, motivations, and focus of data governance programs should be clearly defined and visible to stakeholders (DAMA International, 2017; Patil, 2015; Seiner, 2014). "The more clearly [the program] helps solve organizational problems, the more likely people will change behaviors and adopt governance practices" (DAMA International, 2017, p. 74).

At UBC, improving data quality and reducing the time spent working to mitigate data issues, data security and privacy were some of the primary motivators behind establishing a data governance program. A planned change to the institution's enterprise resource planning, and particularly the need to ensure effective migration and integration, were factors in the timing of the initiative. The goal of delivering "[h]igh quality and accessible data to advance UBC's purpose and vision delivered by integrated data management and principled governance" reflects these institutional goals. (University of British Columbia, n.d.a.).

One of the organizations we interviewed, the British Columbia First Nations' Data Governance Initiative (BC FNDGI), was unique in its goals and motivations. It aims to empower First Nations citizens through collective data ownership within Indigenous nations. The BC FNDGI is discussed further in the *Learning from the Healthcare Sector* section of the report.

Finally, the data governance initiative at the University of Regina is designed to help the University meet its strategic goals. The initiative has a particular emphasis on:

- The measurement of data quality, including errors, defects, and remediation of quality issues; and
- The delivery of meaningful data for leadership and management (Deloitte & University of Regina, 2016, p. 12).

In alignment with these principles, the University follows a framework that establishes a high-level Data Governance Council. The membership of the council includes leadership from several areas of the institution, covering both centralized and decentralized units in the academic, research, and management & administration domains.

The most prevalent goals and motivations for establishing data governance in higher education institutions, identified through literature reviews, institutional scans, and interviews, include security, reliable reporting, and scalability. Managing the risks associated with working with data was one of the primary goals mentioned by interviewees at post-secondary organizations.

Additionally, with data quality standards being a central component of formal data governance, one of the primary goals discussed by institutional interviewees was ensuring accurate reporting, both governmental and internal. Using data to enable more rigorous, effective, and timely research and analysis is another goal. For many organizations with data governance initiatives, this means equipping end-users of the data with accurate and thorough data, and with the tools to work effectively with the data.

Interviewees from institutions with data governance programs or initiatives also mentioned the ability to scale systems to the increasing number and complexity of records across the institution's various departments. Interviewees noted the need for more robust systems as the complexity of records collected by the organization increased, both in f the number of records and the number of metrics.

Frameworks

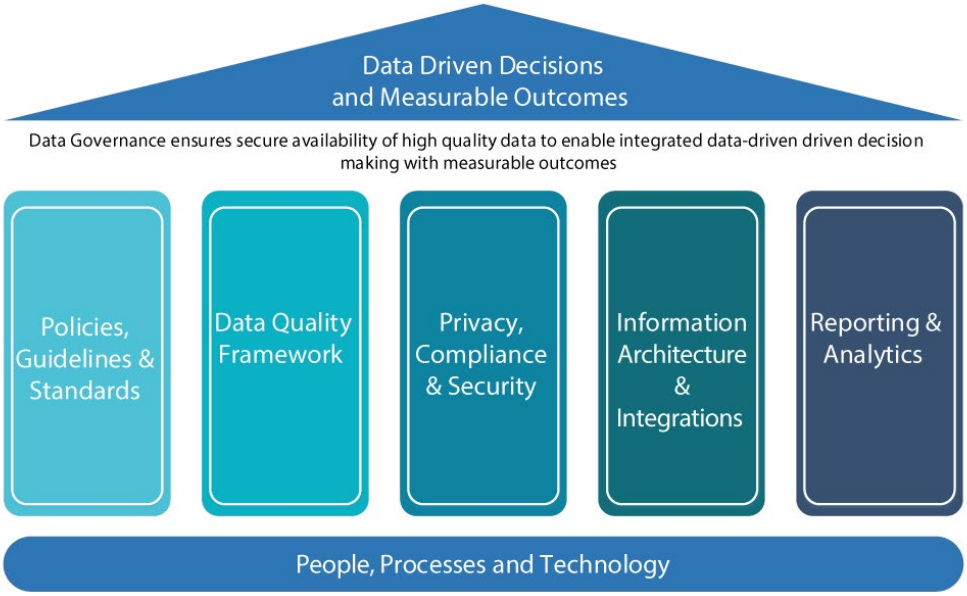
A framework is an organizational system that incorporates the previously identified elements of data governance. Interviewees from organizations with a data governance program and/or framework reported that they had created custom systems based on their needs, with some noting that "one size does not fit all." They mentioned that conducting research on existing systems and customizing a program for their organization was an important part of this process, with four organizations specifically citing Seiner (2014) as a starting point.

While most organizations with a formal data governance program in place were deep into program development, two others were starting their journey. When creating a customized data governance framework, institutions need to consider the size of the institution, budgetary constraints, existing institutional principles, and readiness of its business areas. One interviewee specifically discussed bringing in an external consultant, but most interviewees described an internal process that relied heavily on research and existing data governance frameworks, and yielded a model tailored to the needs of their institution. Another interviewee noted that because of the personalization and customization required to create a data governance program, they did not believe that contracting the project out would be as effective as building it within the institution.

At UBC, a data governance framework was customized to the institution's existing priorities after an extensive literature review. UBC's framework incorporates all the elements of data governance and is presented in **Figure 3**:

- Policies, Guidelines, & Standards (Data Ownership)
- Data Quality Framework (Data Stewardship)
- Privacy, Compliance, and Security (Role Definition and Accessibility)
- Information Architecture & Integrations (Reliable Flow of Information)
- Reporting and Analytics (Knowledge from Information).

Figure 3: UBC Data Governance Framework



Source: University of British Columbia. "[Data Governance] Roles and Responsibilities" by University of British Columbia, n.d.a. (https://cio.ubc.ca/data-governance/data-governance-program). Copyright n.d. by University of British Columbia. Reprinted with permission.

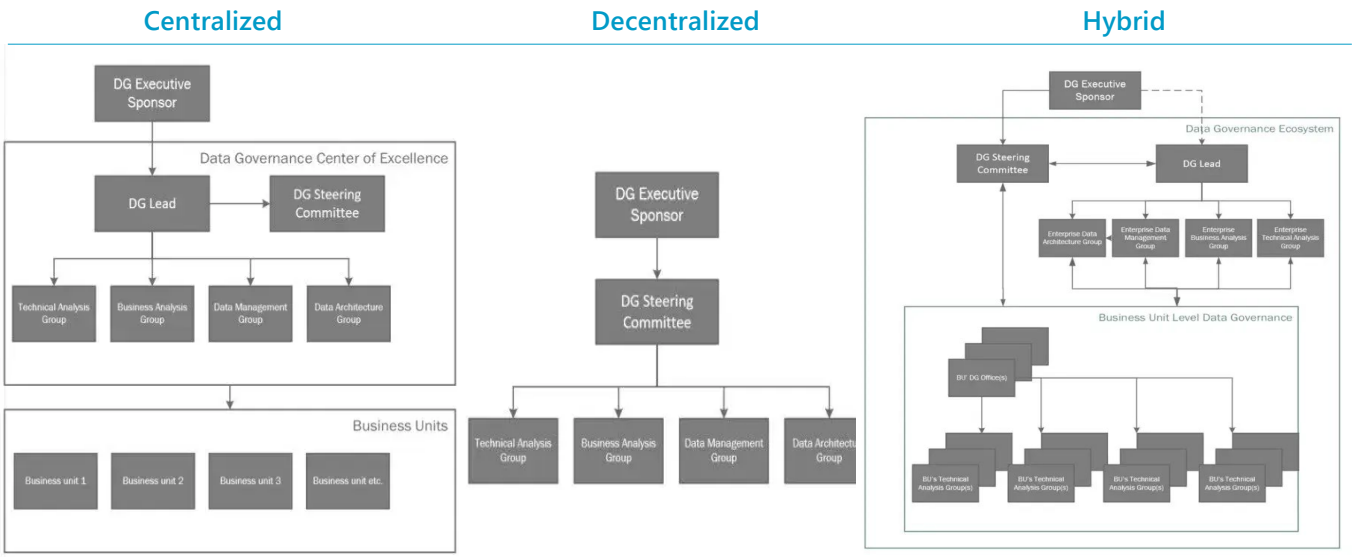
In addition to this framework, a "University Data Model" (UDM) at UBC states the "relationships, rules, constrains, and semantics" across people, organization, location, and curriculum (University of British Columbia, n.d.a.).

Implementation

Patil (2015) describes the data governance implementation structure as containing four levels. The first is the executive level, the responsibility of executive leadership. The second is the strategic level, primarily the responsibility of data stewards and process owners. The third is the program level, primarily the responsibility of governance managers and process owners. Finally, there is the execution level, primarily the responsibility of stewards, quality management, and data architects. An example of this type of structure can be seen in Figure 1: Data Governance Roles at UBC.

The level of centralization in an institution or organization can also influence the type of data governance operating model utilized. Firican (2018) discusses three operating models: centralized, decentralized, and hybrid/federated. Firican describes the pros of the centralized model as having more efficient decision making as decisions rely on a single dedicated data governance lead, a clear reporting structure, the ability to focus on policy, and ease of cost control while the cons are more rigid models, increased bureaucracy, and longer lead time to set up data governance operations. A decentralized model sees the opposite: the structure is flat and has wide representation. It is easy to establish but takes longer to reach consensus and is difficult to coordinate. A hybrid/federated model tries to mix the advantages of each approach. Ideally, it provides a model to provide input up through the organization while making top-down decisions possible, shares ownership of data, and supports a broad array of members. It can be challenging to find someone to lead this part of the operation, as it often requires a skilled full-time leader; it can sometimes be political and can both have more bureaucracy and be challenging to provide effective oversight for decentralized functions.

Figure 4: Data Governance Operating Models (Comparison)



Source: Lights on Data. "Data Governance Operating Models Exposed: Centralized Operating Model" by George Firican, 2018. (https://www.lightsondata.com/data-governance-operating-models-exposed/). Copyright 2018 by Lights on Data. Reprinted with permission.

Source: Lights on Data. "Data Governance Operating Models Exposed: Decentralized Operating Model" by George Firican, 2018. (https://www.lightsondata.com/data-governance-operating-models-exposed/). Copyright 2018 by Lights on Data. Reprinted with permission.

Source: Lights on Data. "Data Governance Operating Models Exposed: Hybrid/Federated Operating Model" by George Firican, 2018. (https://www.lightsondata.com/data-governance-operating-models-exposed/). Copyright 2018 by Lights on Data. Reprinted with permission.

Building a data governance program is an iterative process. Seiner describes data governance as "an evolution, not [a] revolution" (p. 9).

... [D]ata governance won't be completed all at once. Different organizations transition themselves into a data governance state in different ways. Some organizations focus early on specific domains or subject areas of data. Other organizations concentrate on specific business areas, divisions, units, or applications rather than implementing all across the organization at once. Still other organizations focus on a combination of two or three specific domains within business units using specific applications.

This perspective was reflected in our interviews and our scan of data governance programs. Interviewees described data governance as an iterative process, and it was common to see initiatives move through more than one structure before implementation. The representatives of institutions that had already implemented data governance programs recommended starting small and building data governance structures over time. The representative of one institution noted that given the institution's size, an immediate full-scale implementation would be unlikely to succeed. Another institution's representative discussed the importance of identifying and differentiating between small/simple and large/complex data governance projects in order to push certain projects quickly, freeing up resources to put more attention into larger and more complex components.

The University of Regina's program is an example of incremental implementation. The program began with a proof of concept focused on creating a student retention dashboard. The dashboard was intended to provide retention-related insights to members of the university community at a few different levels: Board or executive (institutional view), Dean/Associate Dean (Faculty view), and Student Advisor (individual student view) (Christie, 2016). The institution chose re-

tention as its focus because of its high priority at the University and because of the availability of detailed data. These data were regarded as fragmented and difficult to access or use.

