Big Data Governance
and IBDG Certification Programme

Hong Kong Software Industry Association Seminar

12 Nov 2021

iBDG
Institute of Big Data Governance

About the Speakers

Vincent Chan

Vice Chairman,
Institute of Big Data Governance

Charleston Sin

Secretary General,
Institute of Big Data Governance

Juliet Zhu

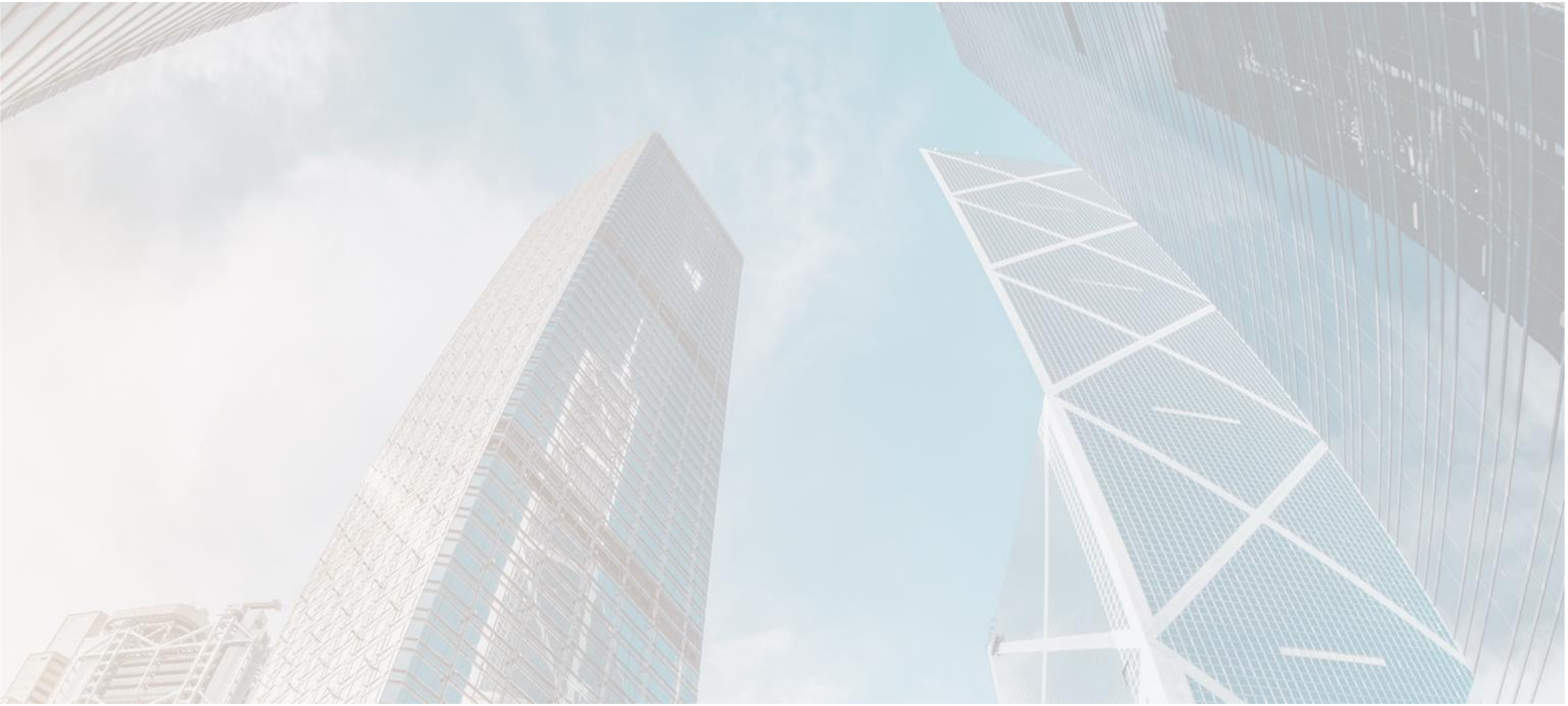
Certification Committee Member
and Lead Author of IBDG Certification Scheme,
Institute of Big Data Governance

Agenda

- Part I : About iBDG
- Part II : Data Governance – Why Do We Care? Regulations Around the World
- Part III - A : Data Governance Best Practice and Independent Verifications – Who Needs to Do What?
- Part III - B : iBDG Big Data Governance Best Practice and Certification Programme
- Part IV : How iBDG Big Data Governance Certification Aligns with Regulations
- Part V : Questions & Answers Session

- Appendix : iBDG Data Governance Assessment Criteria – A Closer Look

Part I -
About iBDG



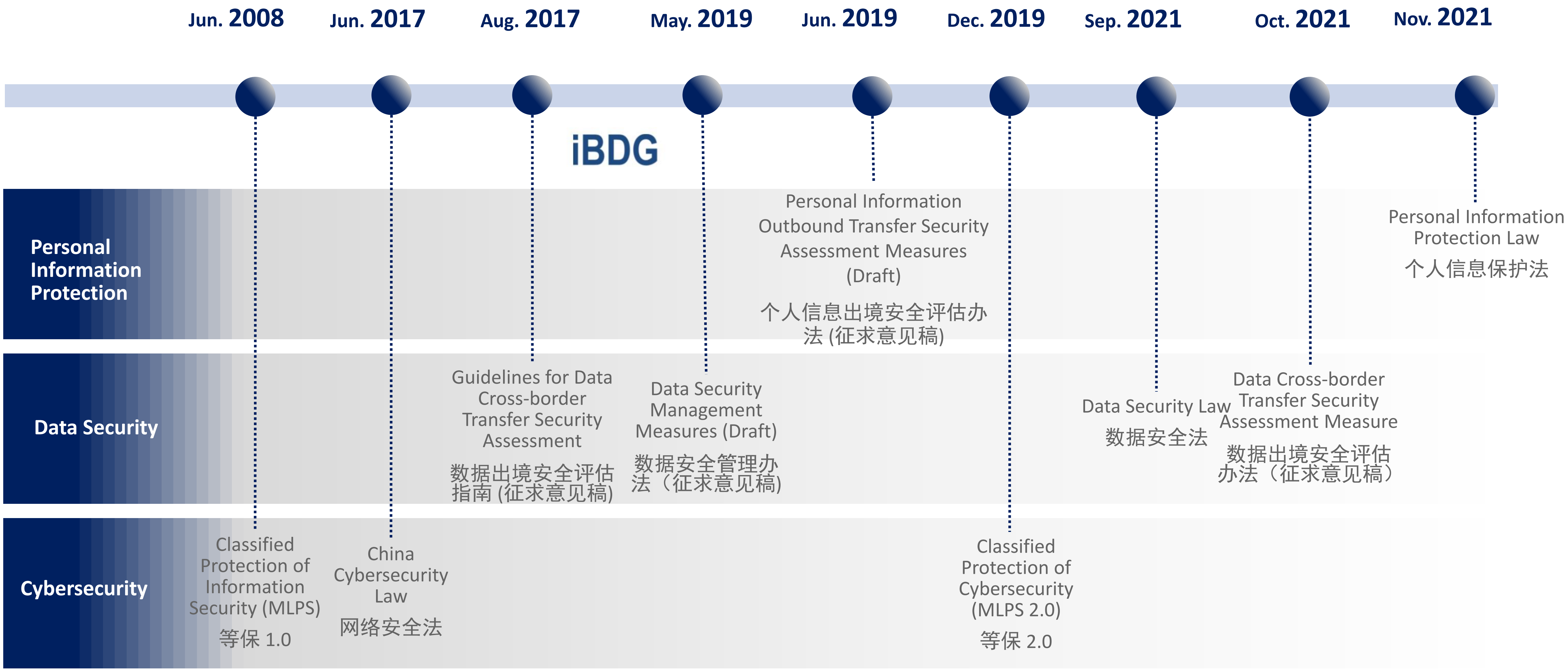
About iBDG – Our Organization

The Institute of Big Data Governance (iBDG)
(香港大数据治理公会)

To allow industry members to comply with the self-regulated governance, iBDG provides the data governance standards, principles and best practices to follow. We also facilitates cross-border data flow by the recognized audits and assessments.

- ➢ Establish Hong Kong as an international data hub, and to foster Hong Kong's high value-add proposition globally by promoting good self-governance for the Big Data industry.
- ➢ Foster self-regulations and provide oversight on members' adherence to governance principles established by the Institute.
- ➢ Act as a conduit between Hong Kong Big Data industry and overseas jurisdictions in the development of Hong Kong as an international data hub.
- ➢ Facilitate innovation and technological development through the effective and proper use of Big Data.

iBDG started along-side with the regulations on Data Security, Personal Information Protection, and Data Cross Border Transfer



Jun. 2008

Jun. 2017

Aug. 2017

May. 2019

Jun. 2019

Dec. 2019

Sep. 2021

Oct. 2021

Nov. 2021

iBDG

Personal Information Protection

Personal Information Outbound Transfer Security Assessment Measures (Draft)

个人信息出境安全评估办法 (征求意见稿)

Personal Information Protection Law

个人信息保护法

Data Security

Guidelines for Data Cross-border Transfer Security Assessment

数据出境安全评估指南 (征求意见稿)

Data Security Management Measures (Draft)

数据安全管理办法（征求意见稿)

Data Security Law

数据安全法

Data Cross-border Transfer Security Assessment Measure

数据出境安全评估办法（征求意见稿）

Cybersecurity

Classified Protection of Information Security (MLPS)

等保 1.0

China Cybersecurity Law

网络安全法

Classified Protection of Cybersecurity (MLPS 2.0)

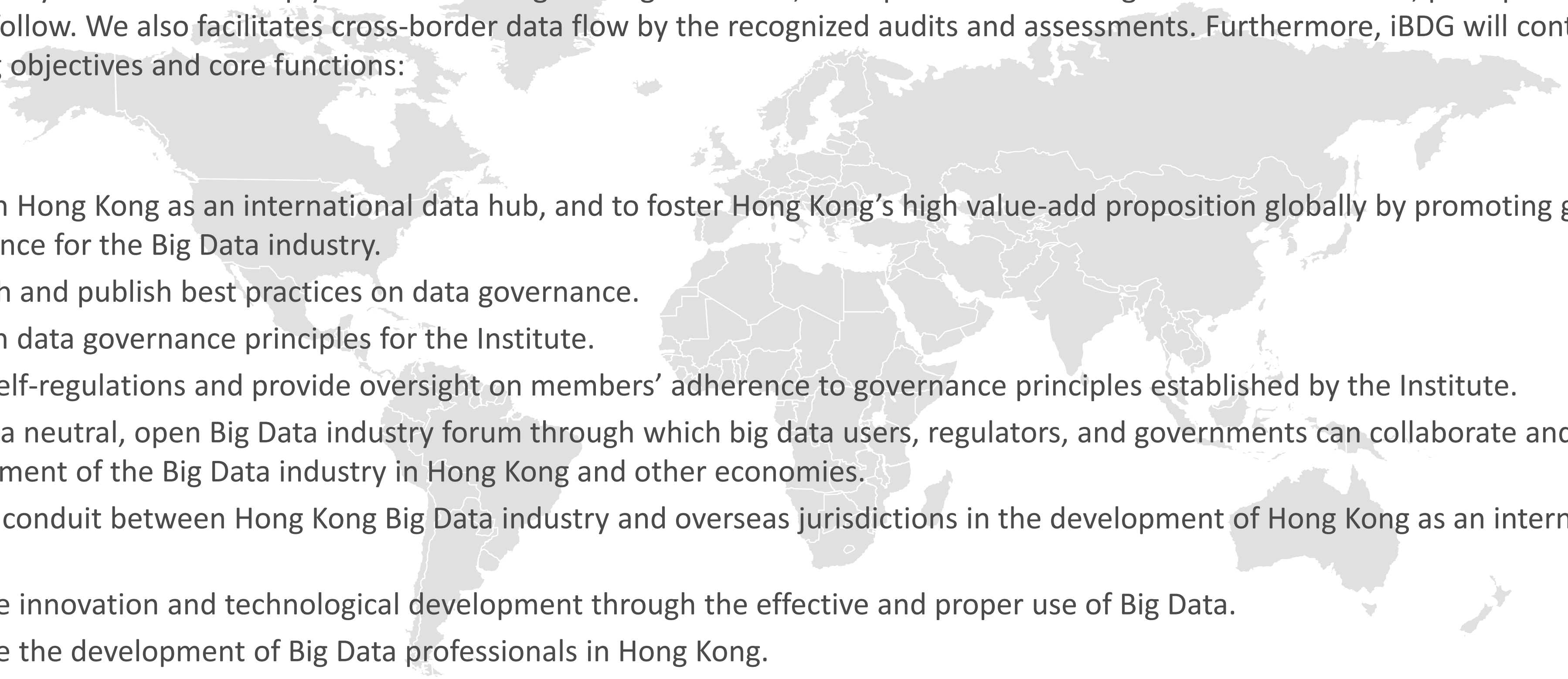
等保 2.0

iBDG’s Vision

Build Hong Kong as an international data hub and promote good self-governance for the Big Data industry

Institute of Big Data Governance (iBDG) aims to build Hong Kong as an international data hub and promote good self-governance for the Big Data industry.

