Applied A.I. Solutions

Foundations of Data Management
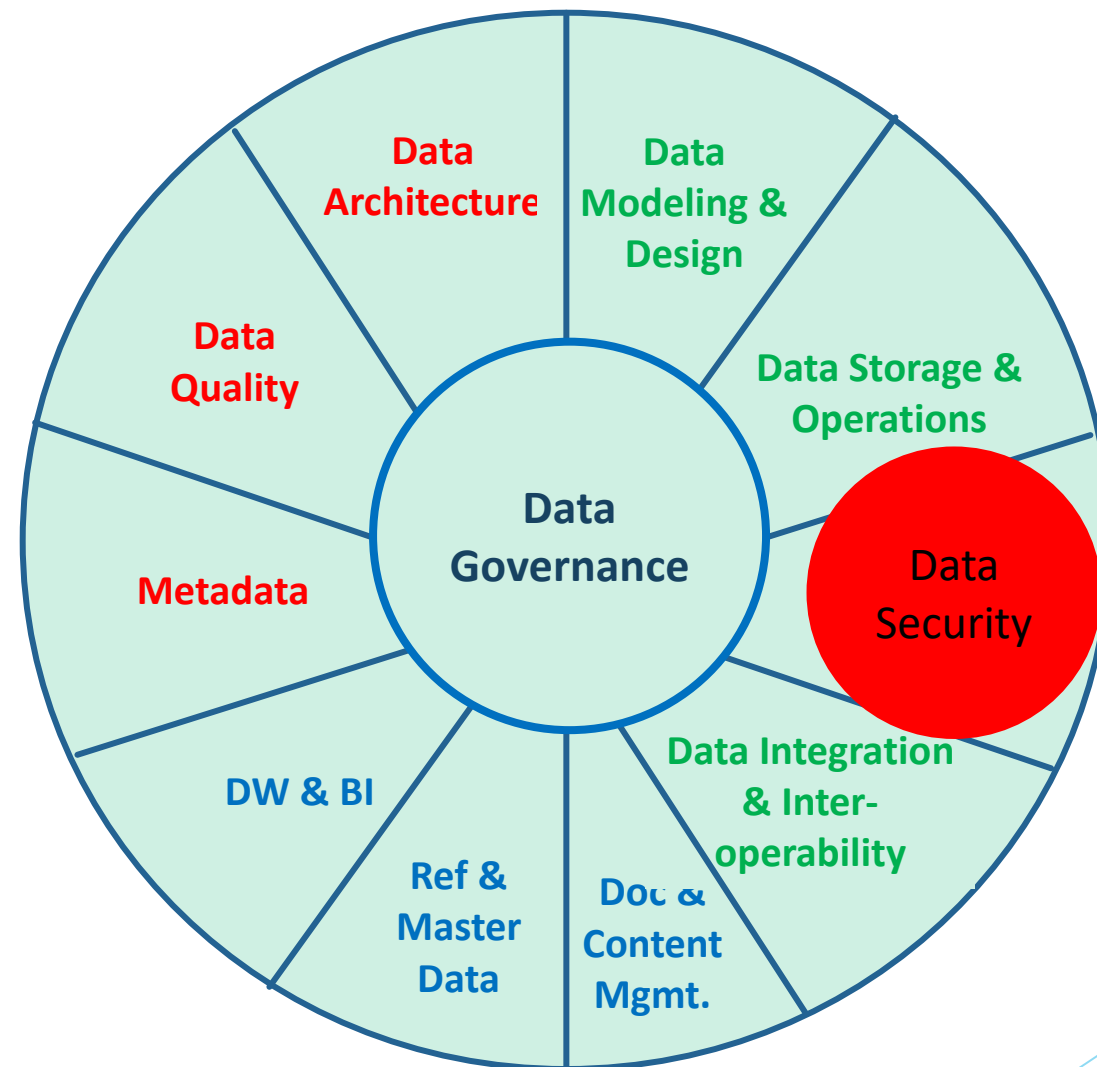
Professor
Daniel Vitaver-Bronstein, B.Sc., EMBA