Data governance has since become a full program at the University of Regina, with a Council and executive sponsorship. There are strategies to develop policies and processes, coordinate data stewards, and communicate to stakeholders. Unlike some larger institutions, the University has elected to amalgamate some of the roles and responsibilities associated with data governance into the role of the Data Governance Officer. This decision was made in part due to institutional size and budget constraints. The full implementation of the data governance program began by prioritizing data standards.

The University of Regina model may be appealing to small- and medium-sized institutions, as well as to those with limited staffing to support data governance. Starting with a pilot project and using existing institutional expertise and committee structures can help to build momentum towards larger data governance initiatives.

Assessing Data Governance Readiness and Maturity

Data governance maturity models allow organizations to assess data governance within their organization across multiple metrics, as well as their readiness to undertake data governance initiatives. While there are multiple data governance maturity metrics, most trace their origins to the Carnegie Mellon Capability Maturity Model (Palk, Curtis, Chrissis, & Weber, 1993). These metrics typically include the roles within the organization; the policies and practices that the organization has implemented; the technology utilized to handle data; data management; the alignment of IT practices and business goals; and the origination of the initiative. Maturity is often graded on a five-point scale, with points such as *initial, repeatable, defined, managed,* and *optimized* (DAMA International, 2017 pp. 534-536). At the "initial" level, data professionals send data autonomously with minimal oversight or controls. At the "defined" level organizations typically introduce scalable data management systems and some level of control to coincide with improved data quality and coordinated policy. At the "optimized" level, data management practices are predictable, using process automation and technology change management. At this stage, organizationally, the focus shifts to continuous improvement.

Organizations and institutions can use self-assessment tools to gauge the maturity of their data governance. For example, the UK Higher Education Statistics Agency provides an Excel workbook with nearly 200 questions across four domains. The answer to each question is a rating on a 4-point scale, and the workbook automatically tallies scores for each domain (given the question format, lower scores equate to higher maturity). The domains are culture; data activities; business process, and technology.

Learning from the Healthcare Sector

Unlike organizations that work with student data, organizations that use health data are more likely to have developed formal data governance programs. Health agencies and care providers have long had data governance standards, because of health-specific legislation that mandates a high standard of care, public concerns about sensitive health data being exposed, and the growth of electronic health records.

Data governance also plays an important role in health sector research. *Better Information for Improved Health: A Vision for Health System Use of Data in Canada* (2013), commissioned by the Conference of Deputy Ministers of Health, outlined the values and benefits of using electronic medical and health records to help improve patient care outcomes, while respecting individual confidentiality. The vision speaks to the importance of de-identifying data and appropriate consent to ensure secondary research is possible. There are four reasons for taking action to use this data:

- The need to improve performance and increase the sustainability of the health system;
- The shifting expectations of Canadians;
- The growth of digitized health data from which we can draw insights and inform actions; and
- The advances that make certain new technologies more viable and easier to use, and traditional ones more cost-effective. (p.3)

Another example of effective data governance in the health sector is the British Columbia First Nations' Data Governance Initiative (BC FNDGI). This initiative was established under the leadership of the Ktunaxa Nation in the Kootenay-Columbia region of BC to facilitate decision-making, planning, and investment. High quality data available is seen as one of the enablers of successful First Nations self-governance. The BC FNDGI was part of the early impetus for health-related outcomes and agreements with provincial and federal health agencies. However, in the subsequent 15 years, the initiative has expanded beyond health.

The BC FNDGI is responsible for overseeing the transformation of the existing, national First Nations Information Governance Centre (FNIGC) survey process in BC. This includes transformation of First Nations governance (ownership and control) and management (access and possession) processes related to data collection, storage, and analysis. The initiative will partner with the University of British Columbia's Data Centre and the Human Early Learning Partnership (HELP) to assist with the administration of surveys, development of a data warehouse, and the establishment of a regional centre feeding into a national FNIGC survey process (BC FNDGI, 2018, pp. 2-3).

The BC FNDGI is a leader in this area due to the goals of their initiative, and due to publicly providing a wealth of communications, templates and agreements for interested First Nations to utilize. The BC FNDGI's data governance ensures that "First Nations communities own, control, access, and possess information about their peoples" (BC FNDGI, n.d.), and it strives for "development and wellness that is self-governing, community-driven, and nation-based" (BC FNDGI, n.d.).

The BC FNDGI (https://www.bcfndgi.com/) makes a variety of communications, documents, and tools publicly available. These include:

- Visioning:
    - Regional First Nations Information Governance Centre (concept paper)
    - Vision Statement for Health, Vibrant, Self-Determining First Nations (video)
    - BC FNDGI Timeline of key events (graphic) including links to key agreements
    - Data Governance Frameworks and Policies:
- The Data Governance Policy Manual
    - Privacy and Security Policy Manual
    - Learning:
    - Data Governance 101 (video)
- Business Processes:
    - Targeted Program Analysis to describe business workflows, data entity assessments, and key system enablers

This level of transparency for data governance-related initiatives is uncommon in Canadian higher education. Some higher education institutions' interviewees felt that certain components of their data governance programs should not be fully visible to the public due to security concerns - our hope is that as data governance capacity builds, more information will become publicly available.

Overview of Data Access and Privacy Legislation for Post-Secondary Organizations

A central component of data governance is ensuring compliance with relevant federal and provincial policies and legislation. This section provides an overview of federal and provincial legislative provisions that may need to be considered in developing and maintaining a data governance program[4].

Introduction to Privacy Legislation

In this section, we discuss the general principles of privacy legislation, as well as providing an overview of specific Acts and their provisions, and how these apply to post-secondary institutions. A post-secondary institution must comply with legislation pertaining to student data, regardless of whether it has a formal data governance program or not. One compelling reason to formalize data governance programs is their inherent ability to lower the likelihood of noncompliance with legislation. Our interviewees cited risk management as a key driving force for adopting a data governance program. In Canada, federal Acts pertain to both public and private organizations, and there are Acts in some provinces pertaining to public- and private-sector organizations.

General Principles of Privacy Legislation

Each piece of legislation discussed in this section has two main goals: data privacy and data access. While Acts may have differing provisions, these common goals lead to similar Acts across Canada's provinces, as well as, to a lesser extent, internationally.

Canada's federal Personal Information Protection and Electronic Documents Act (2000, Schedule 1) [PIPEDA] outlines 10 data privacy principles. Other Acts, including Acts governing the public sector, are also centralized around these principles:

- Accountability
- Identifying purposes
- Consent
- Limiting collection
- Limiting use, disclosure, and retention
- Accuracy
- Safeguards
- Openness
- Individual access
- Challenging compliance

[4] This report reviews legislation from several jurisdictions around the world, and was completed in May 2020, prior to COVID-19, which resulted in changes to both federal and provincial legislation in this area. Institutions should ensure they are following changes in legislation. This report is not an alternative to legal advice from an appropriately qualified professional. If you have specific questions about any legislative or legal matter you should consult with an appropriately qualified professional.

British Columbia's Legislation

Data privacy in the British Columbia public sector is regulated by the Freedom of Information and Protection of Privacy Act (BC) [referred to as BC FIPPA], and in the private sector, under the Personal Information Protection Act (BC) Act (2003; referred to as BC PIPA). Health information in BC is governed by the Personal Health Information Access and Protection of Privacy Act (2008; referred to as BC E-Health), as well as either the federal Privacy Act or PIPEDA, depending on whether the organization is private or public. BC also has several higher education privacy acts which BC universities and colleges must adhere to. In this section, we discuss these pieces of legislation and their implications for higher education in greater detail.

Freedom of Information and Protection of Privacy Act (BC FIPPA)

The core data activities of British Columbia's public institutions are regulated under BC FIPPA. In 1994, one year after BC FIPPA came into effect, the Act was amended to include public post-secondary institutions in the list of public institutions (Office of the University Counsel, University of British Columbia, 2019). A Special Committee to the Legislature conducts reviews of BC FIPPA every six years (Office of the Information & Privacy Commissioner for British Columbia [OIPC], n.d.). This review is mandated by section 80 of the Act.

Private institutions may also be subject to BC FIPPA when programs or services are publicly funded, and when the institution may be considered a service provider.

Private Information Protection Act (PIPA)

Private sector organizations and public organizations engaging in for-profit non-core activities in British Columbia are regulated under BC PIPA(2003). In 2003, PIPA was "deemed substantially similar to PIPEDA" by the federal cabinet, and British Columbia was given an order of exemption allowing compliance with PIPA, rather than with PIPEDA (Office of the Privacy Commissioner, Canada, 2004).

Personal Health Information Access and Protection of Privacy Act (BC E-Health)

BC E-Health (2008) applies to health care bodies and to the establishment of health information banks. It permits collection, use, and potential disclosure of personal health information for identified purposes. The Act establishes a data stewardship committee, whose role is to consider requests for the disclosure of personal information for health research and to make recommendations to the minister, along with annually reporting to the public.

The BC E-Health Act overlaps BC FIPPA in stating that data disclosure inside or, if permitted, outside Canada is authorized for purposes identified in BC FIPPA. For this disclosure to legally take place, an information sharing agreement must be established between the disclosing body and various health organizations; provincial agencies, ministries or crown corporations; health-related regulatory bodies; and aboriginal governments, educational or social services bodies as defined in BC FIPPA.

Higher Education Acts

The University Act (1996) and the Colleges and Institutes Act (1996) regulate colleges, institutes, and universities in BC. Section 26 of BC FIPPA permits "the collection of information [when it] is expressly authorized under an Act", allowing organizations regulated by higher education Acts to collect data. Royal Roads and Thompson Rivers Universities are established under their own respective Acts in British Columbia, and they are also governed by BC FIPPA.

Application of Privacy Acts

For-profit activities conducted by a publicly funded higher education institution that are not part of its core activity may be regulated under private sector legislation. These activities are defined by PIPEDA as "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists" (Personal Information Protection and Electronic Documents Act, 2000, §2(1)).

The Office of the Privacy Commissioner of Canada expands on the differentiation between public and private applications.

> *While municipalities, educational institutions and hospitals may occasionally provide services on a fee basis, they are not, on the whole, engaged in trade and commerce as contemplated by the Canadian Constitution. Furthermore, these institutions are completely or largely dependent on municipally or provincially levied taxes and provincial grants.*
>
> *As a result, our Office is of the view that, as a general rule, CANADA PIPEDA does not apply to the core activities of municipalities, universities, schools, and hospitals. By core activities we mean those activities that are central to the mandate and responsibilities of these institutions. Providing a service for a fee does not necessarily trigger the application of the Act if the service is part of the institution's core activities.*
>
> *... A municipality, university, school or hospital may become subject to the Act when it engages in a non-core commercial activity, unless substantially similar provincial legislation applies. For example, if a university sold or bartered an alumni list, that activity would be considered a commercial activity and that particular transaction would be subject to the [CANADA PIPEDA] Act. As well, personal information collected by a university or a hospital in the course of operating a parking garage would probably be subject to the Act since this would not be considered a core activity.* (Office of the Privacy Commissioner, Canada, 2015)

At the federal level, freedom of information and data in Canada are primarily governed under two pieces of legislation. One is the Privacy Act (1985), which governs the ways governments and federal institutions collect, store, and secure citizen data, as well as ensuring access to data collected about them. The other is the Personal Information Protections and Electronic Documents Act (2000) (CANADA PIPEDA), which ensures the above conditions apply to private entities, as well as to public organizations engaging in commercial activities which are not central to their role (Office of the Privacy Commissioner, Canada, 2015).