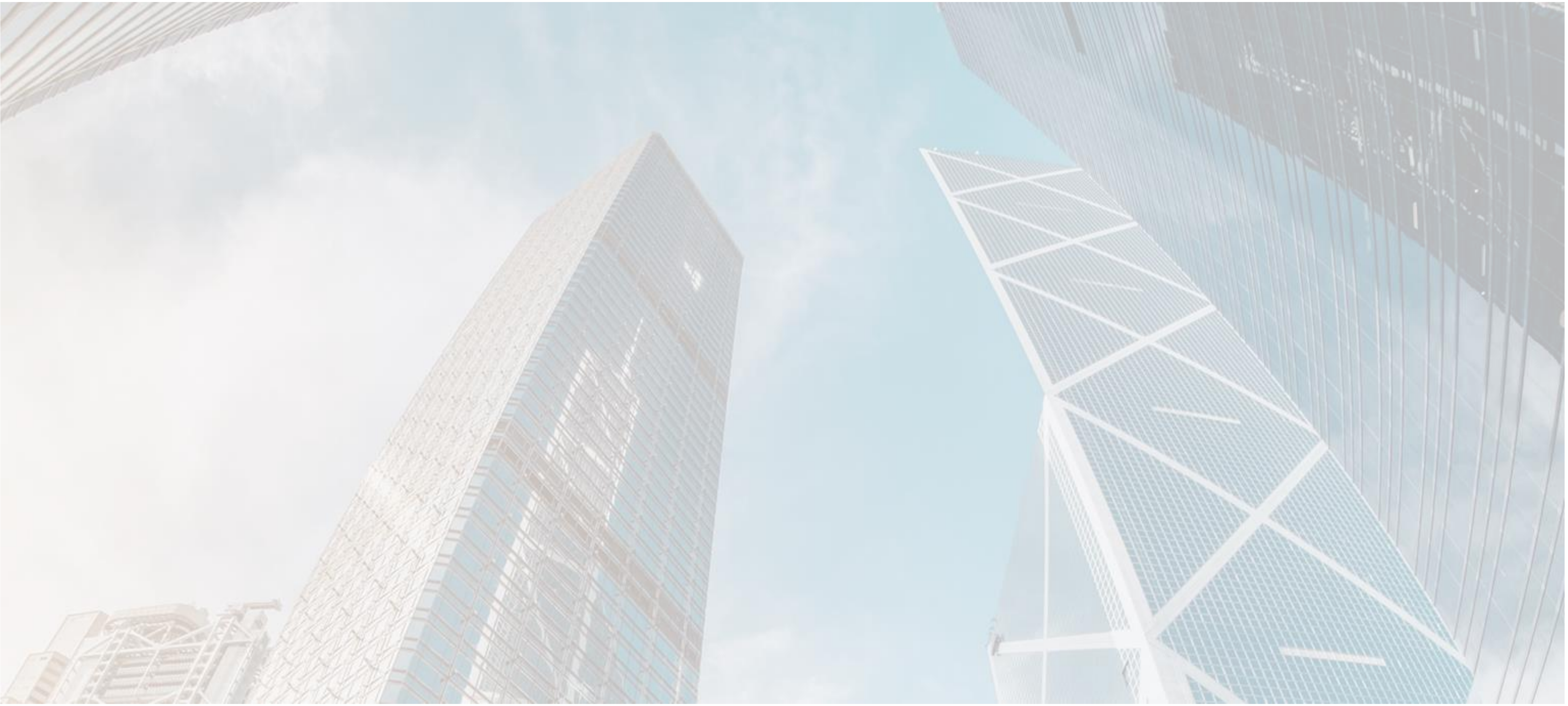
To allow industry members to comply with the self-regulated governance, iBDG provides the data governance standards, principles and best practices to follow. We also facilitates cross-border data flow by the recognized audits and assessments. Furthermore, iBDG will continue to commit the following objectives and core functions:



Objectives

- Establish Hong Kong as an international data hub, and to foster Hong Kong’s high value-add proposition globally by promoting good self-governance for the Big Data industry.
- Research and publish best practices on data governance.
- Establish data governance principles for the Institute.
- Foster self-regulations and provide oversight on members’ adherence to governance principles established by the Institute.
- Provide a neutral, open Big Data industry forum through which big data users, regulators, and governments can collaborate and promote the development of the Big Data industry in Hong Kong and other economies.
- Act as a conduit between Hong Kong Big Data industry and overseas jurisdictions in the development of Hong Kong as an international data hub.
- Facilitate innovation and technological development through the effective and proper use of Big Data.
- Facilitate the development of Big Data professionals in Hong Kong.

Part II :
Data Governance
– Why do we care?



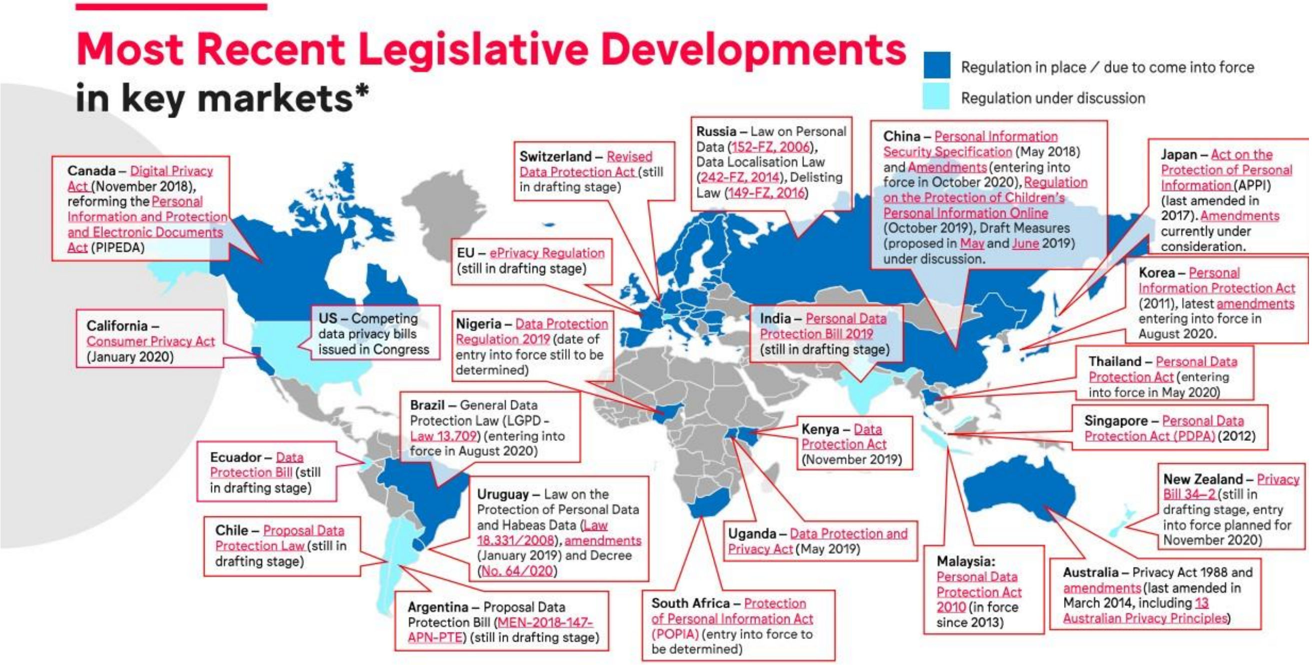
Regulations on Data Security and Personal Information Protection
- Regulations Around the World

“Data is the new oil .., and Analytics is the refinery”

“You never know how valuable your privacy is until you lose it ..”

There are many data protection and privacy laws around the world, and new ones coming all the time as well ..

Many countries have regulations that also restrict data flowing outside of their jurisdictions ..



Most Recent Legislative Developments in key markets*

■ Regulation in place / due to come into force

□ Regulation under discussion

Canada – Digital Privacy Act (November 2018), reforming the Personal Information and Protection and Electronic Documents Act (PIPEDA)

California – Consumer Privacy Act (January 2020)

US – Competing data privacy bills issued in Congress

Switzerland – Revised Data Protection Act (still in drafting stage)

EU – ePrivacy Regulation (still in drafting stage)

Nigeria – Data Protection Regulation 2019 (date of entry into force still to be determined)

Brazil – General Data Protection Law (LGPD - Law 13.709) (entering into force in August 2020)

Ecuador – Data Protection Bill (still in drafting stage)

Chile – Proposal Data Protection Law (still in drafting stage)

Uruguay – Law on the Protection of Personal Data and Habeas Data (Law 18.331/2008), amendments (January 2019) and Decree (No. 64/020)

Argentina – Proposal Data Protection Bill (MEN-2018-147-APN-PTE) (still in drafting stage)

South Africa – Protection of Personal Information Act (POPIA) (entry into force to be determined)

Uganda – Data Protection and Privacy Act (May 2019)

Kenya – Data Protection Act (November 2019)

Russia – Law on Personal Data (152-FZ, 2006), Data Localisation Law (242-FZ, 2014), Delisting Law (149-FZ, 2016)

India – Personal Data Protection Bill 2019 (still in drafting stage)

China – Personal Information Security Specification (May 2018) and Amendments (entering into force in October 2020), Regulation on the Protection of Children's Personal Information Online (October 2019), Draft Measures (proposed in May and June 2019) under discussion.

Japan – Act on the Protection of Personal Information (APPI) (last amended in 2017). Amendments currently under consideration.

Korea – Personal Information Protection Act (2011), latest amendments entering into force in August 2020.

Thailand – Personal Data Protection Act (entering into force in May 2020)

Singapore – Personal Data Protection Act (PDPA) (2012)

Malaysia: Personal Data Protection Act 2010 (in force since 2013)

Australia – Privacy Act 1988 and amendments (last amended in March 2014, including 13 Australian Privacy Principles)

New Zealand – Privacy Bill 34–2 (still in drafting stage, entry into force planned for November 2020)

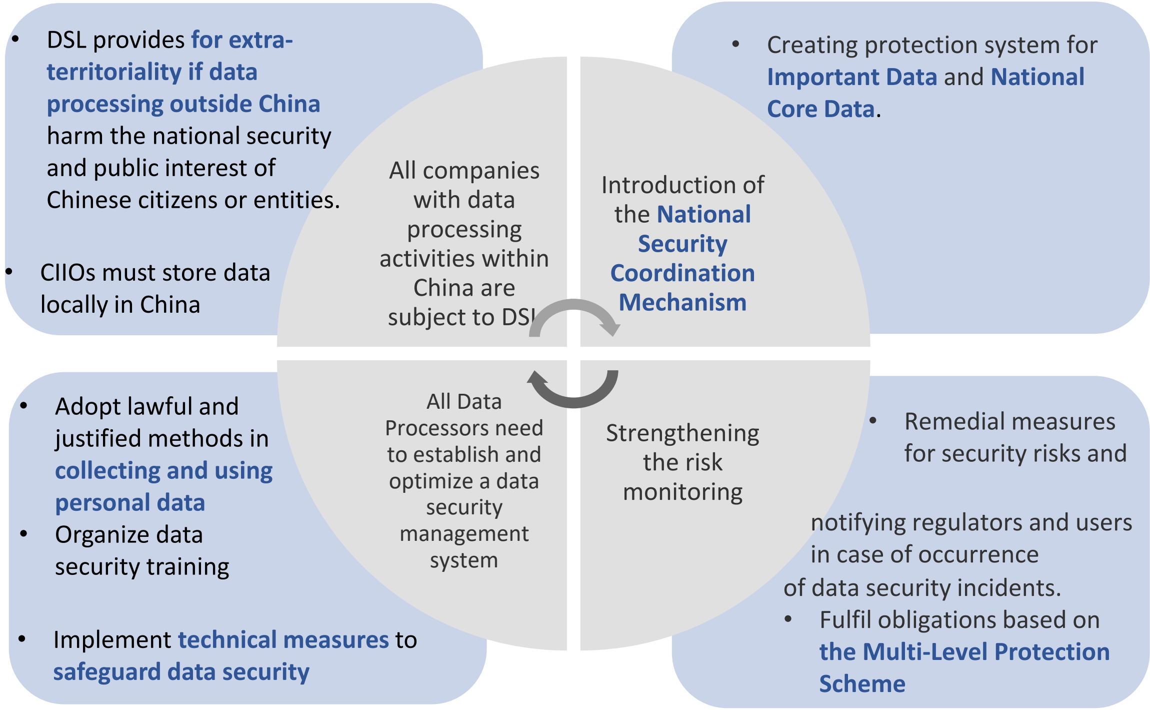
* Source: WFA Global Privacy Map 2020

Regulations on Data Security and Personal Information Protection - Mainland China

Key Requirements of the **Data Security Law (DSL)**

The Data Security Law is intended to regulate data security issues from **a national security perspective** with the following aspects worth being highlighted:

- Introduction of the National Data Security Coordination Mechanism
- Implementation of a Data categorization of classification regime
- Definition of Important Data and National Core Data
- Data Security review system
- Data subject to export control



- DSL provides **for extra-territoriality if data processing outside China** harm the national security and public interest of Chinese citizens or entities.
- CIIOs must store data locally in China

All companies with data processing activities within China are subject to DSL

- Creating protection system for **Important Data** and **National Core Data**.