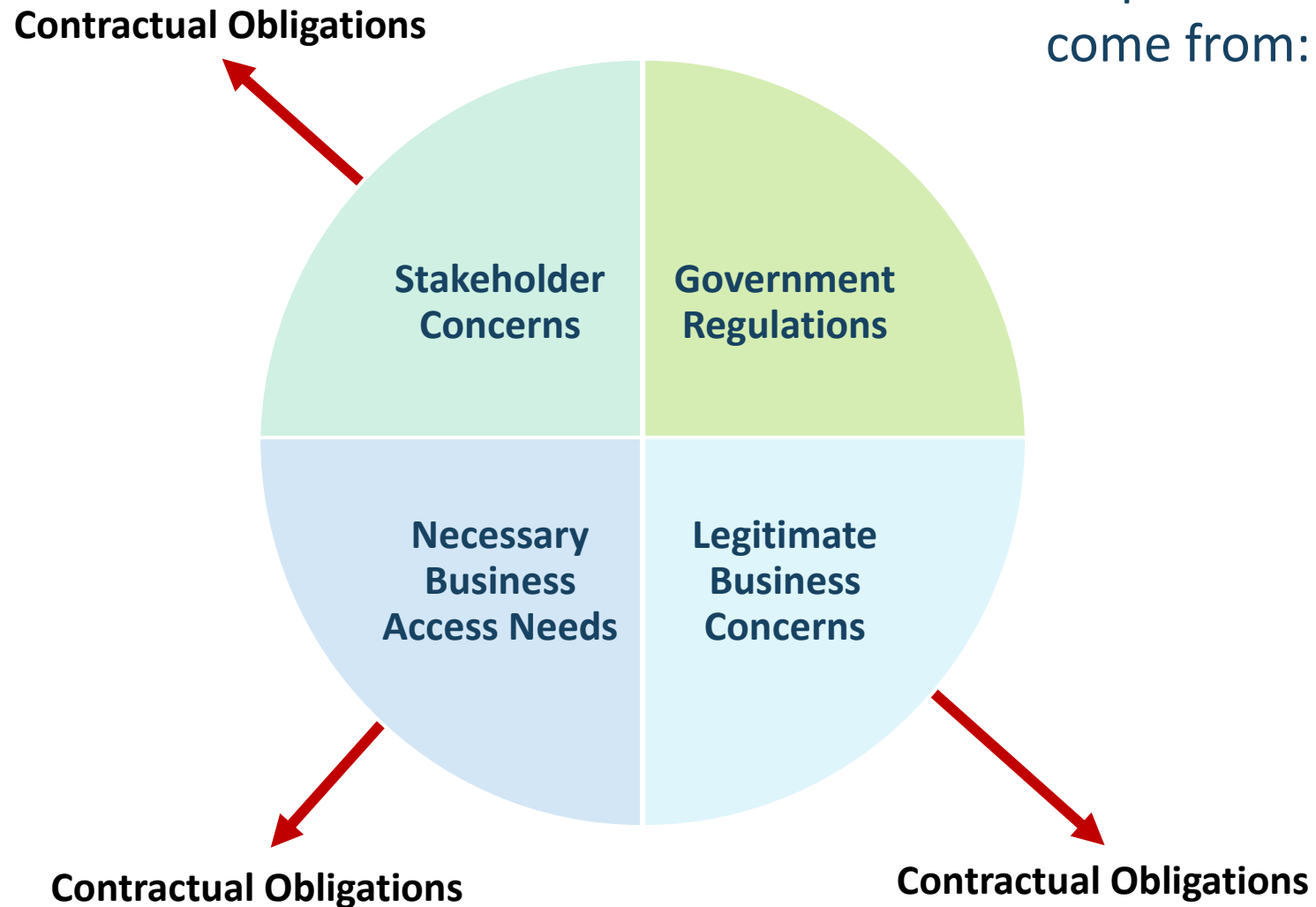daniel.vitaver-bronstein@georgebrown.ca

DATA SECURITY

The DAMA Wheel

1. INTRODUCTION

- ==Protect== information assets in alignment with privacy and confidentiality regulations, contractual agreements, and business requirements

- Ensure that the right people can use, update data in the right way, and that all inappropriate ==access==, update is restricted

Requirements come from:

Contractual Obligations

Stakeholder Concerns

Government Regulations

Necessary Business Access Needs

Legitimate Business Concerns

Contractual Obligations

Contractual Obligations

Data Security Management Framework

Definition

Definition, planning, development, and execution of security policies and procedures to provide proper authentication, authorization access, and auditing of data and information assets

Goals

1. Enabling appropriate, and preventing inappropriate access to data assets

2. Enabling compliance with regulations, policies for privacy, protection, and confidentiality

3. Ensuring that stakeholder requirements for privacy and confidentiality are met

Business   Drivers

DS programs are guided by the following principles:

1. Collaboration

2. Enterprise approach

3. Proactive management

4. Clear accountability

5. Metadata-driven

6. Reduce risk by reducing exposure

Inputs

- Business goals and strategy

- Business rules and processes

- Regulatory requirements

- Enterprise architecture standards

- Enterprise data model

Activities

1. Identify relevant data security requirements

2. Define data security policy

3. Define data security standards

4. Assess current security risks

5. Implement controls and procedures

Deliverables

1. Data security architecture
2. Data security policies
3. Data privacy and confidentiality standards
4. Data security access controls
5. Regulatory compliant data access views
6. Documented security classifications
7. Authentication and user access history
8. Data security audit reports