Some provinces, including British Columbia, are exempt from CANADA PIPEDA. These provinces have created Acts deemed "substantially similar to CANADA PIPEDA" by the Governor in Council (Office of the Privacy Commissioner, Canada, 2017b). Nova Scotia, Newfoundland and Labrador, New Brunswick, and Ontario all have Orders of Exemption for health data through their own health data acts, and Alberta, British Columbia, and Quebec have legislation applicable to the private sector. According to the Privacy Commissioner of Canada,

> *The federal Personal Information Protection and Electronic Documents Act (CANADA PIPEDA), the Alberta Personal Information Protection Act (PIPA) and the British Columbia Personal Information Protection Act (PIPA) all share the same explicitly stated purpose: To govern the collection, use and disclosure of personal information by private sector organizations in a manner that recognizes both the right of the individual to have his or her personal information protected and the need of organizations to collect, use and disclose personal information for purposes that a reasonable person would consider appropriate* (Office of the Privacy Commissioner, Canada, 2004).

Activities occurring within another Canadian jurisdiction must be in compliance with the federal/provincial legislation applicable. When organizations based in exempt provinces are conducting activities within federally regulated provinces, federal Acts apply. When organizations in provinces or territories governed by CANADA PIPEDA operate within BC, they are required to follow CANADA PIPEDA. CANADA PIPEDA also applies to commercial activities that cross provincial lines (Office of the Privacy Commissioner, Canada, 2004). When crossing borders, it is possible that more than one piece of legislation will apply.

Health Acts apply when personal health information is collected. Federally, health information is governed by either the Privacy Act or by CANADA PIPEDA, depending on whether the activity is commercial. Ontario, Manitoba, Newfoundland and Labrador, and New Brunswick have created health data privacy and access Acts that have been deemed substantially similar to CANADA PIPEDA (Office of the Privacy Commissioner, Canada, 2017). British Columbia, Alberta, and Quebec have all passed health legislation which have not been deemed substantially similar and are used in addition to the federal CANADA PIPEDA.

Table 4 displays the privacy legislation governing post-secondary institutions in BC.

Table 4: Privacy Legislation in British Columbia

Institution	Primary BC Privacy Legislation	Additional Legislation
All public institutions and organizations	BC FIPPA	BC PIPA for non-core commercial activities
Private BC-based institutions	BC PIPA	BC FIPPA for publicly funded programs and activities
Public Canadian-based institutions operating in British Columbia	BC PIPA	The relevant public-sector legislation for the province of origin
Private United States-based institutions	BC PIPA	Parent companies comply with the Family Education Right and Privacy Act (1974)
Public health organizations	BC E-Health & BC FIPPA	

Elements of Privacy Legislation in the Context of Public Post-Secondary Institutions

In this section, we discuss aspects of privacy legislation that are likely to be applicable to post-secondary institutions and their data governance programs. We focus on British Columbia but highlight some of the differences in the legislation of other provinces.

Freedom of Information

Ensuring citizens have access to the data being collected about them is one of the primary aims of *BC FIPPA*. (§2(1)(b)) Freedom of Information (FOI) requests allow individuals to verify the accuracy of their data and ensure institutions can be held accountable for the data they store.

BC FIPPA's §5 grants individuals the right to request access to data stored about them by submitting Freedom of Information requests to public bodies (including public post-secondary institutions). In response to a request,

the head of a public body must create a record for an applicant if

(a) the record can be created from a machine-readable record in the custody or under the control of the public body using its normal computer hardware and software and technical expertise, and

(b) creating the record would not unreasonably interfere with the operations of the public body. (§2.6)

Responses to FOI requests should be sent within 30 days (§2.7) and should inform the individual whether their application has been approved or partially approved (§2.8). Should requests be approved, the applicant will be told when, where, and how their information will be given to them. Otherwise, they should be told why they have been refused, and, importantly, given the contact information of someone who can answer their questions, as well as information regarding their appeal or review options.

Sections 12 through 25 of *BC FIPPA* contain exemptions from requests, such as in cases when disclosure of information would be harmful to the institution (§17) or to a third party (§21); in cases where the records are to be released within 60 days (§20); records contain privileged legal advice (§14), etc. Should the request or part of the request be denied, institutions will hold the burden of proving that access was justifiably denied (§ 57). Institutions may charge students the fees incurred in producing and delivering the record (§73).

Once a student has received their personal data records, they may request corrections to their records. When a request is made, the record must either be corrected or, where it is determined that no change will be made to the record, annotated with correction (*BC FIPPA*, §29), and third parties with which the information has been shared must be notified to do the same.

Records which are "used by or on behalf of the public body to make a decision that directly affects the individual" (*BC FIPPA*, §31(b)) should be maintained for a minimum of one year to ensure they can be provided if an individual makes an information request.

According to *BC FIPPA's* §71, "the head of a public body must establish categories of records that are in the custody or under the control of the public body and are available to the public without a request for access under this Act". This information should not contain personal information unless disclosure is allowed under §33.1 or §33.2.

Collection

Section 26 of *BC FIPPA* allows for "the collection of information [when it] is expressly authorized under an Act". In the case of post-secondary institutions, the University Act §27 allows the institution's board to require students to provide the university with "the personal information that relates directly to and is necessary for an operating program or activity of the university, and… the personal information necessary to obtain a personal education number for the student". *BC FIPPA* also allows for the collection of data when "the information relates directly to and is necessary for a program or activity of the public body" (§26l). Additional purposes for collecting student data under *BC FIPPA* can be found in §26, as well as in Appendix 1.1.

Consent

Section 11 of the *BC FIPPA* regulations adds that in regard to sections 26(d), 30.1(a), 32(b) and 33.1(1) of the Act (discussed above), consent must be written, and must specify which pieces of personal information are being consented to. Effective dates for consent should also be identified. When post-secondary institutions collect data, students should be informed of the reason for collection and the legal authority under which it is being collected, and given contact information for someone within the institution who can answer their questions (§27(2)).

In accordance with §27 of *BC FIPPA*, institutions must collect information directly from students. Some of the exemptions allowing indirect collection include cases where the student consents to collection in another manner, and notably, when data are collected for "determining suitability for an honour or award including an honorary degree, scholarship, prize or bursary" (§27(c)(i)).

Limiting the Collection of Data

Institutions are to limit the data they are collecting by ensuring purposeful collection. *BC FIPPA's* §27.1 dictates that information should not be collected when it is not relevant to the post-secondary institution (§27.1(a)) and when the post-secondary institution doesn't plan to use it other than reading and/or transferring it (§27.1(b)).

Storage and Security

Data Security

BC FIPPA requires institutions to make "security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal" (§30). Specific security standards change frequently, and as such are seldom included directly in the legislation. BC's Office of the Information and Privacy Commissioner has published guidelines for public organizations entering into data services contracts (OIPC, 2003) and considerations in using cloud computing (OIPC, 2012). Standard recommendations related to data security include:

- Proper governance, including policies, procedures, and standards with respect to security and privacy.
- Identity and access management controls.
- Infrastructure security, including the ongoing management and maintenance of network, system, and application security.
- Encryption including both transmission and at reset to ensure that any communications cannot be intercepted or deciphered.
- Contract provisions, including enforcing BC FIPPA requirements in contracts with third parties.

Data Residency

Different jurisdictions have different provisions for data residency. British Columbia and Nova Scotia currently have regulations mandating that data must reside in Canada, while Ontario specifies data residency in Canada only for health-related data. If data are stored outside of Canada they may be subject to provisions of the USA PATRIOT Act (2001), or other non-Canadian laws. While the governing legislation may not require it, some organizations create internal policies and procedures regarding data residency.

Data Breaches

According to §30.5 of *BC FIPPA*, any employee of the institution must disclose unauthorized access to the head of the institution (or their designate under this section). Typically, an institution will have a policy or process for exactly what to do in the event of unauthorized access or disclosure. For example, Simon Fraser University requires the employee to complete an online report when there has been unauthorized access to or collection, use, disclosure or disposal of personal information. The report includes sections that identify the employee and their department; a description of the incident (including whether data was stored, accessed, or disclosed outside of Canada); what types and number of individuals may have been affected; what type of personal information may have been breached; existing safeguards; potential harm resulting from the breach; and mitigation and prevention measures for future. A full copy of the online reporting form is in Appendix 3.

Table 5: Sample data residency requirements

Act	Section	Sample Language
BC FIPPA	30.1	A public body must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada, unless one of the following applies: (a)if the individual the information is about has identified the information and has consented, in the prescribed manner, to it being stored in or accessed from, as applicable, another jurisdiction; (b)if it is stored in or accessed from another jurisdiction for the purpose of disclosure allowed under this Act; (c)if it was disclosed under section 33.1 (1) (i.1).
BC PIPA	Not specified in the Act.	
Canada Privacy Act	Not specified in the Act. However, the Treasury Board does have requirements (Brouillard, 2017) that Protected B, Protected C, and classified Government of Canada data must be in a Government of Canada approved facility located within the geographic boundaries of Canada or within the premises of a Government of Canada department located abroad, such as a diplomatic or consular mission.	
Canada PIPEDA	Not specified in the Act.	
Ontario	Restricts only health data.	
Nova Scotia	Public sector data must reside in Canada.	

While BC has provisions regarding data breaches, many other provinces, such as Manitoba and Nova Scotia, do not. CANADA PIPEDA has recently been amended to include necessary notification of privacy breaches (Office of the Privacy Commissioner, Canada, 2018), so it is possible that more provinces will amend their Acts to include this.

Sharing / Disclosure / Use

Privacy Acts also generally contain provisions around sharing, disclosure, and use of personal information. Some general situations where personal information may be used, disclosed, or shared in various Acts include:

- The purposes for which the information was obtained (BC FIPPA, Canada PA, Canada PIPEDA), or which would be considered "reasonable" in the circumstances (BC PIPA, Canada PIPEDA);
- Research and statistical purposes (BC FIPPA, Canada PIPEDA);
- Regulatory or legal requirements;
- Facilitating government payments (BC FIPPA);
- Reducing the risk of harm (BC FIPPA, BC PIPA, Canada PIPEDA);
- Medical reasons (all);
- Clearly benefits the individual and disclosure cannot be provided in a timely manner (BC PIPA); and
- By a politician (member of the federal Parliament or a provincial or territorial legislature) for the purposes of helping the individual better understand or secure government services (BC FIPPA, Canada PA).

Section 69 of *BC FIPPA* mandates that institutions "conduct a privacy impact assessment in accordance with the directions of the minister responsible for [BC FIPPA]". BC FIPPA defines a Privacy Impact Assessment as "an assessment that is conducted by a public body to determine if a current or proposed enactment, system, project, program or activity meets or will meet the requirements of Part 3 of this Act." (§69(1)(f)).

Data linkages have the potential of exposing identifiable information about individuals. Given this, BC FIPPA stipulates that post-secondary institutions "must notify the commissioner of a data-linking initiative or of a common or integrated program or activity at an early stage of developing the initiative, program or activity" (§5.5). *BC FIPPA's* §36.1 expands on data-linkage initiatives that are new or revised. Many other provinces do not contain data linkage provisions.

For more information about data sharing, disclosure, and provisions, see Appendix 1.2: Sharing/ Use/ Disclosure.

Legislation Across Jurisdictions

Provinces Outside of BC: An Overview

In this section, we summarize privacy and access legislation in provinces outside of BC. Each province or territory has its own privacy Act and regulations, and private sector and health data are usually governed by federal acts, unless they are exempt because of being governed by a provincial/territorial act that is sufficiently similar.

Alberta

Data governance in Alberta's public sector is provincially governed by the Freedom of Information and Protection of Privacy Act (2000; referred to as AB FOIP) and corresponding regulations. While the Act came into effect in 1994, post-secondary institutions were not covered by the Act until 1999. Alberta specifies that "[h]ealth information held by post-secondary institutions is covered by the FOIP Act" (Service Alberta, 2018).

The 2014/15 annual report of AB FOIP noted that FOI requests in the education sector had risen from 41 in 2013/14 to 61 (Government of Alberta, 2016). In both years, the education sector was among the 10 sectors receiving the highest numbers of FOI requests (10th and 8th, respectively).