Introduction of the **National Security Coordination Mechanism**

- Adopt lawful and justified methods in **collecting and using personal data**
- Organize data security training
- Implement **technical measures** to **safeguard data security**

All Data Processors need to establish and optimize a data security management system

Strengthening the risk monitoring

- Remedial measures for security risks and notifying regulators and users in case of occurrence of data security incidents.
- Fulfil obligations based on **the Multi-Level Protection Scheme**

Key Requirements of the **Personal Information Protection Law (PIPL)**

Applicability 01

- *Chinese domestic companies*
- *Foreign companies without business presence in china, but selling products and services to China market and collecting data and PI from China, or assessing and analysis behaviors of individuals in China*

Principles 02

- *Principles of openness and transparency*
- *Clear and reasonable purpose*
- *Directly related to the handling purpose*
- *Minimum influence on individual rights and interests*

Legitimacy of Data Processing 03

- *Add other circumstances in addition to "obtaining individuals' consent"*

Data Subject Rights 04

- *Rights to be informed*
- *Right to make decision*
- *Right to restrict or refuse processing of personal information*

Evidence 05

- *The personal information data processor shall assume liability **cannot prove that they are not at fault** where rights and interests on personal information are infringed due to any personal information processing activities*

Responsibility of Entrusted Parties 06

- *Agree with the entrusted party on the purposes, period, means, categories of personal information and protection measures of the entrusted processing, rights and obligations of both parties*

Impact Assessment 07

- *Required for sensitive personal data, use personal information for automated decision making, data transmission to other processors, etc.*
- *Impact on personal rights and interests as well as security risks*
- *3 years record retention*

Automated Decision 08

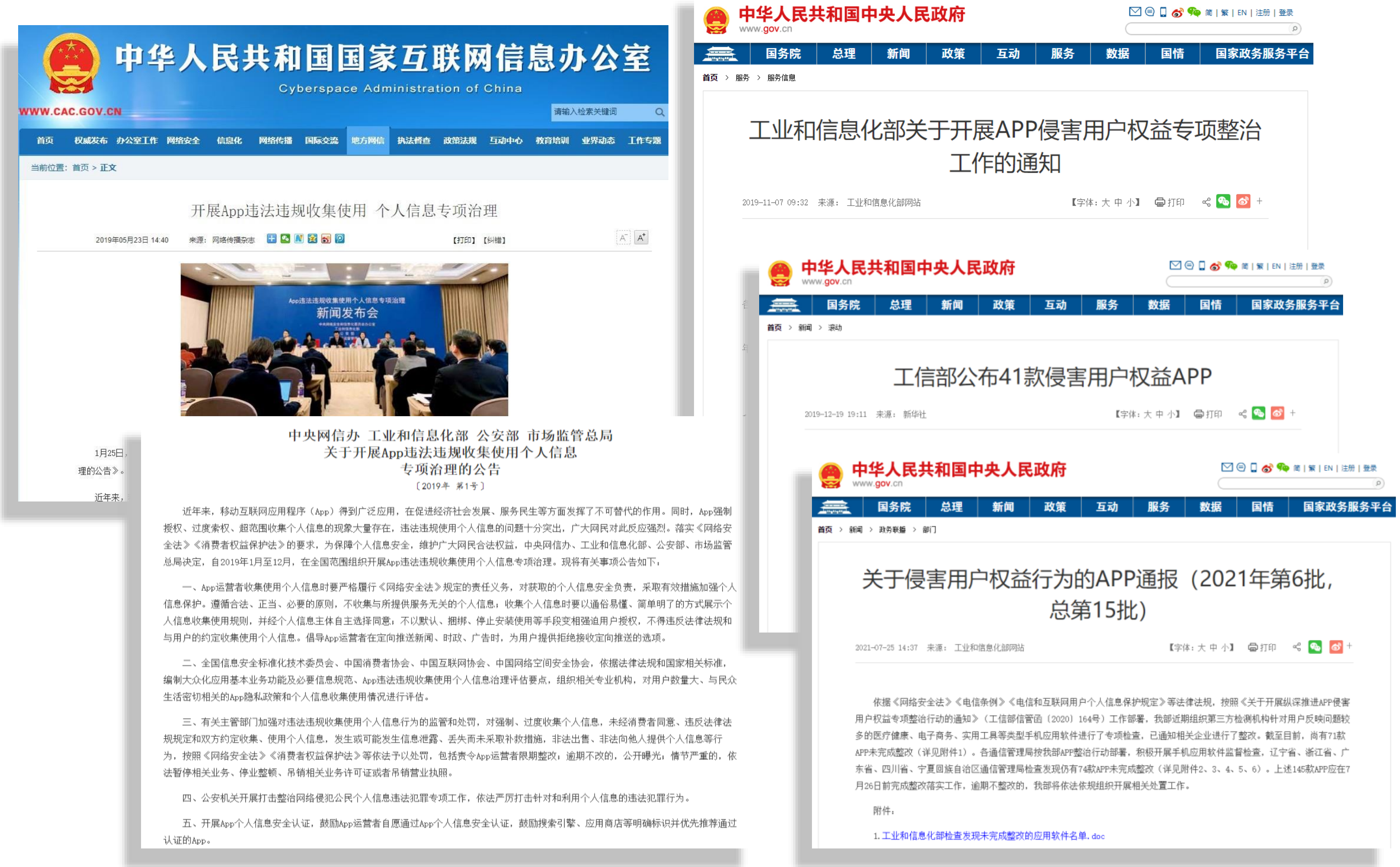
- *Collection of financial status, consumption habits, sensitivity to prices*
- *Data subject have right to request an explanation from the data processor or refuse decisions made by data processor soly based on the automated decision*

Cross-border Data Transfer 09

- *Government security assessment, or certification by professional institution or entering into extract prescribed by government with overseas recipient*

iBDG

Regulations on Data Security and Personal Information Protection – Mainland China (Enforcement Actions)



中华人民共和国国家互联网信息办公室

Cyberspace Administration of China

WWW.CAC.GOV.CN

请输入检索关键词

首页 权威发布 办公室工作 网络安全 信息化 网络传播 国际交流 地方网信 执法督查 政策法规 互动中心 教育培训 业界动态 工作专题

当前位置：首页 > 正文

开展App违法违规收集使用 个人信息专项治理

2019年05月23日 14:40 来源：网络传播杂志 【打印】【纠错】

1月25日，

理的公告》。

近年来，

中央网信办 工业和信息化部 公安部 市场监管总局
关于开展App违法违规收集使用个人信息
专项治理的公告
〔2019年 第1号〕

近年来，移动互联网应用程序（App）得到广泛应用，在促进经济社会发展、服务民生等方面发挥了不可替代的作用。同时，App强制授权、过度索权、超范围收集个人信息的现象大量存在，违法违规使用个人信息的问题十分突出，广大网民对此反应强烈。落实《网络安全法》《消费者权益保护法》的要求，为保障个人信息安全，维护广大网民合法权益，中央网信办、工业和信息化部、公安部、市场监管总局决定，自2019年1月至12月，在全国范围组织开展App违法违规收集使用个人信息专项治理。现将有关事项公告如下：

一、App运营者收集使用个人信息时要严格履行《网络安全法》规定的责任义务，对获取的个人信息安全负责，采取有效措施加强个人信息保护。遵循合法、正当、必要的原则，不收集与所提供服务无关的个人信息；收集个人信息时要以通俗易懂、简单明了的方式展示个人信息收集使用规则，并经个人信息主体自主选择同意；不以默认、捆绑、停止安装使用等手段变相强迫用户授权，不得违反法律法规和与用户的约定收集使用个人信息。倡导App运营者在定向推送新闻、时政、广告时，为用户提供拒绝接收定向推送的选项。

二、全国信息安全标准化技术委员会、中国消费者协会、中国互联网协会、中国网络空间安全协会，依据法律法规和国家相关标准，编制大众化应用基本业务功能及必要信息规范、App违法违规收集使用个人信息治理评估要点，组织相关专业机构，对用户数量大、与民众生活密切相关的App隐私政策和个人信息收集使用情况进行评估。

三、有关主管部门加强对违法违规收集使用个人信息行为的监管和处罚，对强制、过度收集个人信息，未经消费者同意、违反法律法规规定和双方约定收集、使用个人信息，发生或可能发生信息泄露、丢失而未采取补救措施，非法出售、非法向他人提供个人信息等行为，按照《网络安全法》《消费者权益保护法》等依法予以处罚，包括责令App运营者限期整改；逾期不改的，公开曝光；情节严重的，依法暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照。

四、公安机关开展打击整治网络侵犯公民个人信息违法犯罪专项工作，依法严厉打击针对和利用个人信息的违法犯罪行为。

五、开展App个人信息安全认证，鼓励App运营者自愿通过App个人信息安全认证，鼓励搜索引擎、应用商店等明确标识并优先推荐通过认证的App。

中华人民共和国中央人民政府
www.gov.cn

简 | 繁 | EN | 注册 | 登录

国务院 总理 新闻 政策 互动 服务 数据 国情 国家政务服务平台

首页 > 服务 > 服务信息

工业和信息化部关于开展APP侵害用户权益专项整治工作的通知

2019-11-07 09:32 来源：工业和信息化部网站 【字体：大 中 小】 打印

中华人民共和国中央人民政府
www.gov.cn

简 | 繁 | EN | 注册 | 登录

国务院 总理 新闻 政策 互动 服务 数据 国情 国家政务服务平台

首页 > 新闻 > 滚动

工信部公布41款侵害用户权益APP

2019-12-19 19:11 来源：新华社 【字体：大 中 小】 打印

中华人民共和国中央人民政府
www.gov.cn

简 | 繁 | EN | 注册 | 登录

国务院 总理 新闻 政策 互动 服务 数据 国情 国家政务服务平台

首页 > 新闻 > 政务联播 > 部门

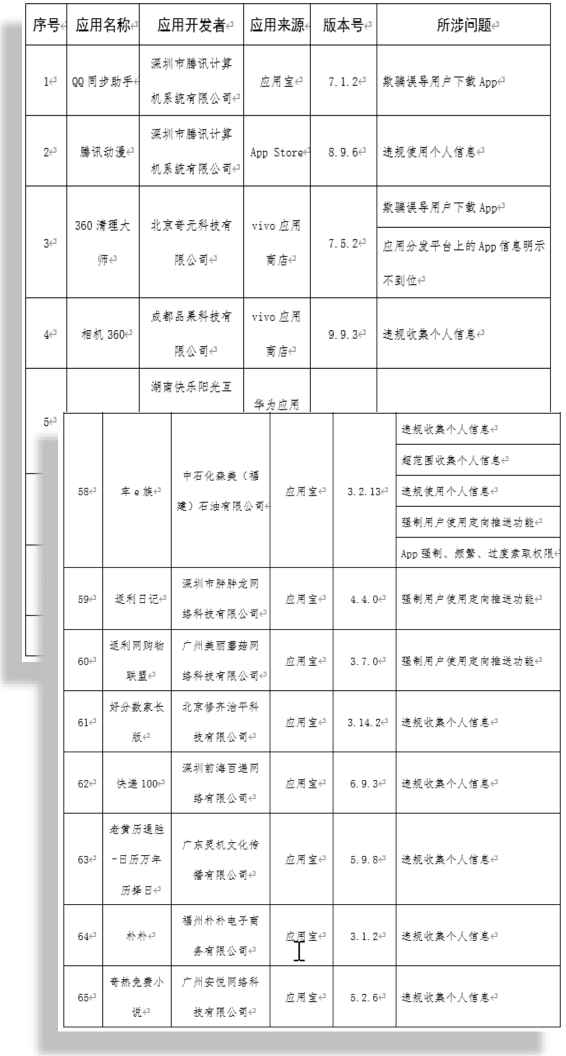
关于侵害用户权益行为的APP通报（2021年第6批，总第15批）

2021-07-25 14:37 来源：工业和信息化部网站 【字体：大 中 小】 打印

依据《网络安全法》《电信条例》《电信和互联网用户个人信息保护规定》等法律法规，按照《关于开展纵深推进APP侵害用户权益专项整治行动的通知》（工信部信管函〔2020〕164号）工作部署，我部近期组织第三方检测机构针对用户反映问题较多的医疗健康、电子商务、实用工具等类型手机应用软件进行了专项检查，已通知相关企业进行了整改。截至目前，尚有71款APP未完成整改（详见附件1）。各通信管理局按我部APP整治行动部署，积极开展手机应用软件监督检查，辽宁省、浙江省、广东省、四川省、宁夏回族自治区通信管理局检查发现仍有74款APP未完成整改（详见附件2、3、4、5、6）。上述145款APP应在7月26日前完成整改落实工作，逾期不整改的，我部将依法依规组织开展相关处置工作。

附件：

1. 工业和信息化部检查发现未完成整改的应用软件名单. doc



序号	应用名称	应用开发者	应用来源	版本号	所涉问题
1	QQ 同步助手	深圳市腾讯计算机系统有限公司	应用宝	7.1.2	欺骗误导用户下载 App
2	腾讯动漫	深圳市腾讯计算机系统有限公司	App Store	8.9.6	违规使用个人信息
3	360 清理大师	北京奇元科技有限公司	vivo 应用商店	7.5.2	欺骗误导用户下载 App 应用分发平台上的 App 信息明示不到位
4	相机 360	成都品果科技有限公司	vivo 应用商店	9.9.3	违规收集个人信息
5		湖南快乐阳光互	华为应用		

58	车 e 族	中石化森美（福建）石油有限公司	应用宝	3.2.13	违规收集个人信息 超范围收集个人信息 违规使用个人信息 强制用户使用定向推送功能 App 强制、频繁、过度索取权限
59	返利日记	深圳市胖胖龙网络科技有限公司	应用宝	4.4.0	强制用户使用定向推送功能
60	返利网购物联盟	广州美丽蘑菇网络科技有限公司	应用宝	3.7.0	强制用户使用定向推送功能
61	好分数家长版	北京修齐治平科技有限公司	应用宝	3.14.2	违规收集个人信息
62	快递 100	深圳前海百递网络有限公司	应用宝	6.9.3	违规收集个人信息
63	老黄历通胜-日历万年历择日	广东灵机文化传播有限公司	应用宝	5.9.8	违规收集个人信息
64	朴朴	福州朴朴电子商务有限公司	应用宝	3.1.2	违规收集个人信息
65	奇热免费小说	广州安悦网络科技有限公司	应用宝	5.2.6	违规收集个人信息

Regulations on Data Security and Personal Information Protection – In Mainland China (Enforcement Actions)

Inquiries about data security and privacy compliance during A-share IPO in recent years

Since 2019, several companies have been inquired about cyber security and data compliance issues during their IPOs