Suppliers	Participants	Consumers
• IT Steering committee • Enterprise architects • Government • Regulatory bodies	• Data Stewards • Information Security Team • Internal Auditors • Process Analysts	• Business Users • Regulatory Auditors

Technical Drivers

Techniques
- CRUDE Matrix Usage
- Immediate security patch deployment
- DS attributes in metadata
- Security needs in project requirements
- Document Sanitization

Tools
- Access control systems
- Protective software
- Identify management tech
- Intrusion detection/ prevention software
- Metadata tracking
- Data masking/ encryption

Metrics
- Security implementation, awareness, incident metrics
- Confidential data proliferation rate

Drivers

1. <mark>Risk Reduction</mark>

   - Identify and classify sensitive data assets

   - Determine how each asset needs to be protected

   - Identify how the information interacts with business

     processes (access)

2. <mark>Business Growth</mark>

   - Security as an Asset

Data Security Essential Concepts

1. Vulnerability
2. Threat
3. Risk
4. Risk Classification
5. Data Security Organization (CISO)
6. Security Processes
7. Encryption
8. Data Integrity

9. Masking
10. Network Security Terms
11. Types of Data Security
12. Types of Data Security Restrictions
13. System Security Risks
14. Hacking
15. Social Threats / Phishing
16. Malware

Risk

Main Risk Factors

- Damage on revenue, business operations and reputation

- Cost to prevent the threat, remediate of vulnerabilities

Risk Classification

- Critical   – Personal Information / financial / health value

- High   – potential direct PI / financial / health value

- Moderate   – little tangible value

Security Processes

- The Four A's

  o Access
  o Audit
  o Authentication
  o Authorization
  o Entitlement

- Monitoring

Encryption

- Hash

- Private-key

- Public-key

Masking

Types

- Persistent Data Masking
  - In-flight persistent masking
  - In-place persistent masking

- Dynamic Data Masking

Methods

- Substitution
- Shuffling
- Temporal variance
- Value variance
- Nulling or deleting
- Randomization
- Encryption
- Expression masking
- Key masking

Types of Data Security Restrictions

- Confidential Level

  o Confidential Data

    – For general audience

    – Internal use only

    – Confidential

    – Restricted confidential

    – Registered confidential

- Regulations

  o Regulated Data

    – Personal Identification Inf. / PIPEDA

    – Financial Sensitive Data

    – Medically Sensitive Data / PHIPA

    – Educational Records

2. ACTIVITIES

a) **Identify Data Security Requirements**

- Business Requirements

- Regulatory Requirements

b) **Define Data Security Policy**

- Enterprise Security Policy

- IT Security Policy

- Data Security Policy

c) **Define Data Security Standards**

- Define Data Confidentiality Levels

- Define Data Regulatory Categories

- Define Security Roles

- Assess Current Security Risks

- Implement Controls and Procedures

Note: for more details refer to DAMA-DMBOK2

3. TOOLS

- Anti-virus software / Security software

- HTTPS

- Identity Management Technology

- Intrusion Detection and Prevention Software

- Firewalls

- Metadata Tracking

- Data Masking / Encryption

4. TECHNIQUES

- <mark>CRUD(E) Matrix Usage</mark>

- Immediate Security Patch Deployment

- Data Security Attributes in Metadata

- Security Needs in Project Requirements

- Document Sanitization or Metadata Cleaning

Note: for more details refer to DAMA-DMBOK2

Properties ~

Size	Not saved yet
Pages	1
Words	0
Total Editing Time	0 Minutes
Title	Foundations of Data Mana.
Tags	AI
Comments	Professor Privileges
Template	Normal.dotm
Status	Active
Categories	AI/ML
Subject	Applied AI Solution
Hyperlink Base	georgebrown.ca
Company	George Brown College

Related Dates

Last Modified	
Created	Today, 11:30 AM
Last Printed	

Related People

Manager	Specify the manager
Author	DV Daniel Vitaver
	Add an author
Last Modified By	Not saved yet

5. IMPLEMENTATION GUIDELINES

- Readiness Assessment / Risk Assessment

  - Training
  - Consistent policies
  - Measure the benefit of security
  - Set security requirements for vendors
  - Build a sense of urgency
  - Ongoing communications

- Organization and Cultural Change

- Data Security in an Outsourced World

- Data Security in Cloud Environments

- Metrics
    a) Security Implementation Metrics

    b) Security Awareness Metrics

    c) Data Protection Metrics

    d) Security Incident Metrics

    e) Confidential Data Proliferation

6. DATA SECURITY GOVERNANCE

- Data Security and Enterprise Architecture

  o Component of the Enterprise Architecture

  o Describes how data security is implemented to satisfy the business rules and external regulations