Data governance in Alberta's private sector is also provincially governed, with its Personal Information Protection Act (AB PIPA) deemed substantially similar to CANADA PIPEDA.

The Alberta Office of Information and Privacy Commissioner clarifies that "[a] student's membership in a school club, such as a gay-straight alliance, is information about that student and is personal information to which the FOIP Act and PIPA apply" (Office of the Information and Privacy Commissioner of Alberta, 2019).

Manitoba

Manitoba's public sector data is governed under the Freedom of Information and Protection of Privacy Act (1997). In 2005, the Act was amended to include post-secondary institutions, with post-secondary institutions expected to comply with the Act by June of 2006.

Private sector data activity in Manitoba is governed federally under CANADA PIPEDA. In Manitoba, the Personal Health Information Act (1997) governs heath data collected at any public body, as opposed to only health organizations (Government of Manitoba, 2017).

New Brunswick

New Brunswick's public sector data is governed by the Right to Information and Protection of Privacy Act (2009). In the private sector, New Brunswick is governed by CANADA PIPEDA.

Newfoundland and Labrador

Newfoundland and Labrador's public sector data is governed by the Access to Information and Protection of Privacy Act (2015). In the private sector, Newfoundland and Labrador is governed by CANADA PIPEDA.

Northwest Territories and Nunavut

Public post-secondary institutions in both the Northwest Territories and Nunavut are required to comply with the Northwest Territories' Access to Information and Protection of Privacy Act. As this law was in force at the time of the creation of Nunavut on April 1, 1999, it became part of the law in Nunavut as well. For commercial activities involving data, Northwest Territories and Nunavut institutions are governed under CANADA PIPEDA.

Nova Scotia

Data at Nova Scotia's public institutions are governed by the Freedom of Information and Protection of Privacy Act (1993). Personal information collected by a Nova Scotia public body must be stored within Canada.

Ontario

Data at Ontario's public sector educational institutions are governed by the Freedom of Information and Protection of Privacy Act (1990). Ontario's health information legislation (Personal Health Information Protection Act, 2004) also requires that personal health data be stored within Canada. Ontario's private sector activities are governed under CANADA PIPEDA.

Dowding (2011) notes that "FIPPA's implementation led Ontario university administrations to review and revise now outdated or inconsistent privacy policies. It also required universities to explain the new legislation, a task that proved to be unexpectedly difficult" ...Before FIPPA's 2006 implementation, post-secondary institutions in Ontario had "no common policies for guaranteeing access to institutional information... or for protecting the privacy of students and faculty".

Quebec

Quebec's public sector data is governed by the Act respecting access to documents held by public bodies and the protection of personal information (2019).

Private sector data in Quebec is governed by an Act respecting the protection of personal information in the private sector (2019).

Saskatchewan

In Saskatchewan, data at public educational institutions are governed by The Freedom of Information and Protection of Privacy Act (1990-91).

Yukon

In the Yukon, the Access to Information and Protection of Privacy Act (YK ATIPP) gives the public a right to access any records held by a public body and the right to individuals to access their own personal information.

United States of America

Currently, many American states are moving private sector data privacy and access bills through their legislatures (Noordyke, 2019). The International Association of Privacy Professionals maintains a listing of the prevailing privacy legislation in all American states, currently available at https://iapp.org/resources/article/state-comparison-table/ At the time of publication of this report, California, Maine, and Nevada are the only states that have enacted privacy legislation.

Europe

The recent introduction of Regulation (EU) 2016/679 of the European Parliament and of the Council, known as the General Data Protection Regulation (GDPR), addresses the protection of persons with regard to the processing of personal data and on the free movement of such data. This has necessitated changes to the way Europe's private and public sectors manage their data. Similar to Canada's PIPEDA, the GDPR aims to ensure freedom of information and to protect privacy. Its provisions impact any organization worldwide, including post-secondary institutions in Canada and the U.S. that process data relating to people in Europe.

Referencing the implications of the GDPR for American colleges, an American lawyer noted that "[every] U.S. educational institution has here and there, somehow, had a relationship with Europe… [t]herefore, you need to be concerned about the new regulation" (McKenzie, 2018). While America's FERPA mostly covers post-secondary institutions, the regulations do vary, and should be reviewed by post-secondary institutions. Similarly, the GDPR may apply to Canadian institutions conducting business within Europe, regardless of whether the individual is a citizen or permanent resident of the European Union.

The GDPR contains a number of other provisions that could impact post-secondary institutions, such as the "right to be forgotten". Individuals can request that their personal data be erased if:

- the personal data is no longer necessary for the purpose which you originally collected or processed it for;
- the data holder is relying on consent as their lawful basis for holding the data, and the individual withdraws their consent;
- the data holder is relying on legitimate interests as their basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- the data holder is processing the personal data for direct marketing purposes and the individual objects to that processing;
- the data holder has processed the personal data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle);
- the data holder has to do it to comply with a legal obligation; or
- the data holder has processed the personal data to offer information society services to a child (Information Commissioner's Office, 2019).

Discussion: Key Considerations and Recommendations for Post-Secondary Organizations

The discussion regarding data governance in the context of higher education has two components. First, higher education institutions hold a significant amount of personal information, and must work within the highly developed regulatory framework outlined above. In such an environment, privacy breaches, data loss, and other non-compliance with legislation need to be mitigated. At the same time, data can potentially be used as an asset, allowing higher education institutions or organizations to improve in a variety of areas. These might include student satisfaction; retention and/or performance, teaching strategies, accuracy and ease of institutional research and reporting; institutional decision-making; fundraising; and data accessibility (Reid-Martinez & Mathews, 2015). Our scan of Canadian institutions found that data governance is most often practiced informally. Those with formal data governance programs have either implemented their programs recently or are still in the development process.

One of the most common themes we identified was the need for a shift toward a data-driven culture within the institution or organization. This included defining roles and responsibilities, implementing effective methods and structures for communication, ensuring buy-in across the institution, active and communicative leadership, training, and clearly outlined goals and motivations all backed by resource allocation that supports these goals and motivations. Interviewees emphasized that data governance is a shared responsibility, touching nearly every stakeholder who works in an organization; stewards, custodians, executive leaders, and users are all necessary for the success of data governance initiatives. Intra-institution collaboration and communication is important for higher education institutions given the various ways in which different departments intersect. While these departments may have differing uses of and goals for data, definitions should be consistent institution-wide.

Ensuring data privacy and security, enabling reliable institutional research and reporting through increased data quality, and keeping up with increasingly large amounts of increasingly complex data are the primary goals of data governance in higher education institutions and organizations. Institutions may have other goals for their data, as well as broader institutional goals, and data governance initiatives should remain in alignment with these. Our findings showed that risk reduction and opportunities for more accurate reporting and analytics were primary goals in pursuing data governance, whether or not the institution had a full program in place. The motivations of institutions and organizations will vary based on concerns regarding their institutional data, such as difficulty in dealing with increasing volumes of data or reliability issues.

In addition to collaboration amongst departments, some interviewees noted that it was not necessary to 'reinvent the wheel,' advising that institutions look to what others with developed or developing data governance programs are doing. While we recommend that organizations have at least one designated employee for data governance, much of the work will be done by those with existing responsibilities. As data stewardship becomes a part of many existing positions, higher education institutions will need to balance these initiatives with the other day-to-day operations of their employees.

We recommend that higher education institutions and organizations start small in the creation of data governance programs and initiatives. Initiatives can start with a pilot or proof-of-concept, perhaps within a select number of departments (like those best equipped for the initiative, such as IT, the Registrar's Office, or Institutional Research).

Ideally, however, the initiative will involve some of the academic units. Institutions and organizations should also leverage existing institutional structures, governance enterprises, policies, and regulations. For example, it may be more effective to embed data governance into an existing governing body with relevant stakeholders, rather than to create a new committee.

The initiative should also be supported by executive leadership and by buy-in throughout the organization, as well as a sufficient allocation of resources. Technology-based resources can support elements of data governance, especially in terms of collection, storage and records, analysis, and sharing, but these resources were emphasized less in our data than people-based resources, such as regular meetings of committees and groups involved in data governance, staff training, and additional staff members.

Data security is one of the most significant aspects of data governance. Most institutions recognize data security, privacy, risk reduction, and compliance as key drivers of data governance. Anonymized and/or compiled data can minimize risk while allowing for the same depth of analysis as data which have not been aggregated.

Given the variety of legislative provisions and regulations across provinces, as well as across data types (public, private, and health), institutions should frequently review legislation within the context of their operations. The increase of data-driven culture and the speed of technological advances mean that legislation will often not be caught up to current data practices and possibilities. One interviewee noted that effective data governance discussions and structures should go beyond maintaining compliance. Effective data governance programs should allow for quick responses to any legislative changes.

Our recommendations for institutions developing formal data governance programs and initiatives are:

1. Create a customized program with institutional goals, policies, and procedures based on current research and practice;
2. Leverage existing institutional structures and governance expertise;
3. Implement incrementally, expecting and allowing for iteration;
4. Ensure adequate executive leadership;
5. Establish communication structures;
6. Support buy-in by clearly stating goals;
7. Use resources such providing ongoing training and workshops, rather than only using tools and technologies;
8. Consider intersections of various departments who may interact with data in varying ways; and
9. Create and maintain systems for measuring the progress and success of the program.

Future Research

This research highlights that data governance is an area of increasing interest for post-secondary institutions, admissions and transfer organizations, and health organizations. The rapid rate of progress and change in legislation, research, and institutional and organizational practices in data governance in the context of higher education institutions necessitates an ongoing discussion. Institutions and organizations scanned as part of this report will be in different phases of development and implementation in the coming years, and we will likely see the emergence of formal

data governance programs in institutions and organizations which have not begun initiatives as of the creation of this report. Given this, future scans should revisit landscapes, recommendations and best practices to ensure they remain current.

We did not aim to establish a benchmark with which to compare the success of established data governance programs within higher education. Future research can utilize benchmarks to ask what types of frameworks, executive support, human resources, and institutional visibility successful programs have, relative to those deemed unsuccessful.

Most of the representatives of the post-secondary institutions interviewed for this research approached data governance as a collaboration between business areas, information technology, and institutional research. Private industry does not usually have an equivalent to institutional research. The research literature suggests that data governance should be led by the needs of the business. Research into strategies used by leaders in institutional research to ensure buy-in across business units would help further illuminate strategies for successful data governance programs.

Finally, a more in-depth comparison of data governance frameworks used in higher education versus those used outside of it would help to better illustrate how higher education differs from enterprise, while highlighting best practices that are shared.

Acknowledgements

The research team gratefully acknowledges the support and funding for this research from the British Columbia Council on Admissions &Transfer, particularly Robert Adamoski and the Research Committee for sharing their perspectives throughout the project, for reviewing the drafts, and suggesting improvements. We owe a debt of gratitude to George Firican, founder of Lights on Data and Director of Data Governance & Business Intelligence within the Development and Alumni Engagement Unit at the University of British Columbia, and Keith Fortowsky, the Data Governance Of-ficer at the University of Regina. George shared his time and expertise with us early in our data governance journey, recommending readings, resources, and people to connect with to learn more. Beyond participating in an interview, Keith provided additional recommendations for research articles and data governance examples to help our team. Several other data governance leaders from across North America took the time to share their perspectives on data governance through surveys and targeted interviews, for which we are extremely grateful. We thank Marcela Hernandez, the Chief Data Officer at the University of British Columbia, and Jon Coller, the Chief Information Security Officer at the University of Saskatchewan for their support of this research.

References

Access to Information and Protection of Privacy Act, Statutes of the Northwest Territories (1994, c. 20).

Access to Information and Protection of Privacy Act, Revised Statutes of Yukon (2002, c. 1).

Access to Information and Protection of Privacy Act, Statutes of Newfoundland and Labrador (2015, c. A-1.2).