Time	Company	Inquires from Issuance Examination Committee of China Securities Regulatory Commission (CSRC)	Industry
2019.10	宜搜天下	Whether there is any **unauthorized acquisition of user data**, whether the acquisition of personal data has an explicit prompt to the user, whether the collected data is limited to the necessary scope, whether it is only a general prompt to collect user information, whether use data **beyond the scope of user authorization, or directly collect data without the authorization of other platforms**.	Internet and related services
2020.07	D+ 中数智汇	The specific method of the **issuer's publicly obtained data from the Internet**, the technology used, whether the content is legal and compliant, whether the procedure is proper; whether there is a special Internet method (or technology) to collect social information that is not publicly available or requires special permission, The information subject agrees and other pre-procedures to obtain data.	Software and IT services
2020.07	蚂蚁集团 ANT GROUP ANT GROUP CO., LTD. 螞蟻科技集團股份有限公司	Whether the **data sharing** between the issuer and Alibaba Group complies with the agreement between the issuer and the customer, and whether there is any infringement of the customer's legitimate interests; combined with the **data sharing agreement** between the issuer and Alibaba and other related entities, explain whether the arrangement violates the relevant laws and regulations related to information protection.	Internet and related services
2021.03	intellifusion 云天励飞	The issuer's product development and production involved in the acquisition and use of data, thus whether the permission of the collector is obtained, whether there is any violation of personal privacy or other legal rights, etc., whether **the acquisition, management and use of data** are legal and compliant, whether there are disputes or potential disputes, and whether the relevant risks are fully disclosed.	Software and IT services
2021.04	MEGVII 旷视	(1) The issuer's technology, business, and products (or services) involve specific links in **data collection, cleaning, management, and application**; the specific **types of data** involved in different **links, text, images, and videos**, etc.; (2) Whether the issuer's own core technology involves the application of a large amount of data, if so, the **source of the relevant data** and its compliance; (3) Whether the issuer provides products (or services) externally involving **the collection and use of data**, if yes, explain the **source of the data** and its legal compliance; (4) The issuer guarantees compliance measures in all aspects of data collection, cleaning, management, and use	Software and IT services
2021.06	云从科技 CLOUDWALK	Explain the company's measures and plans to ensure that the **artificial intelligence technology** is controllable and in line with ethical standards, as well as the **protection measures for customer privacy.**	Software and IT services

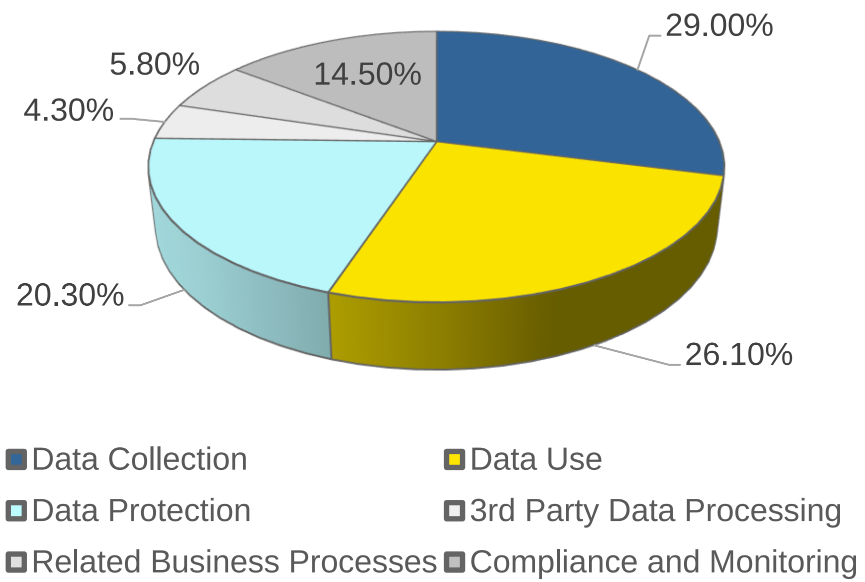
** Source: Shanghai Securities Exchange and Shenzhen Securities Exchange websites*

Regulations on Data Security and Personal Information Protection – In Mainland China (Enforcement Actions)

Inquiries about data security and privacy compliance during A-share IPO in recent years

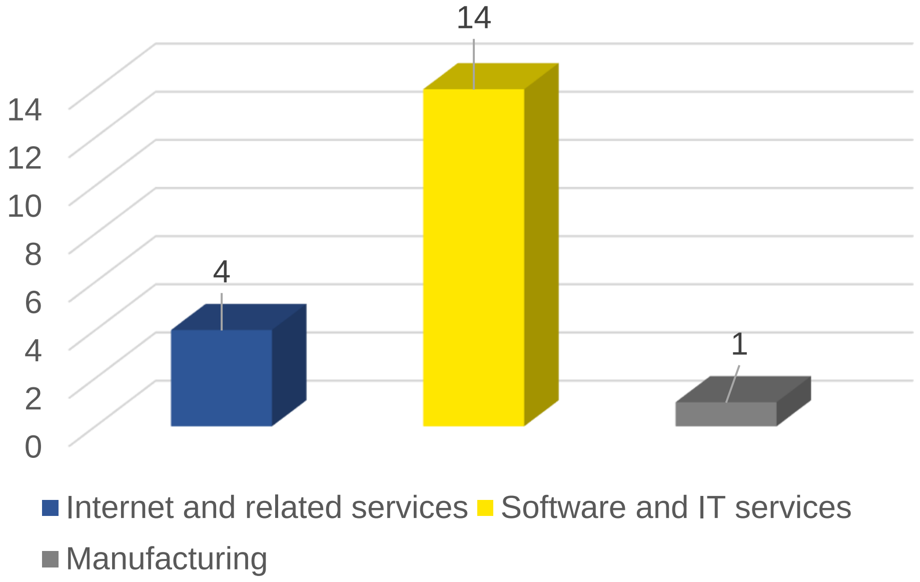
Since 2019, several companies have been inquired about cyber security and data compliance issues during their IPOs

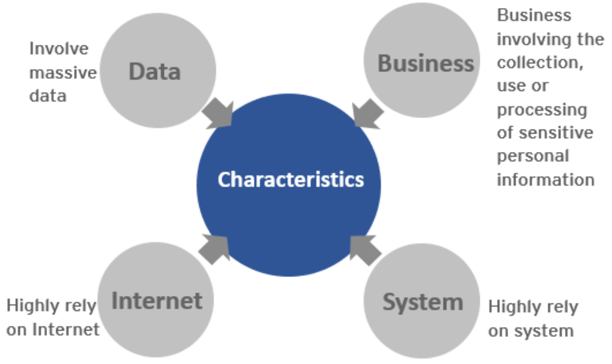
Types of Inquiries from Issuance Examination Committee



Types of IPO companies that received data security and privacy related inquiries from 2019 to 2021

(including the Science and Technology Innovation Board)



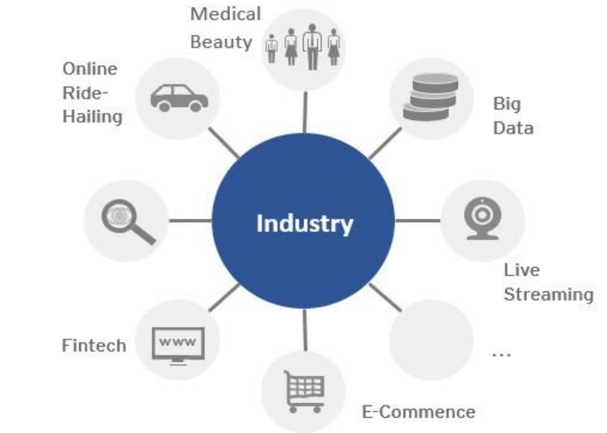

Characteristics

Data
Involve massive data

Business
Business involving the collection, use or processing of sensitive personal information

Internet
Highly rely on Internet

System
Highly rely on system


Industry

Medical Beauty

Online Ride-Hailing

Big Data

Live Streaming

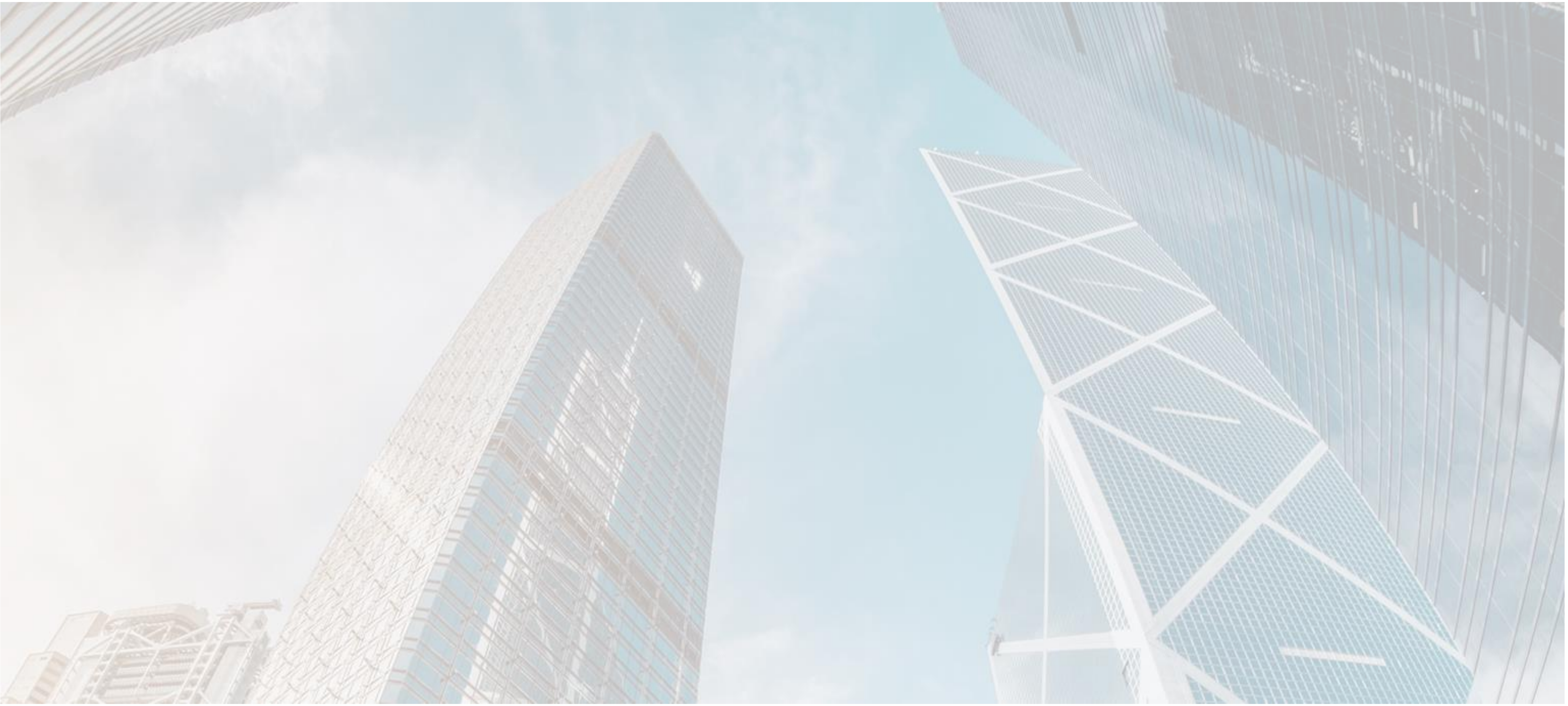
Fintech

E-Commence

...

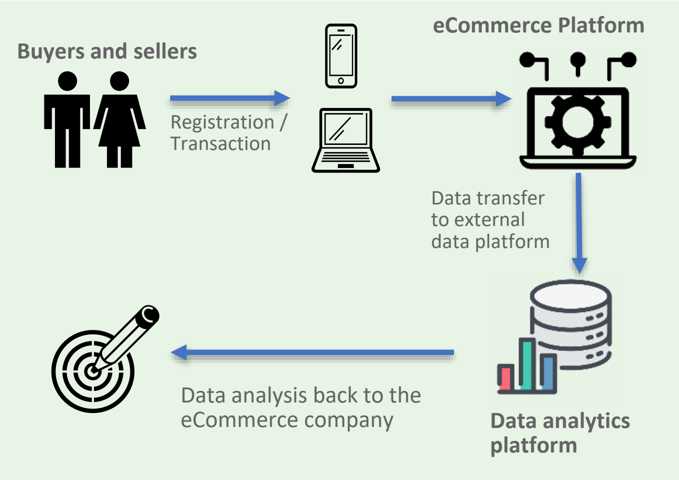
* *Source: Shanghai Securities Exchange and Shenzhen Securities Exchange websites*

Part III – A:
Data Governance Best Practice & Independent Verifications – Who Needs to do What?



Some Example Scenarios Where You May Come Across Data
- Scenario 1: Different Roles in Data Processing Activities

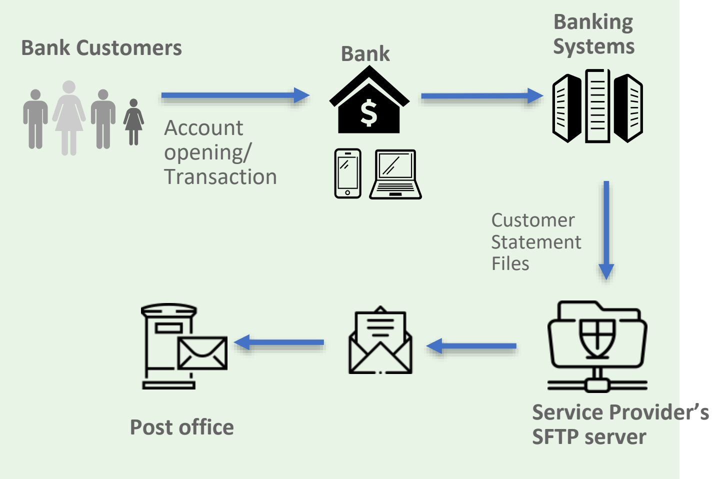
eCommerce



Buyers and sellers
Registration / Transaction
eCommerce Platform
Data transfer to external data platform
Data analytics platform
Data analysis back to the eCommerce company

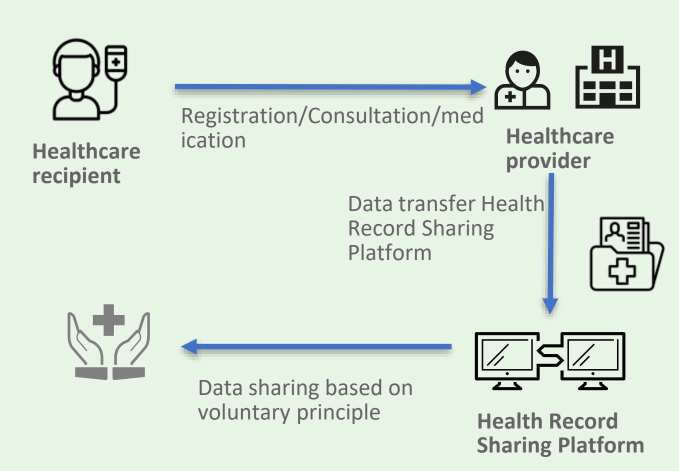
An eCommerce company uses an external data platform for improving search experience, identifying and optimizing relevant advertisements, and performing click stream analysis to understand how the eCommerce company's customers (both buyers and sellers) leverage their marketplace.