Act respecting access to documents held by public bodies and the protection of personal information, Compilation of Québec Laws and Regulations (2019, c. A-2.1).

Act respecting the protection of personal information in the private sector, Compilation of Québec Laws and Regulations (2019, c. P-39.1).

Act respecting the sharing of certain health information, Compilation of Québec Laws and Regulations (2019, c. P-9.0001).

Backscheider, N., et al. (2015) *Establishing data stewardship models*. ECAR Working Group Paper. Retrieved from https://library.educause.edu/-/media/files/library/2015/12/ewg1514-pdf

Blair, D., et al. (2014). *Research data storage*. ECAR Working Group Paper. Retrieved from https://library.educause.edu/-/media/files/library/2014/7/ewg1403-pdf.pdf.

British Columbia First Nations' Data Governance Initiative [BC FNDGI]. (n.d.). *British Columbia First Nations' Data Governance Initiative*. Retrieved from https://www.bcfndgi.com

British Columbia First Nations' Data Governance Initiative [BC FNDGI] (2018) *British Columbia First Nations' Data Governance Centre – Concept Paper*. Retrieved from https://bcfndgi.com/s/Data-Centre-Concept-Paper.docx

Brouillard, M. (2017, November 1). *Direction for electronic data residency (IT Policy Implementation Notice No. 2017-02)*. Retrieved from the Government of Canada website: https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/direction-electronic-data-residency.html

Christie, B. (2016). *The successful launch of a data governance regime*. Presented at the HEIR Network Conference. Retrieved from the University of Regina website: https://www.uregina.ca/orp/assets/projects-presentations/christie-heir-launching-dg.pdf

College and Institute Act, Revised Statutes of British Columbia (1996, c. 52).

Data Republic. (2019, April 5). Data Governance vs Data Management. Retrieved from https://www.datarepublic.com/blog/data-governance-vs-data-management

DAMA International (2017). *Data management body of knowledge* (2nd ed.). Basking Ridge, NJ: Technics Publications.

Deloitte & University of Regina (2016, June). *Data governance and reporting framework, phase 2: Data governance council transition document*. Retrieved from the University of Regina website: https://www.uregina.ca/orp/assets/d-g/final-deloitte-dg-rpt-oct-2016.pdf

Dowding, M. R. (2011). Interpreting privacy on campus: The Freedom of Information and Personal Privacy Act and Ontario universities. *Canadian Journal of Communication, 36*(1), 11–30. doi: 10.22230/cjc.2011v36n1a2252

E-Health (Personal Health Information Access and Protection of Privacy) Act, Statutes of British Columbia (2008, c. 38).

Family Educational Rights and Privacy Act, 20 U.S.C § 1232g (1974).

Firican, G. (2018). Data Governance Operating Models. Retrieved from: https://www.lightsondata.com/data-governance-operating-models-exposed

Firican, G. (2019). 1st Step in Setting Up a Business Glossary. Retrieved from https://www.youtube.com/watch?v=V8mPIcm0mjw

Fraser Health Authority (2015). Information and Data Governance. Retrieved from https://www.fraserhealth.ca/-/media/Project/FraserHealth/FraserHealth/About-Us/Accountability/Policies/InformationAndDataGovernance-Policy-201501.pdf

Freedom of Information and Protection of Privacy Act, Revised Statutes of Prince Edward Island (1988, c. F-15.01).

Freedom of Information and Protection of Privacy Act, Revised Statutes of Ontario (1990, c. F.31).

Freedom of Information and Protection of Privacy Act, Statutes of Nova Scotia (1993, c. 5).

Freedom of Information and Protection of Privacy Act, Revised Statutes of British Columbia (1995, c. 165).

Freedom of Information and Protection of Privacy Act, Revised Statutes of Alberta (2000, c. F-25).

Freedom of Information and Protection of Privacy Regulation (B.C. Reg. 155/2012). (2012, July 3). *BC Gazette Part II*. Retrieved from http://www.bclaws.ca/civix/document/id/bcgaz2/bcgaz2/v55n13_155-2012

Government of Alberta (2016, April). *Freedom of information and protection of privacy: Annual report 2013-14 and 2014-15.* Retrieved from http://www.servicealberta.gov.ab.ca/foip/resources/annual-reports.cfm

Government of British Columbia (n.d.). DataBC. Retrieved from https://www2.gov.bc.ca/gov/content/data/about-data-management/databc

Government of British Columbia (2017). Data Custodianship Guidelines for the Government of British Columbia. Retrieved from https://www2.gov.bc.ca/assets/gov/data/data-management/data_custodianship_guidelines_for_the_government_of_bc.pdf

Government of Canada (n.d.). A Data Strategy Roadmap for the Federal Public Service. Retrieved from https://www.canada.ca/content/dam/pco-bcp/documents/clk/Data_Strategy_Roadmap_ENG.pdf

Government of Manitoba (2017). *A review of The Freedom of Information and Protection of Privacy Act.* Retrieved from https://www.gov.mb.ca/fippa/fippareview.html

Grealou, L. (2016). Single Source of Truth vs Single Version of Truth. Retrieved from https://www.linkedin.com/pulse/single-source-truth-vs-version-lionel-grealou

Gregory, A. (2011). Data governance—Protecting and unleashing the value of your customer data assets. *Journal of Direct, Data and Digital Marketing Practice, 12*(3), 230–248. doi: 10.1057/dddmp.2010.41

Health Information Act. Revised Statutes of Alberta § c. H-5 (2000).

Holak, B. (2019, March 25). *Building a business glossary enhances data governance.* Retrieved from https://searchdatamanagement.techtarget.com/news/252460155/Building-a-business-glossary-enhances-data-governance

Information Commissioner's Office (2019, May 22). *Guide to the General Data Protection Regulation.* Retrieved from the Information Commissioner's Office website: https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

Jim, C., & Chang, H. C. (2018). The current state of data governance in higher education. *Proceedings of the Association for Information Science & Technology, 55*, 198–206. doi: 10.1002/pra2.2018.14505501022

Luftman, J. (2003). Assessing IT/business alignment. *Information Systems Management, 20*(4), 9–15. doi: 10.1201/1078/43647.20.4.20030901/77287.2

McKenzie, L. (2018, March 13). European rules (and big fines) for American colleges. *Inside Higher Ed.* Retrieved from https://www.insidehighered.com/news/2018/03/13/colleges-are-still-trying-grasp-meaning-europes-new-digital-privacy-law

National Association of State Chief Information Officers. (2009b). Data Governance Part III: Frameworks – Structure for Organizing Complexity. Retrieved from https://nascio.org/Portals/0/Publications/Documents/NASCIO-DataGovernancePTIII.pdf

National Student Clearinghouse, EDUCAUSE, & REN-ISAC. (2018). *Why cybersecurity matters: And what registrars, enrollment managers and higher education should do about it.* Retrieved from http://www.studentclearinghouse.org/blog/what-registrars-enrollment-managers-and-higher-education-should-do-about-cybersecurity/

Noordyke, M. (2019, April 18). *US state comprehensive privacy law comparison.* Retrieved from https://iapp.org/news/a/us-state-comprehensive-privacy-law-comparison/

Office of the Information and Privacy Commissioner for British Columbia (2003, May). *Data services contracts.* Retrieved from https://www.oipc.bc.ca/guidance-documents/1460

Office of the Information and Privacy Commissioner for British Columbia (2012, June). *Cloud computing guidelines for public bodies.* Retrieved from https://www.oipc.bc.ca/guidance-documents/1427

Office of the Information and Privacy Commissioner for British Columbia (n.d.). *Legislation.* Retrieved from https://www.oipc.bc.ca/about/legislation/

Office of the Information and Privacy Commissioner of Alberta (2019, September). *Advisory on disclosing a student's participation in a school club.* Retrieved from https://www.oipc.ab.ca/resources/a-to-z.aspx

Office of the Privacy Commissioner of Canada (2004, November 5). *Questions and answers regarding the application of PIPEDA, Alberta and British Columbia's Personal Information Protection Acts.* Retrieved from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/02_05_d_26/

Office of the Privacy Commissioner of Canada (2015, December 16). *The application of PIPEDA to municipalities, universities, schools, and hospitals.* Retrieved from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/02_05_d_25/

Office of the Privacy Commissioner of Canada (2017a, January 30). *Interpretation bulletin: Commercial activity.* Retrieved from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_03_ca/

Office of the Privacy Commissioner of Canada (2017b, May 29). *Provincial legislation deemed substantially similar to PIPEDA.* Retrieved from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/provincial-legislation-deemed-substantially-similar-to-pipeda/

Office of the Privacy Commissioner of Canada (2018, October 29). *What you need to know about mandatory reporting of breaches of security safeguards.* Retrieved from https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/

Office of the University Counsel, University of British Columbia (2019, September 10). *About the Freedom of Information and Protection of Privacy Act.* Retrieved from https://universitycounsel.ubc.ca/subject-areas/access-and-privacy-general/access-to-information/about-fippa/

Otto, B. (2011). A morphology of the organisation of data governance. 19th European Conference on Information Systems.. Retrieved from https://www.researchgate.net/publication/221407900_A_morphology_of_the_organisation_of_data_governance

Palk, M., Curtis, B., Chrissis, M. B., & Weber, C. (1993). *Capability maturity model for software, version 1.1 (*Technical Report No. CMU/SEI-93-TR-024). Retrieved from http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=11955

Patil, N. (2015). *Data governance: The pragmatic way.* Emids. Retrieved from https://www.emids.com/wp-content/uploads/2018/06/emids_WP_DataGovernance_2015.pdf.

Personal Health Information Act, Statutes of Newfoundland and Labrador (2008, c. P-7.01).

Personal Health Information Act, Statutes of Nova Scotia (2010, c. 41).

Personal Health Information Privacy and Access Act, Statutes of New Brunswick (2009, c. P-7.05).

Personal Health Information Protection Act, Statutes of Ontario (2004, c. 3, Schedule A).

Personal Information Protection Act, Statutes of British Columbia (2003, c. 63).

Personal Information Protection Act, Statutes of Alberta (2003, c. P-6.5).

Personal Information Protection and Electronic Documents Act, Statutes of Canada (2000, c. 5).

Privacy Act, Revised Statutes of Canada (1985, c. P-21).

Reeves, J., & Pearlman, L. (2017). *Digital capabilities in higher education, 2016: Analytics* [Research Report]. EDUCAUSE. Retrieved from https://library.educause.edu/-/media/files/library/2017/9/ers1713.pdf

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (2016).

Reid-Martinez, K., & Mathews, M. (2015). *Big Data in Higher Education.* Center for Digital Education. Retrieved from https://www.d2l.com/wp-content/uploads/2016/02/big-data-in-education-report.pdf.

Reinitz, B. (2019). *The Impact of Analytics on the Higher Education Workforce.* EDUCAUSE. Retrieved from https://er.educause.edu/blogs/2019/8/the-impact-of-analytics-on-the-higher-education-workforce

Right to Information and Protection of Privacy, Statutes of New Brunswick (2009, c. R-10.6).

Seiner, R. (2014). *Non-invasive data governance: The path of least resistance and greatest success* (1st ed.). Basking Ridge, NJ: Technics Publications.

Service Alberta (2018, February). *Frequently asked questions for post-secondary institutions.* Retrieved from http://www.servicealberta.gov.ab.ca/foip/documents/FAQ_Post_Secondary_(Jan07_updated_Feb_14).pdf

Simon Fraser University (n.d.). *Privacy Breach Report—Archives and Records Management.* Retrieved from https://www.sfu.ca/archives/foipop/PrivacyBreach/privacy-breach-report.html

The Freedom of Information and Protection of Privacy Act, Statutes of Saskatchewan (1990, c. F-22.01).

The Freedom of Information and Protection of Privacy Act, Statutes of Manitoba (1997, c. 50).

The Personal Health Information Act, Statutes of Manitoba (1997, c. 51).