Banking



A bank outsources the printing and lettershopping process to a third-party service provider. Encrypted monthly customer statements are transferred to the service provider's SFTP server. After printing and lettershopping, the service provider would deliver the letters to post office for mailing.

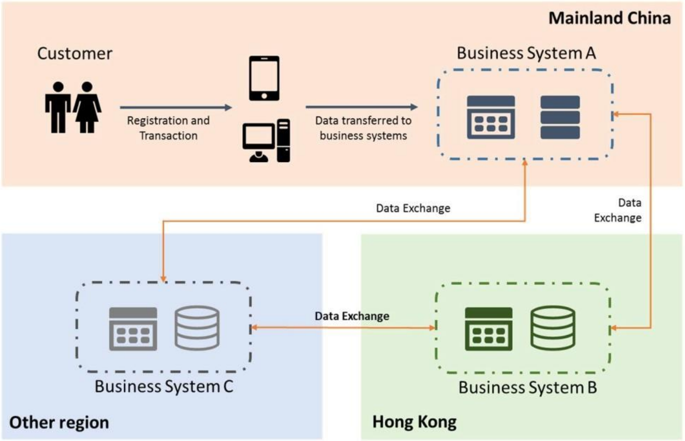
Healthcare



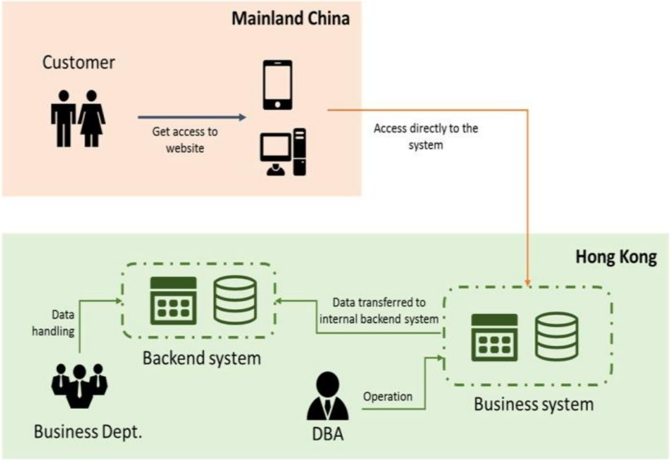
Healthcare recipient
Registration/Consultation/medication
Healthcare provider
Data transfer Health Record Sharing Platform
Health Record Sharing Platform
Data sharing based on voluntary principle

A medical record sharing platform collects healthcare recipient's health records and shares with authorized healthcare providing organisations, improve efficiency and quality of care, improve continuity and integration of care.

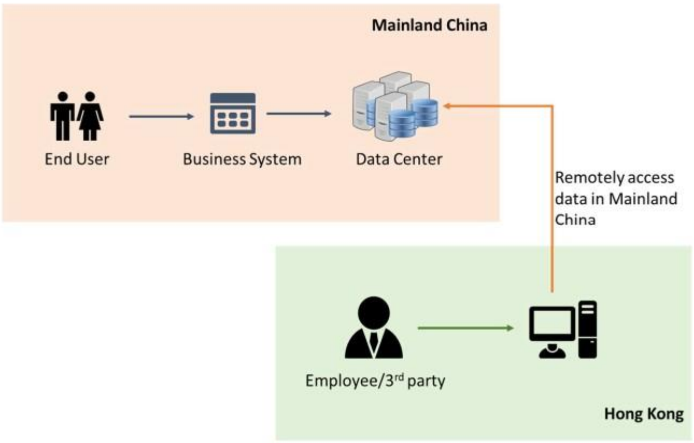
Some Example Scenarios Where You May Come Across Data
- Scenario 2: Data Cross-border Transfer



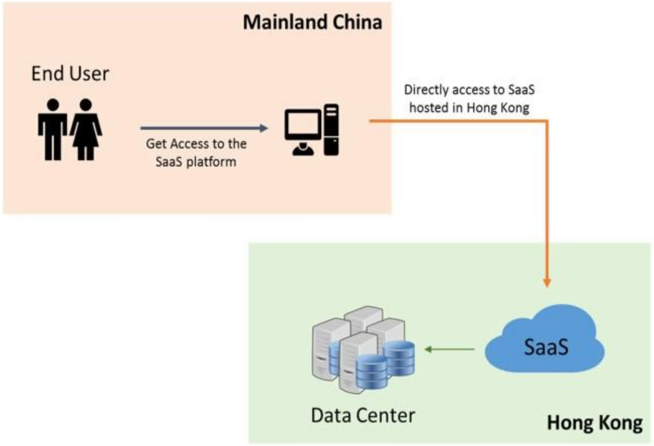
A multinational company collects customer personal information and transaction information in mainland China and stores them in its local business system. Those data collected are transmitted to the business system in Hong Kong on a daily basis and that business system is used to manage transaction data across all Asia-Pacific locations.



A multinational company has set up a data center in Hong Kong and built its application servers and databases hosted in that data center, which means that the data generated in mainland China will be directly stored in its foreign data center.



A multinational company has set up a data center in mainland China, which provides infrastructure for most of its business systems, while the operation and maintenance team of that company is based in Hong Kong. The staff in Hong Kong carry out their work through remote access to servers and databases of the data center located in mainland China for management and maintenance purpose.

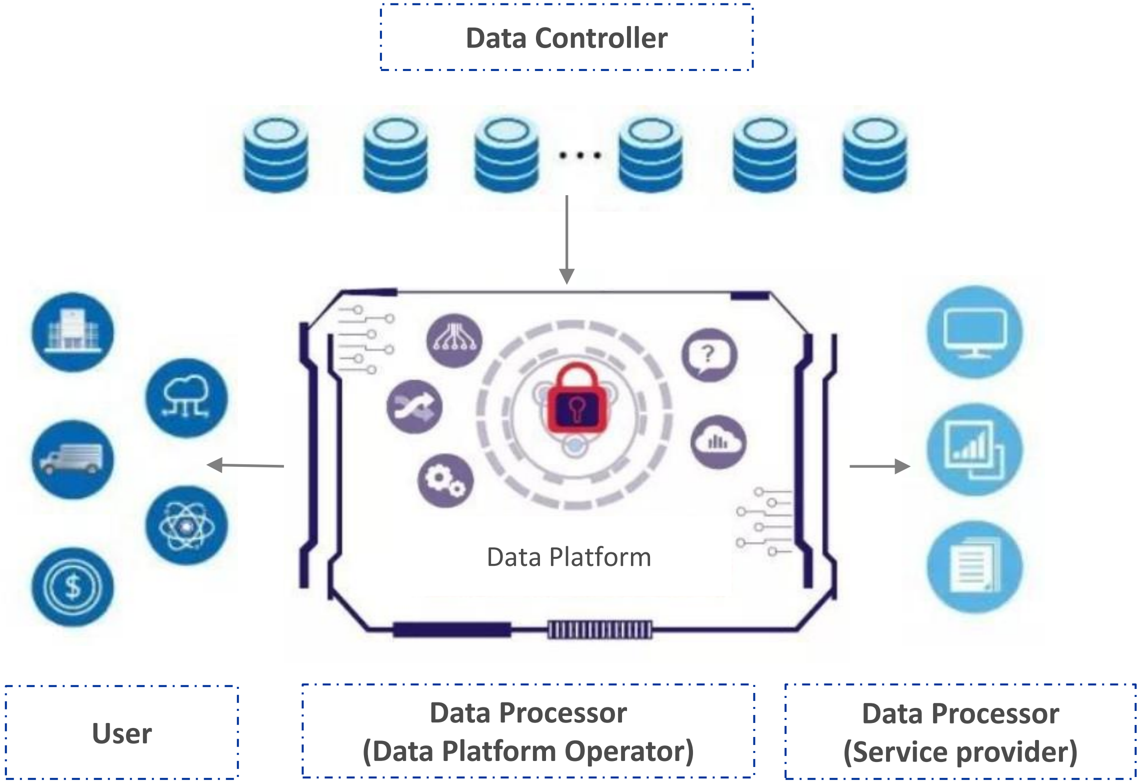

Mainland China
End User
Get Access to the SaaS platform
Directly access to SaaS hosted in Hong Kong
SaaS
Data Center
Hong Kong

For cloud service providers that do not have data centers established in mainland China, companies may subscribe their cloud services which are operating in the data centers located in Hong Kong (or other locations) if those companies want to carry out business activities in mainland China by subscribing to cloud services.

** Source: Hong Kong Smart City Consortium – Building Hong Kong as an International Data Hub*

Some Example Scenarios Where You May Come Across Data - the Different Roles

Scenario 1



Data Controller

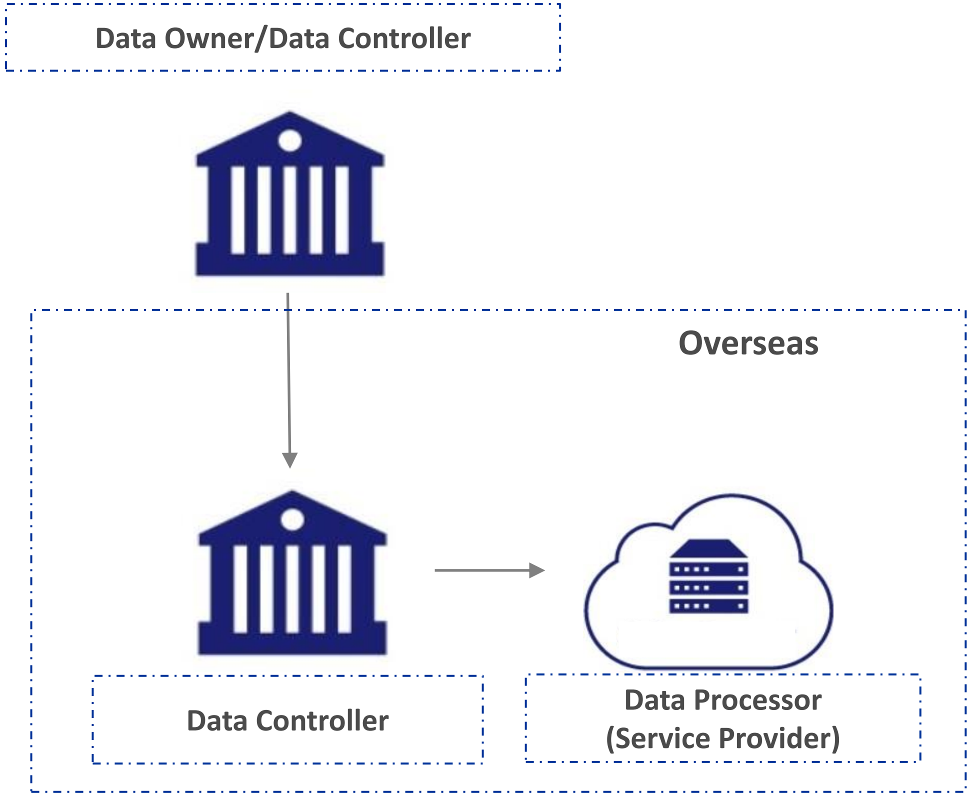
Data Platform

User

Data Processor
(Data Platform Operator)

Data Processor
(Service provider)

Scenario 2



Data Owner/Data Controller

Overseas

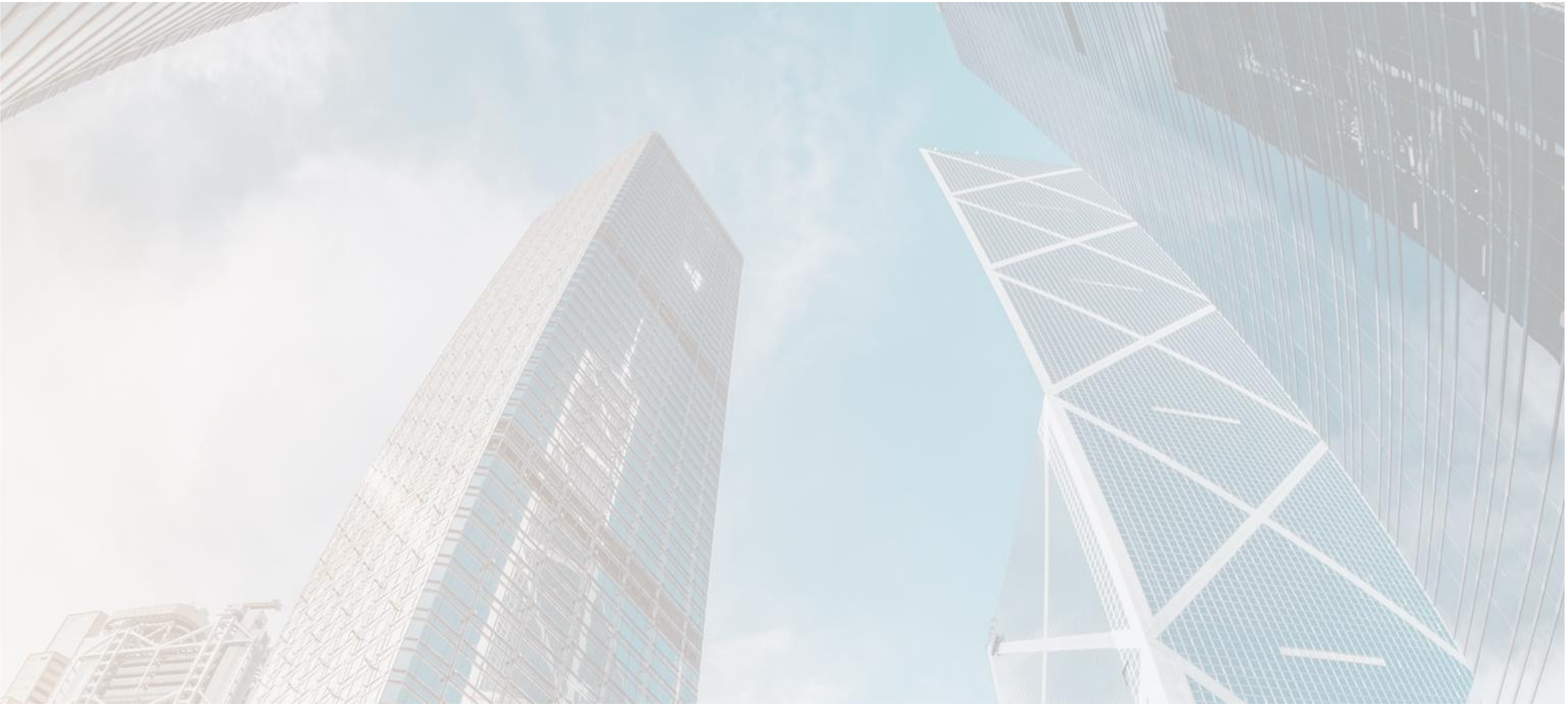
Data Controller

Data Processor
(Service Provider)

Whichever role you play, whether you may be the Data Controller or Data Processor, or Service Provider to the Data Controller or Processor), you are responsible for protecting data, and often need to prove it through independent verifications.

Part III – B:

Introducing iBDG’s Big Data Governance Certification Programme



iBDG Big Data Governance Assessment Criteria 2.0
- Underlying China National and International Standards

The *iBDG Big Data Governance Assessment Criteria 2.0* (“iBDG Assessment Criteria” or “Assessment Criteria”) are formulated in the 14 control domains, which are mapped to the following national and international standards. These references provide an overview on which standards *iBDG Assessment Criteria* are based, and which are not. In addition, users who already hold respective certifications or aligned their organization and processes along one or several of these standards can document the implementation of *iBDG Assessment Criteria* largely through referencing their individual safeguards to the requirements of *iBDG Assessment Criteria*.

National standards

- Information security techniques — Data Security Capability Maturity Model (信息安全技术-数据安全能力成熟度模型) (DSMM)
- Information Security Technology- Baseline for Cybersecurity Classified Protection (Part1： Security General Requirements) - Level 3 (信息安全技术-信息系统安全等级保护测评要求 – 通用三级)
- Information Security Technology- Guidelines for Data Cross-Border Transfer Security Assessment (信息安全技术-数据出境安全指南 （征求意见稿） 2017.08.25)
- Information Security Technology- Guidelines for Personal information Cross-Border Transfer Security Assessment (个人信息出境安全评估办法（征求意见稿）2019.06.13)

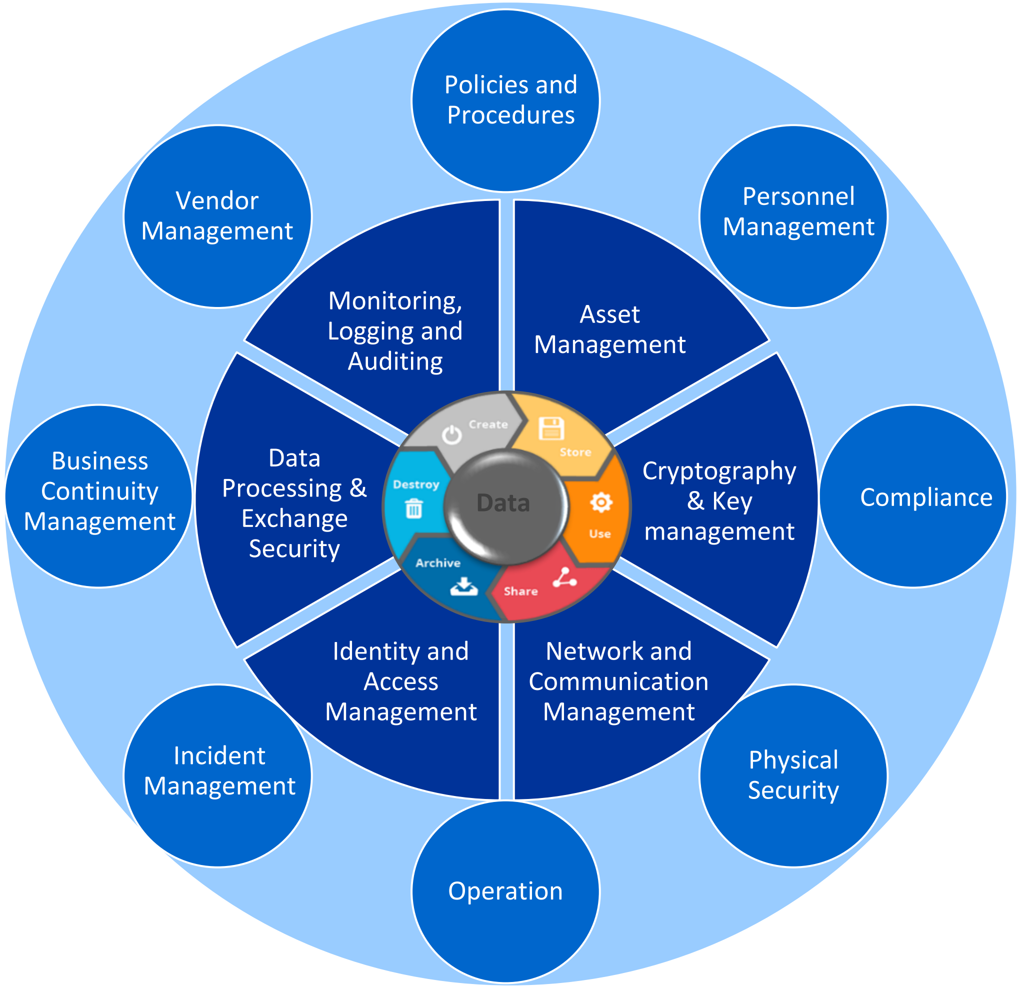
International standards

- ISO/IEC 270001:2013
- CSA-Cloud Controls Matrix 3.0.1 (CCM)
- BSI- Cloud Computing Compliance Controls Catalogue (C5)
- AICPA - Trust Services Principles (TSP) Criteria 2017

iBDG Big Data Governance Certification Programme
- Control Objectives

Protection on data should be implemented throughout the data life cycle.

- **Data Protection Domains** - six control domains (i.e. asset management, cryptograph and key managements, network and communication management, identity and access management, data processing and exchange security, monitoring, logging and audit) include the control measures and safeguards when the data were created, stored, used, shared, archived or destroyed, without which the data security, confidentiality, integrity and privacy may not be ensured.
- **Control Environment Domains** - eight general control domains (i.e. policies and procedures, personnel management, compliance, incident management, vendor management, business continuity management, operation and physical security) set out the general control objectives to support the protection on data by providing a sound control environment to support the proposed control measures and safeguards in the aforementioned six domains.



Policies and Procedures
Vendor Management
Personnel Management
Monitoring, Logging and Auditing
Asset Management
Business Continuity Management
Data Processing & Exchange Security
Create
Store
Destroy
Data
Use
Archive
Share
Cryptography & Key management
Compliance
Identity and Access Management
Network and Communication Management
Incident Management
Physical Security
Operation

iBDG Big Data Governance Certification Programme
- Control Objectives

The baseline of iBDG Assessment Scheme covers 14 control domains which are set out in the table below with the corresponding objectives.

► **Data Protection Domain (6)**

No.	Control Domains	Objectives
A	Asset Management	To identify the assets (including the data that the organization owns/controls/processes and storing/processing facilities) and responsible persons as well as define an appropriate level of protection.
B	Cryptography and Key management	To safeguard data security through adopting appropriate and effective cryptography.
C	Identity and Access Management	To prevent unauthorized access to data through authentication and access authorization.
D	Network and Communication Management	To protect data transmitting in networks and the corresponding information processing systems.
E	Data Processing and Exchange Security	To ensure data security, confidentiality and integrity during data processing, data import and export, data interfacing across multiple systems and data sharing with the authorized parties.
F	Monitoring, Logging and Auditing	To detect and prevent unauthorized access, abuse and leakage of data throughout the data life cycle.

iBDG Big Data Governance Certification Programme
- Control Objectives

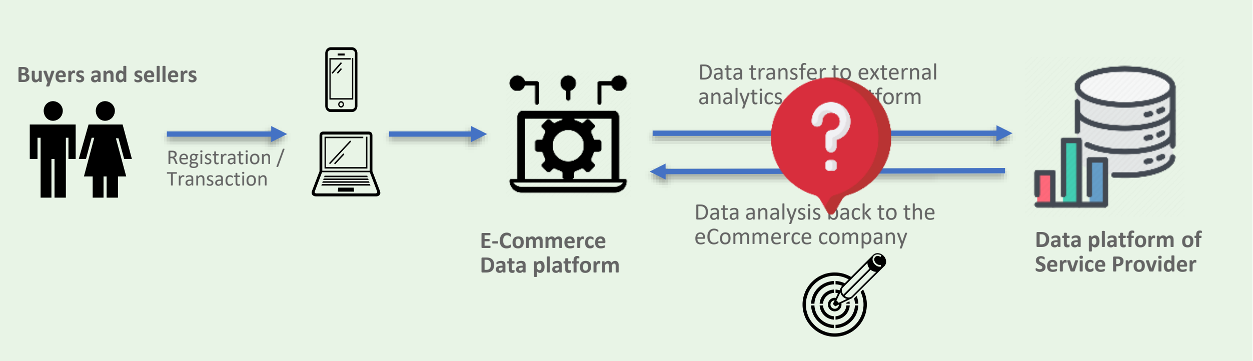
The baseline of iBDG Assessment Scheme covers 14 control domains which are set out in the table below with the corresponding objectives.

- **Control Environment Domain (8)**

No.	Control Domains	Objectives
G	Policies and Procedures	To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
H	Personnel Management	To ensure that employees, service providers and suppliers are aware of their roles and responsibilities regarding information security and in compliance with data security requirements from onboarding till offboarding.
I	Compliance	To ensure compliance with laws, statutory, regulatory or contractual obligations and data security, confidentiality and privacy requirements.
J	Incident Management	To ensure data security incidents associated with information systems are communicated and addressed in a timely manner.
K	Vendor Management	To protect information that can be accessed by vendors and monitor the agreed upon services and security requirements.
L	Business Continuity Management	To ensure and maintain continuous business operations through planning, implementing and testing business continuity practice as well as incorporating safeguards.
M	Operation	To ensure continuous and uninterrupted operations by implementing appropriate safeguards such as regular data backup and restoration, capacity planning and monitoring, change management as well as handling vulnerabilities, malfunctions and errors.
N	Physical Security	To prevent unauthorized physical access and protect against environmental threats.

iBDG Big Data Governance Certification Programme
- Illustration: Application of the Control Objectives

Illustration - eCommerce


Buyers and sellers
Registration / Transaction
E-Commerce Data platform
Data transfer to external analytics platform
Data analysis back to the eCommerce company
Data platform of Service Provider

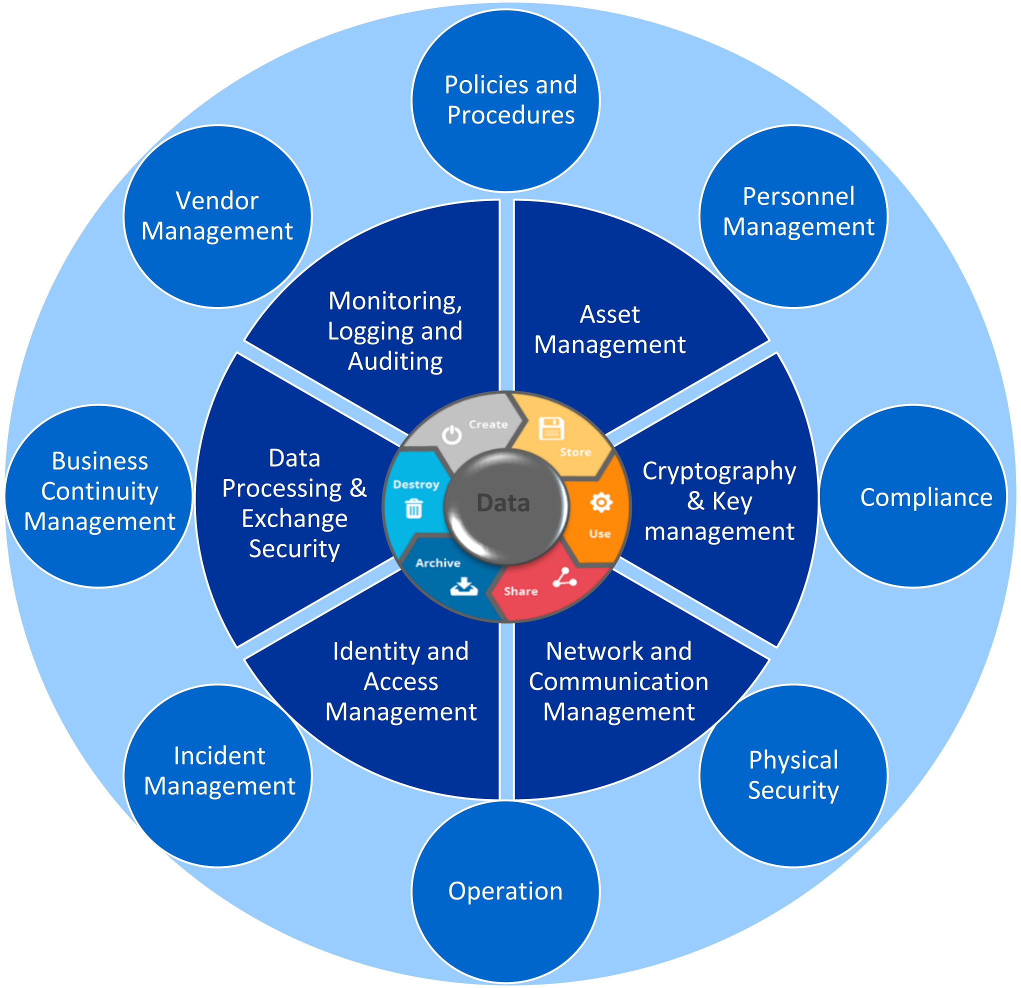
A1. The Company regularly maintains and updates the complete information asset list, which includes not only the data owned by the Company, but also the data controlled and processed by the Company after obtained the data from the data provider.