University Act, Revised Statutes of British Columbia (1996, c. 468).

University of British Columbia (2019). Information Security Policy. Retrieved from https://universitycounsel-2015.sites.olt.ubc.ca/files/2019/08/Information-Systems-Policy_SC14.pdf

University of British Columbia (n.d.a.). Data Governance Program. Retrieved from https://cio.ubc.ca/data-governance/data-governance-program

University of British Columbia. (n.d.b.). Data Governance Program: People. Retrieved from https://cio.ubc.ca/data-governance/people

University of Saskatchewan (2005). Data Management Policy. Retrieved from: https://policies.usask.ca/policies/operations-and-general-administration/data-management.php

University of Saskatchewan. (n.d.a.). Data Governance Framework. Retrieved from https://www.usask.ca/avp-ict/documents/data-governance-framework.pdf

University of Saskatchewan. (n.d.b.). Data Handling and Storage Guidelines. Retrieved from https://www.usask.ca/avp-ict/documents/data-guidelines.pdf

USA PATRIOT Act, Pub. L. No. 107–56, 115 Stat. 272 (2001).

Yukon Information and Privacy Commissioner (2020). Right of Access. Retrieved from https://www.ombudsman.yk.ca/yukon-information-and-privacy-commissioner/for-the-public/i-want-access-to-request-records

Appendix 1: Legislation Scan

The legislation scan covered legislation relevant to data governance in the context of post-secondary, health, and governmental organizations. The appendices that follow only include the sections of legislation that were most relevant to this purpose, rather than the entire legislation.

Appendix 1.1: Collection, Use, and Disclosure

Prescribed Purpose

Act	Section	Sample Language
BC FIPPA	26(d)	(a) the collection of the information is expressly authorized under an Act, (b) the information is collected for the purposes of law enforcement, (c) the information relates directly to and is necessary for a program or activity of the public body, (d) with respect to personal information collected for a prescribed purpose, (i) the individual the information is about has consented in the prescribed manner to that collection, and (ii) a reasonable person would consider that collection appropriate in the circumstances (e) the information is necessary for the purposes of planning or evaluating a program or activity of a public body, (f) the information is necessary for the purpose of reducing the risk that an individual will be a victim of domestic violence, if domestic violence is reasonably likely to occur, (g) the information is collected by observation at a presentation, ceremony, performance, sports meet or similar event (i) at which the individual voluntarily appears, and (ii) that is open to the public, or (h) the information is personal identity information that is collected by (i) a provincial identity information services provider and the collection of the information is necessary to enable the provincial identity information services provider to provide services under section 69.2, or (ii) a public body from a provincial identity information services provider and the collection of the information is necessary to enable (A) the public body to identify an individual for the purpose of providing a service to the individual, or (B) the provincial identity information services provider to provide services under section 69.2.
BC PIPA	2	[...] recognizes both the right of individuals to protect their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.
	10	10 (1) On or before collecting personal information about an individual from the individual, an organization must disclose to the individual verbally or in writing (a) the purposes for the collection of the information, and (b) on request by the individual, the position name or title and the contact information for an officer or employee of the organization who is able to answer the individual's questions about the collection. (2) On or before collecting personal information about an individual from another organization without the consent of the individual, an organization must provide the other organization with sufficient information regarding the purpose of the collection to allow that other organization to determine whether the disclosure would be in accordance with this Act.
Canada PA	5 (2)	A government institution shall inform any individual from whom the institution collects personal information about the individual of the purpose for which the information is being collected.
	7	Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be used by the institution except (a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose; or (b) for a purpose for which the information may be disclosed to the institution under subsection 8(2).
Canada PIPEDA	D1 (3)	An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.

Consent

Act	Section	Sample Language
BC FIPPA	26(d)	(d) with respect to personal information collected for a prescribed purpose, (i) the individual the information is about has consented in the prescribed manner to that collection, and (ii) a reasonable person would consider that collection appropriate in the circumstances,
BC PIPA	6(1), 6(2)	Consent required 6 (1) An organization must not (a) collect personal information about an individual, (b) use personal information about an individual, or (c) disclose personal information about an individual. (2) Subsection (1) does not apply if (a) the individual gives consent to the collection, use or disclosure, (b) this Act authorizes the collection, use or disclosure without the consent of the individual, or (c) this Act deems the collection, use or disclosure to be consented to by the individual.
Canada PA	7	Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be used by the institution except (a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose; or (b) for a purpose for which the information may be disclosed to the institution under subsection 8(2).
Canada PIPEDA	6.1	For the purposes of clause 4.3 of Schedule 1, the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.

Exceptions to Consent

Act	Section	Sample Language
BC FIPPA	71	(1) Subject to subsection (1.1), the head of a public body must establish categories of records that are in the custody or under the control of the public body and are available to the public without a request for access under this Act. (1.1) The head of a public body must not establish a category of records that contain personal information unless the information (a) may be disclosed under section 33.1 or 33.2, or (b) would not constitute, if disclosed, an unreasonable invasion of the personal privacy of the individual the information is about. (1.2) Section 22 (2) to (4) applies to the determination of unreasonable invasion of personal privacy under subsection (1.1) (b) of this section. 2) The head of a public body may require a person who asks for a copy of an available record to pay a fee to the public body. (3) Subsection (1) does not limit the discretion of the government of British Columbia or a public body to disclose records that do not contain personal information.

Continued on following page...

BC PIPA	15	(1) An organization may use personal information about an individual without the consent of the individual, if (a) the use is clearly in the interests of the individual and consent cannot be obtained in a timely way, (b) the use is necessary for the medical treatment of the individual and the individual does not have the legal capacity to give consent, (c) it is reasonable to expect that the use with the consent of the individual would compromise an investigation or proceeding and the use is reasonable for purposes related to an investigation or a proceeding, (d) the personal information is collected by observation at a performance, a sports meet or a similar event (i) at which the individual voluntarily appears, and (ii) that is open to the public, (e) the personal information is available to the public from a source prescribed for the purposes of this paragraph, (f) the use is necessary to determine suitability (i) to receive an honour, award or similar benefit, including an honorary degree, scholarship or bursary, or (ii) to be selected for an athletic or artistic purpose, (g) the personal information is used by a credit reporting agency to create a credit report if the individual consented to the disclosure for this purpose, (h) the use is required or authorized by law, (h.1) the personal information was collected by the organization under section 12 (1) (k) or (l) and is used to fulfill the purposes for which it was collected, (i) the personal information was disclosed to the organization under sections 18 to 22, (j) the personal information is needed to facilitate (i) the collection of a debt owed to the organization, or (ii) the payment of a debt owed by the organization, (k) a credit reporting agency is permitted to collect the personal information without consent under section 12 and the information is not used by the credit reporting agency for any purpose other than to create a credit report, or (l) the use is necessary to respond to an emergency that threatens the life, health or security of an individual. (2) An organization may use personal information collected from or on behalf of another organization without the consent of the individual to whom the information relates, if (a) the individual consented to the use of the personal information by the other organization, and (b) the personal information is used by the organization solely (i) for the purposes for which the information was previously collected, and (ii) to assist that organization to carry out work on behalf of the other organization.
Canada PA	7 (a,b)	Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be used by the institution except (a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose; or (b) for a purpose for which the information may be disclosed to the institution under subsection 8(2).
	8 (1)	Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be disclosed by the institution except in accordance with this section.
Canada PIPEDA	7 (1)	7 (1) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may collect personal information without the knowledge or consent of the individual only if (a) the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way; (b) it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province; (b.1) it is contained in a witness statement and the collection is necessary to assess, process or settle an insurance claim; (b.2) it was produced by the individual in the course of their employment, business or profession and the collection is consistent with the purposes for which the information was produced; (c) the collection is solely for journalistic, artistic or literary purposes; (d) the information is publicly available and is specified by the regulations; or (e) the collection is made for the purpose of making a disclosure (i) under subparagraph (3)(c.1)(i) or (d)(ii), or (ii) that is required by law.

Appendix 1.2: Sharing/ Use/ Disclosure

Act	Section	Sample Language
BC FIPPA	32	A public body may use personal information in its custody or under its control only (a) for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose (see section 34), (b) if the individual the information is about has identified the information and has consented, in the prescribed manner, to the use, or (c) for a purpose for which that information may be disclosed to that public body under sections 33 to 36.
	33	There are several cases where a public body can disclose personal information. This section instead summarizes selected cases that may be applicable to educational organizations. • If the individual has consented to disclosure. • Legislation in BC or Canada that authorizes or requires disclosure. • In accordance with the provision of a treaty, arrangement or written agreement. • To an individual who is a minister, officer, or employee of a public body; or an employee or associate of a service provider to a public body. • To an officer or employee of the public body, or to a minister, if the information is urgently needed for the health and safety of that individual. • For legal purposes. • To the minister responsible for the Coroners Act. • For the purposes of facilitating payments to the Province. • For the purposes of regulatory bodies related to professional occupations. • For the purpose of reducing the risk of violence or harm. • If the information was collected by observation at a public event that the individual voluntarily attended. • The information was disclosed by the individual on social media, was compiled by the public body for the purpose of engaging individuals in discussion or promotion. • Is for research or statistical purposes.
BC PIPA	17	Subject to this Act, an organization may disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances and that (a) fulfill the purposes that the organization discloses under section 10 (1), (b) for information collected before this Act comes into force, fulfill the purposes for which it was collected, or (c) are otherwise permitted under this Act.
	18	(1) An organization may only disclose personal information about an individual without the consent of the individual, if (a) the disclosure is clearly in the interests of the individual and consent cannot be obtained in a timely way, (b) the disclosure is necessary for the medical treatment of the individual and the individual does not have the legal capacity to give consent, (c) it is reasonable to expect that the disclosure with the consent of the individual would compromise an investigation or proceeding and the disclosure is reasonable for purposes related to an investigation or a proceeding, (d) the personal information is collected by observation at a performance, a sports meet or a similar event (i) at which the individual voluntarily appears, and (ii) that is open to the public, (e) the personal information is available to the public from a source prescribed for the purposes of this paragraph, (f) the disclosure is necessary to determine suitability (i) to receive an honour, award or similar benefit, including an honorary degree, scholarship or bursary, or (ii) to be selected for an athletic or artistic purpose, (g) the disclosure is necessary in order to collect a debt owed to the organization or for the organization to repay an individual money owed to them by the organization, (h) the personal information is disclosed in accordance with a provision of a treaty that (i) authorizes or requires its disclosure, and (ii) is made under an enactment of British Columbia or Canada,

Continued on following page...