A2. The Company classifies assets based on legal restrictions, contract restrictions, data type, value, geographic location, sensitivity to unauthorized disclosure/modification, and importance to the Company, and label the data it received.

A3. The Company develops an appropriate set of procedures for handling in accordance with the asset classification mechanism adopted by the organization.

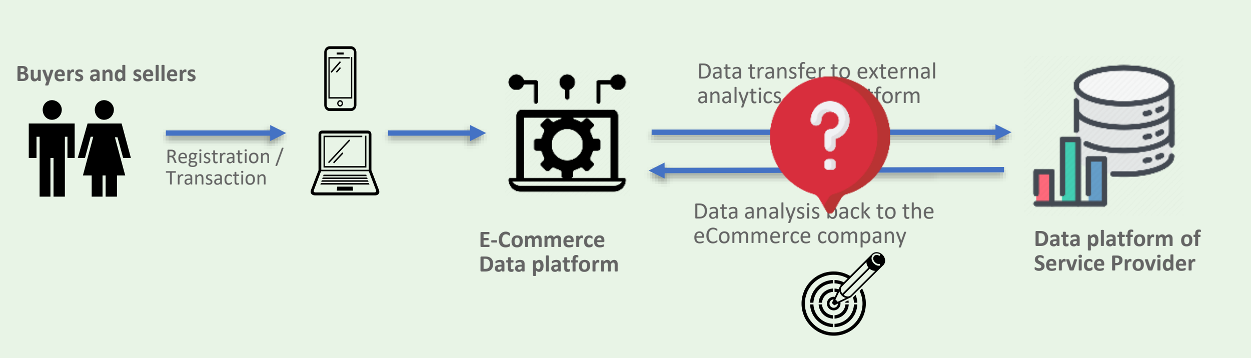
E7. Contractual terms are set out between the Company and data provider regarding data use purpose, data delivery method, retention period, disposal methods, confidentiality/non-disclosure and security responsibility and obligations during data supply chain management

D2. The data traffic in jointly used network environments is segregated to ensure the confidentiality and integrity of the data transmitted.


Policies and Procedures
Vendor Management
Personnel Management
Monitoring, Logging and Auditing
Asset Management
Business Continuity Management
Data Processing & Exchange Security
Data
Create
Store
Use
Share
Archive
Destroy
Cryptography & Key management
Compliance
Identity and Access Management
Network and Communication Management
Incident Management
Physical Security
Operation

iBDG Big Data Governance Certification Programme
- Illustration: Application of the Control Objectives

Illustration - eCommerce


Buyers and sellers
Registration / Transaction
E-Commerce Data platform
Data transfer to external analytics platform
Data analysis back to the eCommerce company
Data platform of Service Provider

B3. The Company implements technical measures regarding the use of encryption for protection of sensitive data in transmission (e.g., system interfaces, over public networks, and electronic messaging)

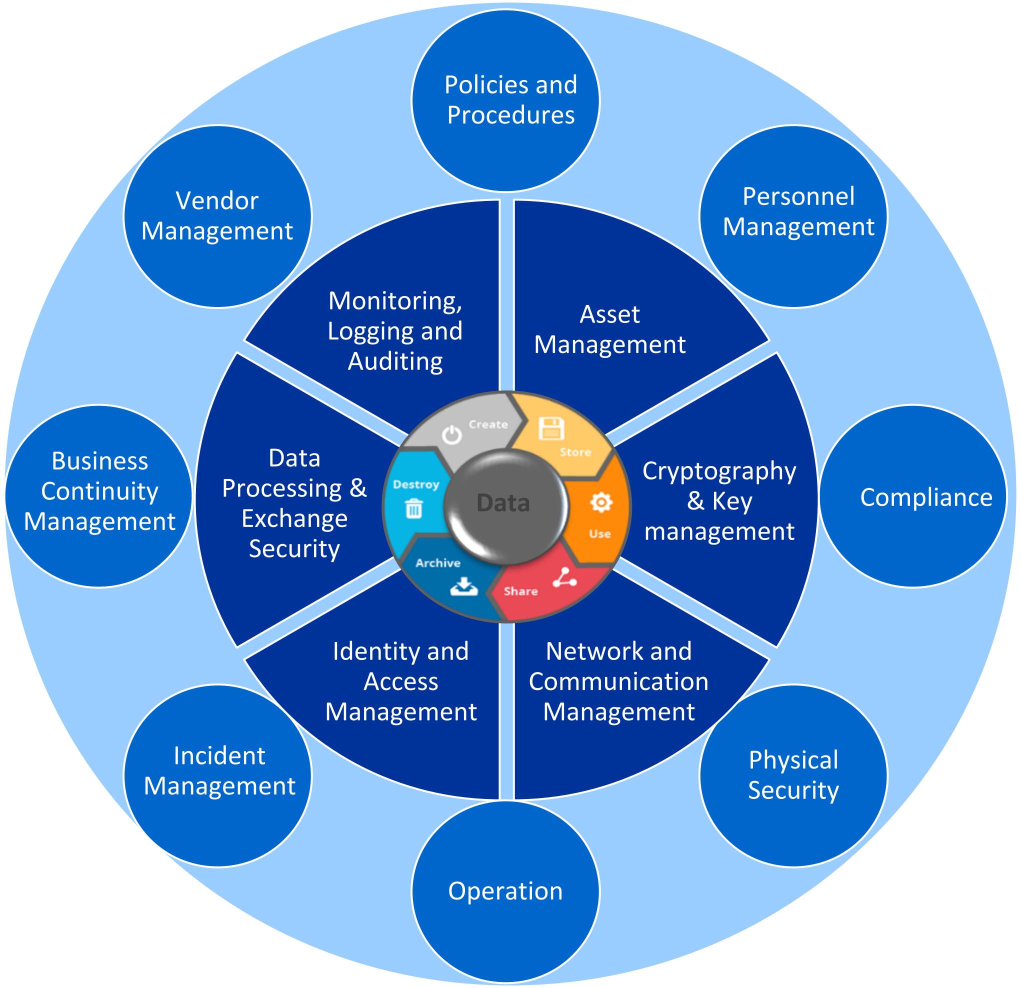
B4. The Company implements technical measures regarding the use of encryption for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations) and data in use (memory)

C1. Authentication and access maintenance procedures are established.

E1. The Company establishes policies and procedure and implements technical measures to support the data desensitization requirements when applicable.

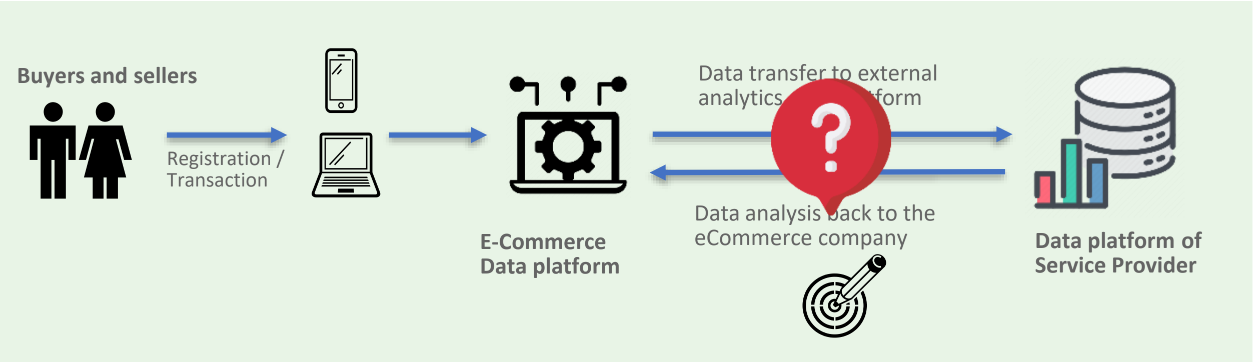
E2. The Company implements technical measures to support the protection on PII /important data/sensitive data during data processing and to ensure justifiable use and analysis of data.

E3. The Company uses secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data. Data import and export are controlled and monitored. Cache in data import and export channels are cleansed to prevent malicious data restoration.


Policies and Procedures
Personnel Management
Compliance
Physical Security
Operation
Incident Management
Business Continuity Management
Vendor Management
Monitoring, Logging and Auditing
Asset Management
Cryptography & Key management
Network and Communication Management
Identity and Access Management
Data Processing & Exchange Security
Data
Create
Store
Use
Share
Archive
Destroy

iBDG Big Data Governance Certification Programme
- Illustration: Application of the Control Objectives

Illustration - eCommerce

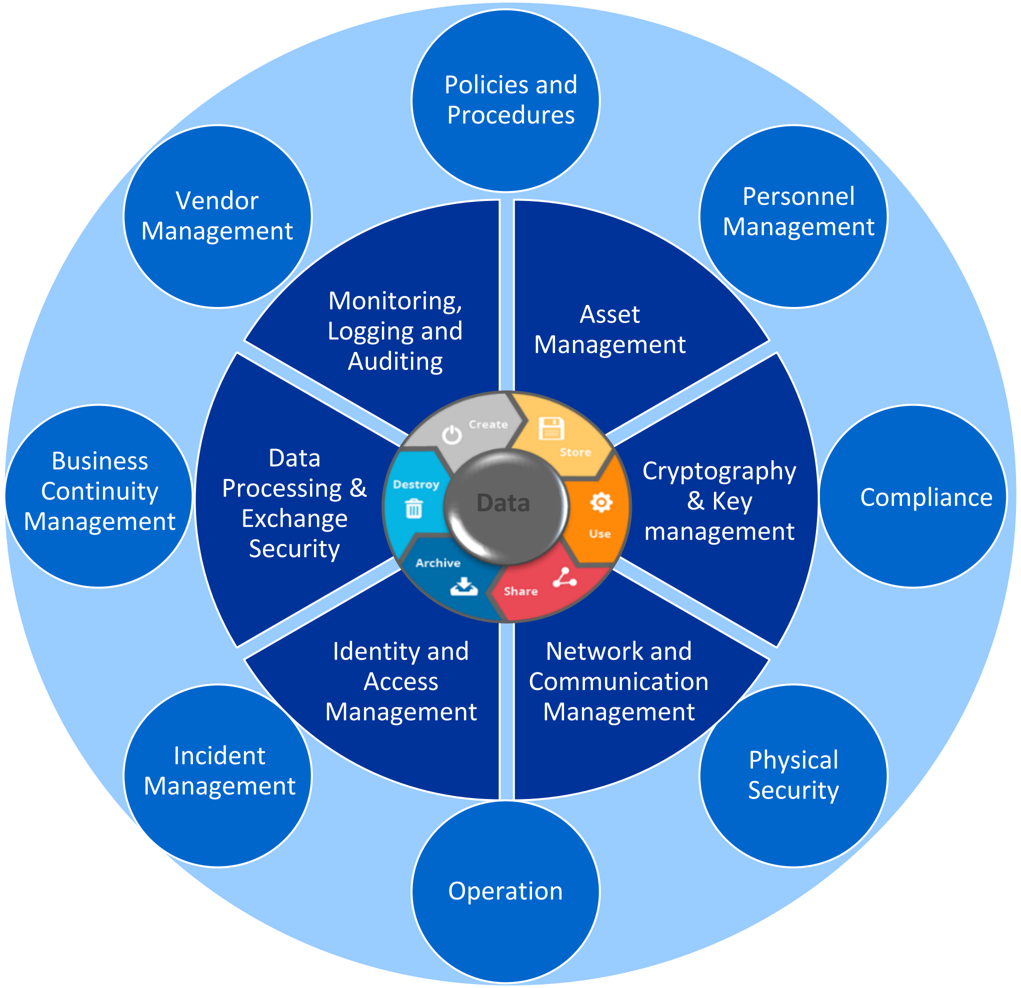

Buyers and sellers
Registration / Transaction
E-Commerce Data platform
Data transfer to external analytics tform
Data analysis back to the eCommerce company
Data platform of Service Provider

A5. The Company set up policies and procedures and technical measures to ensure secure and irrevocable disposal of assets, which include data and data storage media

F2. Data log recording access to and operation on data shall be produced, kept and regularly reviewed. The monitoring and auditing during each phase of data life cycle are enforced to prevent unauthorized access, abuse and leakage of data.

F3. The Company deploys the necessary data leakage prevention real-time monitoring technology and tools, monitor and report the unauthorized external distribution of personal information, important data, etc.