		(i) the disclosure is for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body with jurisdiction to compel the production of personal information, (j) the disclosure is to a public body or a law enforcement agency in Canada, concerning an offence under the laws of Canada or a province, to assist in an investigation, or in the making of a decision to undertake an investigation, (i) to determine whether the offence has taken place, or (ii) to prepare for the laying of a charge or the prosecution of the offence, (k) there are reasonable grounds to believe that compelling circumstances exist that affect the health or safety of any individual and if notice of disclosure is mailed to the last known address of the individual to whom the personal information relates, (l) the disclosure is for the purpose of contacting next of kin or a friend of an injured, ill or deceased individual, (m) the disclosure is to a lawyer who is representing the organization, (n) the disclosure is to an archival institution if the collection of the personal information is reasonable for research or archival purposes, (o) the disclosure is required or authorized by law, or (p) the disclosure is in accordance with sections 19 to 22.
Canada PA	2	(2) Subject to any other Act of Parliament, personal information under the control of a government institution may be disclosed (a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose; (b) for any purpose in accordance with any Act of Parliament or any regulation made thereunder that authorizes its disclosure; (c) for the purpose of complying with a subpoena or warrant issued or order made by a court, person or body with jurisdiction to compel the production of information or for the purpose of complying with rules of court relating to the production of information; (d) to the Attorney General of Canada for use in legal proceedings involving the Crown in right of Canada or the Government of Canada; (e) to an investigative body specified in the regulations, on the written request of the body, for the purpose of enforcing any law of Canada or a province or carrying out a lawful investigation, if the request specifies the purpose and describes the information to be disclosed; (f) under an agreement or arrangement between the Government of Canada or any of its institutions and the government of a province, the council of the Westbank First Nation, the council of a participating First Nation as defined in subsection 2(1) of the First Nations Jurisdiction over Education in British Columbia Act, the council of a participating First Nation as defined in section 2 of the Anishinabek Nation Education Agreement Act, the government of a foreign state, an international organization of states or an international organization established by the governments of states, or any institution of any such government or organization, for the purpose of administering or enforcing any law or carrying out a lawful investigation; (g) to a member of Parliament for the purpose of assisting the individual to whom the information relates in resolving a problem; (h) to officers or employees of the institution for internal audit purposes, or to the office of the Comptroller General or any other person or body specified in the regulations for audit purposes; (i) to the Library and Archives of Canada for archival purposes; (j) to any person or body for research or statistical purposes if the head of the government institution (i) is satisfied that the purpose for which the information is disclosed cannot reasonably be accomplished unless the information is provided in a form that would identify the individual to whom it relates, and (ii) obtains from the person or body a written undertaking that no subsequent disclosure of the information will be made in a form that could reasonably be expected to identify the individual to whom it relates; (k) to any aboriginal government, association of aboriginal people, Indian band, government institution or part thereof, or to any person acting on behalf of such government, association, band, institution or part thereof, for the purpose of researching or validating the claims, disputes or grievances of any of the aboriginal peoples of Canada;

Continued on following page...

		(l) to any government institution for the purpose of locating an individual in order to collect a debt owing to Her Majesty in right of Canada by that individual or make a payment owing to that individual by Her Majesty in right of Canada; and (m) for any purpose where, in the opinion of the head of the institution, (i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or (ii) disclosure would clearly benefit the individual to whom the information relates.
Canada PIPEDA	4.5	Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.
	7.2	(2) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may, without the knowledge or consent of the individual, use personal information only if (a) in the course of its activities, the organization becomes aware of information that it has reasonable grounds to believe could be useful in the investigation of a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, and the information is used for the purpose of investigating that contravention; (b) it is used for the purpose of acting in respect of an emergency that threatens the life, health or security of an individual; (b.1) the information is contained in a witness statement and the use is necessary to assess, process or settle an insurance claim; (b.2) the information was produced by the individual in the course of their employment, business or profession and the use is consistent with the purposes for which the information was produced; (c) it is used for statistical, or scholarly study or research, purposes that cannot be achieved without using the information, the information is used in a manner that will ensure its confidentiality, it is impracticable to obtain consent and the organization informs the Commissioner of the use before the information is used; (c.1) it is publicly available and is specified by the regulations; or (d) it was collected under paragraph (1)(a), (b) or (e).
	7.3	Recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances. Disclosure without knowledge or consent (3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is (a) made to, in the Province of Quebec, an advocate or notary or, in any other province, a barrister or solicitor who is representing the organization; (b) for the purpose of collecting a debt owed by the individual to the organization; (c) required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records; (c.1) made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that (i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs, (ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, (iii) the disclosure is requested for the purpose of administering any law of Canada or a province, or (iv) the disclosure is requested for the purpose of communicating with the next of kin or authorized representative of an injured, ill or deceased individual; (c.2) made to the government institution mentioned in section 7 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act as required by that section;

Continued on following page...

7.3	(d) made on the initiative of the organization to a government institution or a part of a government institution and the organization (i) has reasonable grounds to believe that the information relates to a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, or (ii) suspects that the information relates to national security, the defence of Canada or the conduct of international affairs; (d.1) made to another organization and is reasonable for the purposes of investigating a breach of an agreement or a contravention of the laws of Canada or a province that has been, is being or is about to be committed and it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the investigation; (d.2) made to another organization and is reasonable for the purposes of detecting or suppressing fraud or of preventing fraud that is likely to be committed and it is reasonable to expect that the disclosure with the knowledge or consent of the individual would compromise the ability to prevent, detect or suppress the fraud; (d.3) made on the initiative of the organization to a government institution, a part of a government institution or the individual's next of kin or authorized representative and (i) the organization has reasonable grounds to believe that the individual has been, is or may be the victim of financial abuse, (ii) the disclosure is made solely for purposes related to preventing or investigating the abuse, and (iii) it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the ability to prevent or investigate the abuse; (d.4) necessary to identify the individual who is injured, ill or deceased, made to a government institution, a part of a government institution or the individual's next of kin or authorized representative and, if the individual is alive, the organization informs that individual in writing without delay of the disclosure; (e) made to a person who needs the information because of an emergency that threatens the life, health or security of an individual and, if the individual whom the information is about is alive, the organization informs that individual in writing without delay of the disclosure; (e.1) of information that is contained in a witness statement and the disclosure is necessary to assess, process or settle an insurance claim; (e.2) of information that was produced by the individual in the course of their employment, business or profession and the disclosure is consistent with the purposes for which the information was produced; (f) for statistical, or scholarly study or research, purposes that cannot be achieved without disclosing the information, it is impracticable to obtain consent and the organization informs the Commissioner of the disclosure before the information is disclosed; (g) made to an institution whose functions include the conservation of records of historic or archival importance, and the disclosure is made for the purpose of such conservation; (h) made after the earlier of (i) one hundred years after the record containing the information was created, and (ii) twenty years after the death of the individual whom the information is about; (h.1) of information that is publicly available and is specified by the regulations; or (h.2) [Repealed, 2015, c. 32, s. 6] (i) required by law.

Appendix 2: Data Governance Interview Template

Thank you for taking the time to discuss your institution's/organization's data governance program. As mentioned in our email, this research project is sponsored by the British Columbia (Canada) Council on Admissions and Transfer, and aims to better understand the data governance landscape in education, healthcare, and government. It is our hope that we can name your organization as a participant in this process, but if you'd prefer to remain anonymous, please let us know. We will be taking notes during the interview - if there is anything that you'd like off the record, just let us know and we will not record it. At this time that we should stress that there are no right or wrong answers for this type of research - it is exploratory in nature. Whether you are new to data governance or consider yourself and organization seasoned veterans, your perspective will help others in the community looking to learn more about data governance.

1. Requests Anonymity? (Yes/No)

We have a handful of questions to guide today's conversation, but certainly welcome any new conversation topics as we go. If there's an area that is outside your domain of knowledge, you are welcome to pass or suggest that there is someone else at the organization who we should reach out to.

The rough ordering of this interview will be from high-level into detail, starting with questions about your data governance program in general, moving to questions that focus on more specific aspects related to it, and a couple summary experience questions.

We'll start with the high-level questions:

2. Do you have a data governance program / initiative in place currently? If so, how long has it been in place?
3. Prior to establishing data governance as a program / initiative, are you aware whether it took place informally? Approximately how far back were conscious efforts made with respect to data governance?
4. What was the motivation behind focusing more on data governance? (ie: institutional priority, legislation, policy, etc)
5. What are the goals of your data governance program?
6. Does your organization follow a particular data governance framework; did you adapt one for your organization, or build one from scratch? Are there any materials around your framework online or that you can share?

In this section, we move to the more granular questions:

7. Is responsibility for data governance centralized or shared across units? If centralized, which group leads it? How do you ensure buy-in across the organization?
8. In terms of roles and responsibilities related to data governance, does your organization have any of the following (yes/no with elaboration if needed.
    - Executive / leadership sponsorship (data governors)?
    - Data governance steering committee?
    - What types of people are on this? How frequently do they meet?
    - Data owners?
        - What types of people fill these roles? Do they meet?

- Data stewards.
    - What types of people fill these roles? Do they meet?
- Data stakeholders, producers, custodians, brokers, and consumers, others?

9. In terms of tools, do you utilize any of the following?:
    - Business glossaries (such as Data Cookbook, Collibra, etc)
    - Data lineage tools
    - Common information repositories (data warehouse, data lake, etc)
    - Extract, Transform, Load tools
    - Templates, such as those for mapping infrastructure, architecture, and tools
10. Does your organization have specific policies in place related to the following domains?
    - Data collection
    - Data storage
    - Information security
    - Information sharing
    - Internal reporting and analysis
    - Public reporting and analysis

Last but not least, a couple of summary questions:

11. What do you feel is working particularly well about your data governance program? What areas do you feel could be improved?

12. Do you have any advice for organizations just beginning their data governance journey?

13. Are there any materials around your framework online or that you can share?

14. Anything else we should have asked you?

Thank you so very much for taking the time to discuss data governance with us today. Your insight will help others learn more about this process in the future. Over the coming months, we will conduct several other interviews like this one, in addition to deep scans of national and subnational legislation and organizational policy. We expect a final draft of the report to be with BCCAT's research committee early in 2020, with the hope that a report will be published in spring (subject to approval, of course).

Appendix 3: Online Survey Instrument

The British Columbia Council on Admissions & Transfer (BCCAT) has contracted Plaid Consulting (https://plaid.is) to conduct a study on data governance policy models at post-secondary institutions, related central data repositories, and health and governmental organizations.

This survey aims to learn more about data governance policy and practice at your institution/organization. The survey will take approximately 10 minutes to complete. Your responses will help to provide a strong understanding and benchmarking of data governance in education, health, and government. Your institution/organization will remain anonymous in publication, but will be known to the researchers should you provide this information.

We appreciate your time and thank you in advance for contributing to this project.

For more information about this project please contact:

- Plaid Consulting at info@plaid.is
- BCCAT at info@bccat.ca

Survey responses will be encrypted and stored securely in Canada; following completion of the study they will be destroyed. Survey responses will not be linked to individual institutions in publication.

Publishing will be at the discretion of the BC Council on Admissions and Transfer. Often their work is published on their website at bccat.ca.

Your completion of the survey implies informed consent.

If you wish to revoke your consent, you can either not participate in the survey, or fill in the option provided on the final survey page.

1. What country are you primarily located in for your work? (Select One)

- Canada
- United States
- Other (please specify)

2. What province/territory are you primarily located in for your work? (Select One)

- asked only of those who selected "Canada" in Question 1.

3. What state/district are you primarily located in for your work

- asked only of those who selected "United States" in Question 1.

4. Which industry do you primarily work in? (Select One)

- Education
- Health
- Government
- Other

If Other: This survey is primarily targeted at those working in education, health, and government. While your response to this survey is greatly appreciated, it may not be used for further analysis.

5. Which organization do you primarily work for? If you prefer that your organization remain anonymous, please leave this field blank.

6. What category best describes your institution/organization (Select One)

- asked only of those who selected "Education" in Question 4.

- Post-Secondary Institution
- Common Data Repository / Application Service
- K-12 Educational Institution (eg: High School)
- School Board
- Ministry responsible for Education
- Ministry responsible for Advanced Education
- Other

7. Which sector best describes your post-secondary institution? (Select Many)

- asked only of those who selected "Education" in Question 4.

- Member of Colleges and Institutes Canada
- Member of Polytechnics Canada
- Member of Universities Canada
- 2-year college/university in the United States
- 4-year college/university in the United States
- Other

8. Is your institution public or private? (Select One)

- asked only of those who selected "Education" in Question 4.

- Public
- Private

9. What category best describes your health organization? (Select One)

- asked only of those who selected "Health" in Question 4.

- Health authority
- Hospital
- Other healthcare facility
- Other health care administration

10. What category best describes your governmental organization? (Select One)

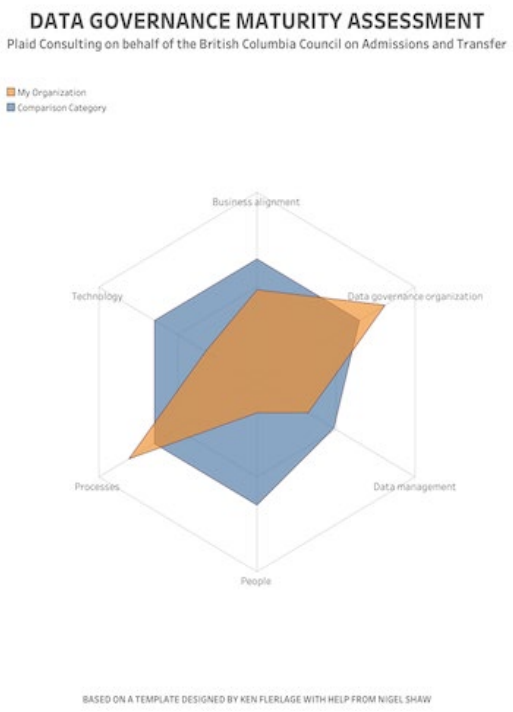
- asked only of those who selected "Government" in Question 4.

- National government ministry
- Subnational government ministry
- National arms-length government branch (government entity with limited direct government control, crown corporation, state corporation, etc.)
- Subnational arms-length government branch (government entity with limited direct government control, crown corporation, state corporation, etc.)
- Other

11. Would you like to receive a report that benchmarks your institution based on this survey? (Select One). As part of the final report, our hope is to be able to benchmark based on aggregate groups as defined previously. We will not publish individual organizational benchmarks in the report, but we'd be happy to provide you a custom chart (as a PDF) that shows how your institution/organizations compares to the averages of other organizations surveyed. An example of such is shown below. Note that you'll need to provide your contact information in order for us to send this to you.

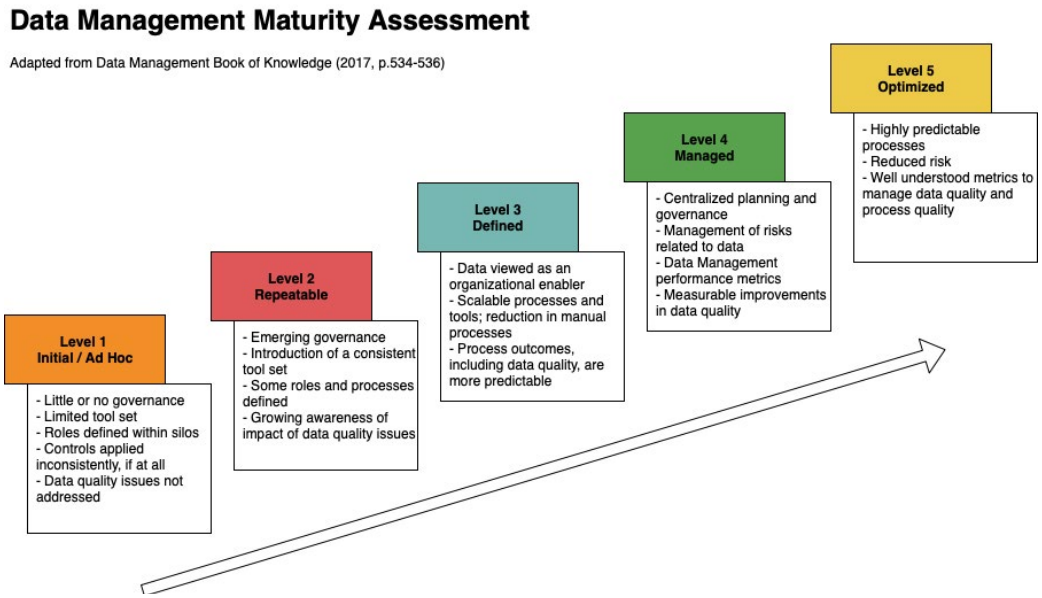
- Yes
- No

If yes - Please enter your email address



Benchmark

In this section, you will be asked to fill in a series of Likert scale questions for categories related to data governance. In all cases, the responses are from 1 (Initial / Ad Hoc) to 5 (Optimizing), plus options for "not applicable" and "I don't know", as shown in the chart below.



A more detailed set of definitions for the maturity levels is shown In **Table 3** (note that this table was originally shown within the online survey instrument – it is omitted here for brevity).

The definitions of each category to be rated are shown below.

Category	Definition	Reference
People	Organizational staff are aware of the importance of data governance, have integrated awareness in the organizational culture, and are able to effectively implement it.	For this study
Processes	The organization has processes and practices related to the effective planning, management, security, and documentation of data.	For this study
Technology	The organization has appropriate technology supports in place to facilitate data governance. This could include metadata management tools, data dictionaries, and/or data lineage systems, among others.	For this study
Data management	Data is treated as a valuable business asset that needs proactive management across a range of dimensions such as quality, access, and metadata throughout the data lifecycle.	Gregory (2011)
Business alignment	Both IT and line business organizations work towards a positive relationship with an alignment in data governance goals.	Luftman (2003)
Data governance organization	The organization has well defined data governance goals and appropriate structures aligned to those goals.	Otto (2011)

References were shown in the online survey but are now in the **References** section.

12. Please rate your organization on a scale consisting of 1 (Initial / Ad Hoc), 2 (Repeatable), 3 (Defined), 4 (Managed), 5 (Optimized) plus Not Applicable and I do not know based on the definitions in Table 3. This question showed a Likert scale with the following levels for each of six areas: People, Processes, Technology, Data Management, Business Alignment, and Data Governance Organization

13. Does your institution/organization practice data governance due to any of the following influences? (Select Many)

- Federal legislation
- Provincial/State legislation
- Local legislation
- Institution/organization policy
- Institution/organization practice

14. Does your institution/organization have any data governance-related materials posted online that you can share with us? If so, please provide the link(s) below.

If materials are only in document format, you can email them to info@plaid.is

15. Does your institution/organization have a data governance program in place currently? (Select One)

- Yes
- No

16. Please help us better understand the size of your data governance team(s) relative to your overall organizational size. Approximately how many full-time equivalent staff belong to the following groups?

- Within the core data governance team
- Within distributed data governance team(s)
- Within the organization overall

Respondents were able to select from bins including:
1-2, 3-4, 5-9, 10-24, 25-49, 50-99, 100-249, 250-499, 500-999, 1,000-4,999, and 5,000+

17. How long has your data governance program existed?

- 5 or more years
- 3-4 years
- 1-2 years
- New

18. In the context of how well established your DG program is, On a scale of 1-5, how successful are your data governance efforts to date? (Select One)

- Very unsuccessful
- Somewhat unsuccessful
- Neutral
- Somewhat successful
- Very successful

19. Is there any advice you'd give to institutions/organizations just beginning their data governance journey?

20. Would you be interested in participating in a follow up interview to discuss your data governance program in more detail?

- Yes
- No

21. Would you like to be emailed when a final version of the report is published?

Note: The British Columbia Council on Admissions and Transfer will make the final decision on whether to publish or not publish this work.

- Yes
- No

22. What is your name?

- Only asked of those who said yes to questions 19 or 20

We'll use this information to contact you based on your interest in either a follow up interview or an emailed copy of the final report

23. Please enter your email address

- Only asked of those who said yes to questions 19 or 20

This information may be pre-populated if you provided an email address earlier in the survey.

Optional - If you wish to revoke your informed consent, please type the word "Revoke"; into the box below, and click Submit. If you still wish to be included in the study, please leave this box blank, and click Submit.

Due to the anonymous nature of this survey, once you hit Submit and have not typed “Revoke”, your data cannot be removed.

Thanks very much for completing this survey!

Your feedback will help to inform data governance practices in education, health, and government. Please remember to hit the Submit button below.

For more information about this project please contact:

- Plaid Consulting at info@plaid.is
- BCCAT at info@bccat.ca

To learn more about Plaid’s privacy policy click here.

Appendix 4: Example of a Privacy Breach Report

This is Simon Fraser University's Privacy Breach Report form as it existed on November 18, 2019.

Page 1 of 5

SFU SIMON FRASER UNIVERSITY ENGAGING THE WORLD

Archives and Records Management

Privacy Breach Report

A privacy breach occurs when there is unauthorized access to or collection, use, disclosure or disposal of personal information.

To report a privacy breach, complete and submit this online form. Fields marked with an asterisk (*) are mandatory, i.e. the form will not submit if they are left blank. Please note that you cannot save this form; you must complete it and submit it in a single session. Upon submitting the form, you will receive an email that includes all the data that you entered. The Information and Privacy Officer may contact you with follow-up questions upon receiving your report.

Contact information

SFU Department *

Contact name *

FirstName LastName

Job title *

Telephone

Email *

Incident description

Date of breach

Choose date...

Date breach discovered

Choose date...

Page 2 of 5

Date reported to SFU Information and Privacy Officer

18 November, 2019

Description of breach *

Accessed or disclosed outside Canada?

- Yes
- No

Was the personal information accessed from or disclosed outside Canada?

Stored on server outside Canada?

- Yes
- No

Is the personal information being stored on a server or servers outside Canada? If yes, provide name of service provider and location of server(s) below

Service provider

Location of server

Enter city and country

Individuals affected

Types of individuals affected

- SFU staff
- SFU faculty / instructors
- SFU students
- SFU alumni
- SFU retirees
- Other external third parties

Number of individuals whose privacy was breached

Number of individuals who inappropriately received information

Page 3 of 5

Additional information relating to affected individuals

Personal Information breached

Types of personal information breached

- [ ] Personal contact information
- [ ] Age / birthdate
- [ ] Sex
- [ ] Marital or family status
- [ ] Identifying number
- [ ] Race or national or ethnic origin
- [ ] Educational history
- [ ] Medical history
- [ ] Disabilities
- [ ] Blood type
- [ ] Religious / political beliefs / associations
- [ ] Employment history
- [ ] Financial history
- [ ] Criminal history
- [ ] Images
- [ ] Contact information of family member

Select all that apply; elaborate below in "Additional information relating to personal information breached"

Additional information relating to personal information breached

Safeguards

Existing physical security measures

- [ ] Locked offices / desks / file cabinets
- [ ] Alarm systems
- [ ] Surveillance video
- [ ] Other

Select all that apply; elaborate below in "Additional information relating to safeguards"

Existing technical security measures

Page 4 of 5

- [ ] Passwords
- [ ] Encryption
- [ ] Other

Select all that apply; elaborate below in "Additional information relating to safeguards"

Existing procedural security measures

- [ ] Security clearances
- [ ] Systems access protocols / restrictions
- [ ] Policies and procedures
- [ ] Training / education
- [ ] Contractual provisions
- [ ] Other

Select all that apply; elaborate below in "Additional information relating to safeguards"

Additional information relating to safeguards

Harm resulting from breach

Types of harm resulting from breach

- [ ] Identity theft
- [ ] Physical harm
- [ ] Hurt / humiliation / damage to reputation
- [ ] Loss of business / employment / educational opportunities
- [ ] Breach of contractual obligations
- [ ] Future breaches due to similar technical failures
- [ ] Failure to meet professional or certification standards
- [ ] Other

Select all that apply; elaborate below in "Additional information relating to harm"

Additional information relating to harm

Mitigation and prevention

Immediate steps taken to contain and reduce harm resulting from breach

- [ ] Information deleted or recovered
- [ ] Police notified

Page 5 of 5

- [ ] Locks changed
- [ ] Security codes changed
- [ ] Passwords changed
- [ ] Systems access privileges revoked
- [ ] Information systems shut down
- [ ] Other

Select all that apply; elaborate below in "Additional information relating to mitigation and prevention"

Long-term strategies to correct the situation

- [ ] Staff training
- [ ] Revise / develop policy or procedures
- [ ] Privacy and security audit
- [ ] Change bulk email address
- [ ] Contractor supervision strategies
- [ ] Revise / develop contract language
- [ ] Other

Select all that apply; elaborate below in "Additional information relating to mitigation and prevention"

Additional information relating to mitigation and prevention

Submit Reset

BCCAT

Your guide through post-secondary education.