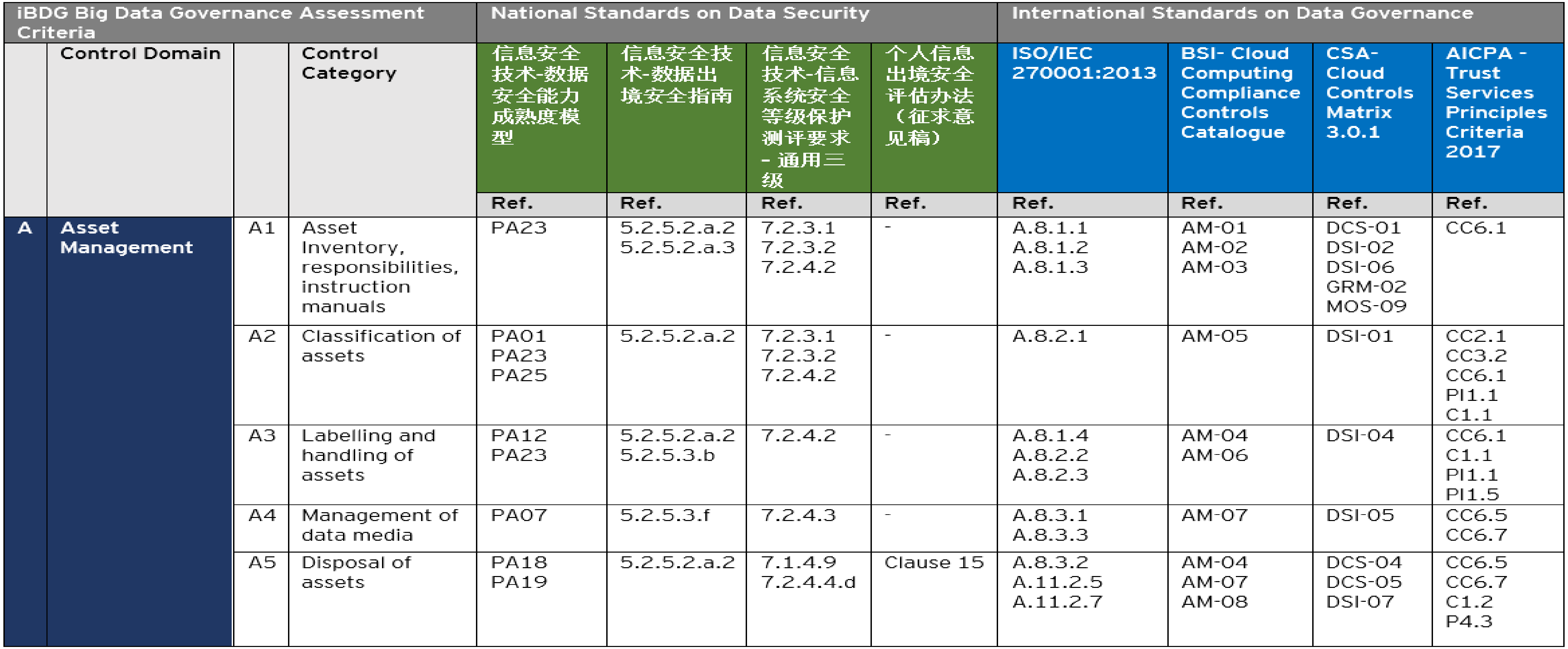
F6. Logs are retained in sufficient time frame in accordance with legislative, regulatory, contractual and business requirements.


Policies and Procedures
Personnel Management
Compliance
Physical Security
Operation
Incident Management
Business Continuity Management
Vendor Management
Monitoring, Logging and Auditing
Asset Management
Cryptography & Key management
Network and Communication Management
Identity and Access Management
Data Processing & Exchange Security
Data
Create
Store
Use
Share
Archive
Destroy

iBDG Big Data Governance Certification Programme
- Underlying National and International Standards

Referencing iBDG Assessment Criteria to National and International Standards

For illustration



iBDG Big Data Governance Assessment Criteria				National Standards on Data Security				International Standards on Data Governance			
	Control Domain		Control Category	信息安全技术-数据安全能力成熟度模型	信息安全技术-数据出境安全指南	信息安全技术-信息系统安全等级保护测评要求 - 通用三级	个人信息出境安全评估办法（征求意见稿）	ISO/IEC 270001:2013	BSI- Cloud Computing Compliance Controls Catalogue	CSA- Cloud Controls Matrix 3.0.1	AICPA - Trust Services Principles Criteria 2017
				Ref.	Ref.	Ref.	Ref.	Ref.	Ref.	Ref.	Ref.
A	Asset Management	A1	Asset Inventory, responsibilities, instruction manuals	PA23	5.2.5.2.a.2 5.2.5.2.a.3	7.2.3.1 7.2.3.2 7.2.4.2	-	A.8.1.1 A.8.1.2 A.8.1.3	AM-01 AM-02 AM-03	DCS-01 DSI-02 DSI-06 GRM-02 MOS-09	CC6.1
		A2	Classification of assets	PA01 PA23 PA25	5.2.5.2.a.2	7.2.3.1 7.2.3.2 7.2.4.2	-	A.8.2.1	AM-05	DSI-01	CC2.1 CC3.2 CC6.1 PI1.1 C1.1
		A3	Labelling and handling of assets	PA12 PA23	5.2.5.2.a.2 5.2.5.3.b	7.2.4.2	-	A.8.1.4 A.8.2.2 A.8.2.3	AM-04 AM-06	DSI-04	CC6.1 C1.1 PI1.1 PI1.5
		A4	Management of data media	PA07	5.2.5.3.f	7.2.4.3	-	A.8.3.1 A.8.3.3	AM-07	DSI-05	CC6.5 CC6.7
		A5	Disposal of assets	PA18 PA19	5.2.5.2.a.2	7.1.4.9 7.2.4.4.d	Clause 15	A.8.3.2 A.11.2.5 A.11.2.7	AM-04 AM-07 AM-08	DCS-04 DCS-05 DSI-07	CC6.5 CC6.7 C1.2 P4.3

iBDG Certification Process

Preparation by the Company

Planning – Audit plan is agreed between the organization and the independent auditor regarding the audit scope, audit timeline and reporting schedule, etc.

Organization under audit

iBDG Accredited Auditor

- Identify expectations
- Gain high-level understanding of key processes
- Benchmark with ***iBDG Big Data Governance Assessment Criteria***
- Verify whether processes and controls are properly designed
- Prepare recommendations for improvements

Performs examination

Execution – The audit is expected to be conducted through performance of the following activities:

- Review of relevant documentation (e.g. design specifications, operational flow, security policies and standards, operational control procedures, logs, etc.)
- Discussion with management and relevant personnel
- Observation of actual performance of operational procedures
- Sample review of relevant records or logs
- Security review of technical components

Evaluation – Evaluate the system descriptions and design and operational effectiveness of controls referencing to ***iBDG Big Data Governance Assessment Criteria***

Communicate results

Reporting – The report is provided to management of the organization on data governance and protection control design and operation effectiveness.

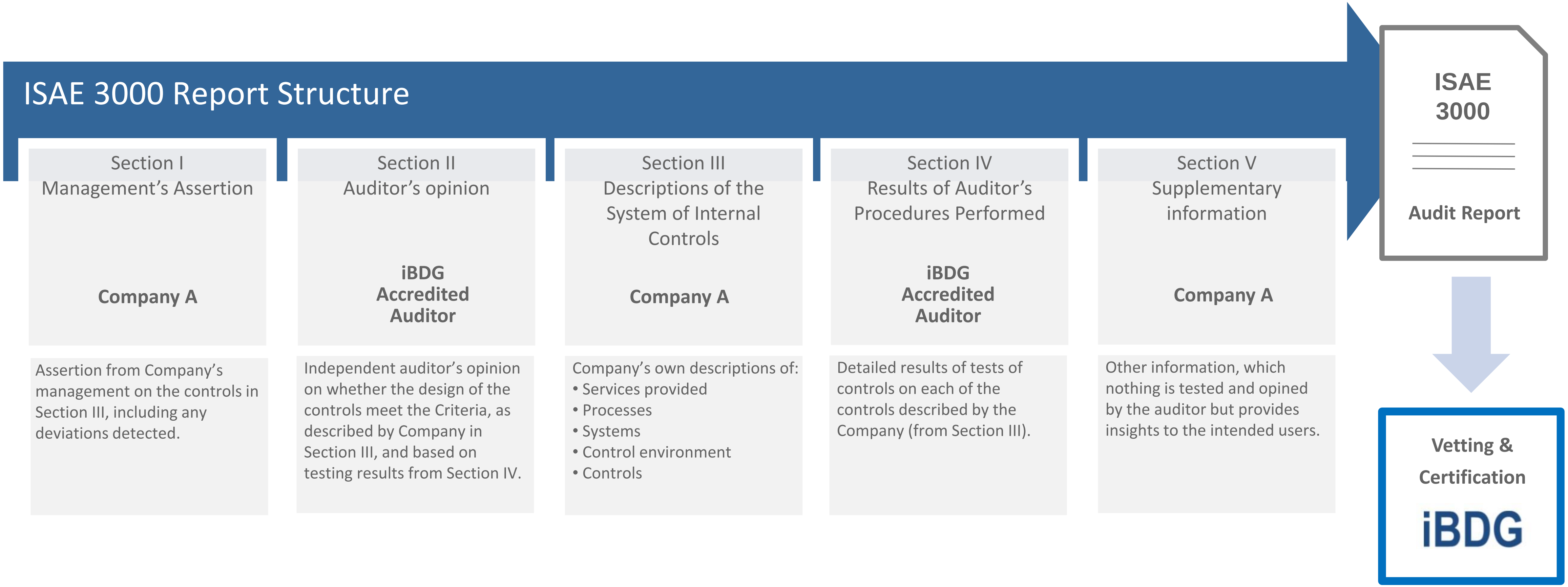
Findings and recommendations report

ISAE 3000 Report with ***iBDG Big Data Governance Assessment Criteria***

Auditing and reporting is carried out by applying **ISAE 3000 (Revised) "Assurance Engagements Other than Audits or Reviews of Historical Financial Information"**. ISAE 3000 (Revised) describes general requirements for the qualification and conduct of an auditor as well as for accepting, planning and carrying out an audit engagement.

During the examinations the organization under audit can improve processes and implement controls to mitigate any identified findings and risks. With this approach there will be a continuous improvement for the organization under audit. Also, the organization shall keep its controls up to date in accordance with legislative, regulatory, contractual and business requirements

iBDG Certification Process
- Auditor Report and iBDG Vetting & Certification



ISAE 3000 Report Structure

Section I	Section II	Section III	Section IV	Section V
Management's Assertion	Auditor's opinion	Descriptions of the System of Internal Controls	Results of Auditor's Procedures Performed	Supplementary information
Company A	**iBDG Accredited Auditor**	**Company A**	**iBDG Accredited Auditor**	**Company A**
Assertion from Company's management on the controls in Section III, including any deviations detected.	Independent auditor's opinion on whether the design of the controls meet the Criteria, as described by Company in Section III, and based on testing results from Section IV.	Company's own descriptions of: • Services provided • Processes • Systems • Control environment • Controls	Detailed results of tests of controls on each of the controls described by the Company (from Section III).	Other information, which nothing is tested and opined by the auditor but provides insights to the intended users.

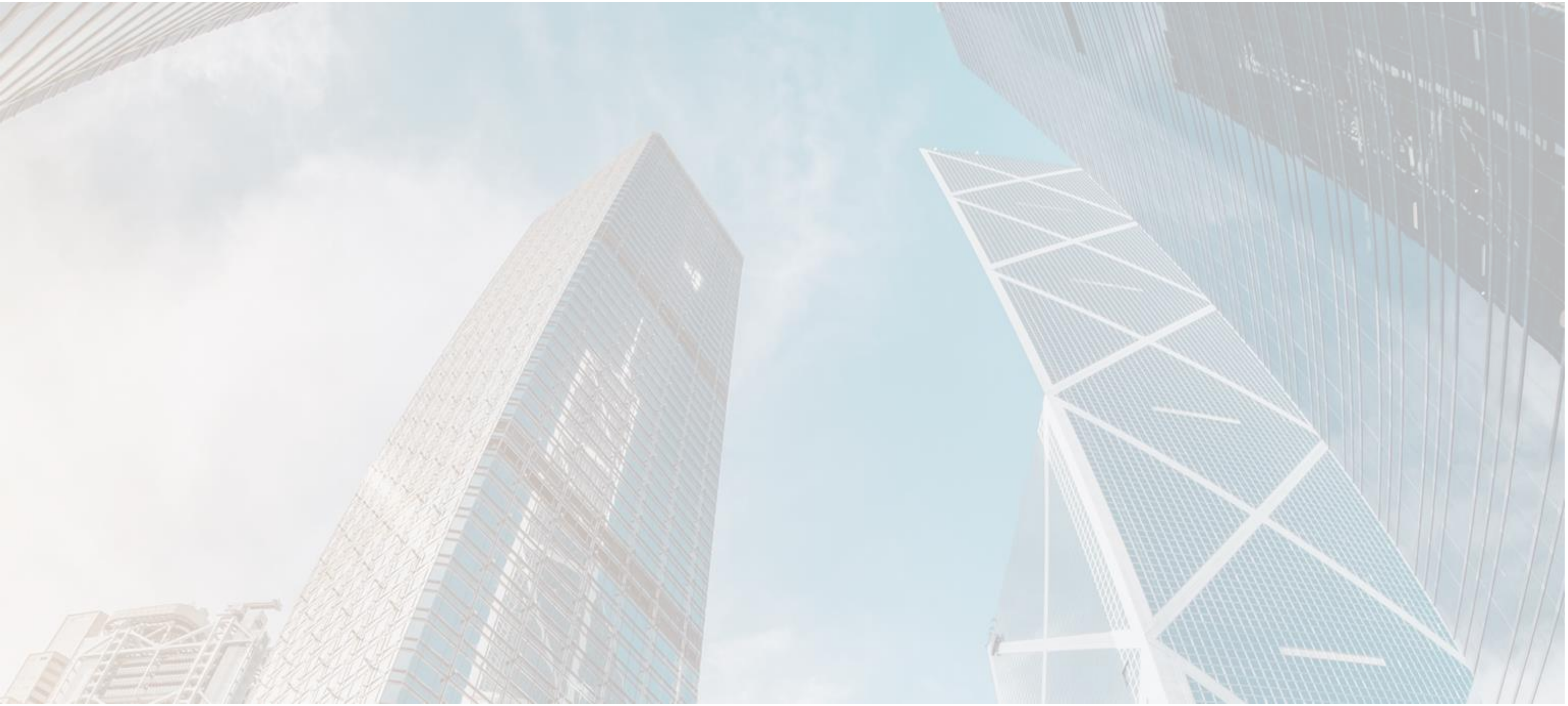
ISAE 3000

Audit Report

Vetting & Certification

iBDG

Part IV :
How iBDG’s Certification Aligns with Regulatory Requirements



iBDG Big Data Governance Certification Programme
– Alignment with the Requirements of Data Security Law

Area	Data Security Law
Data Security Assessment and Certification	**Article 18:** The state is to promote the development of services such as data security testing, appraisals, and certification, and support professional institutions to carryout data security testing, appraisals, and certification service activities. The state is to support collaboration among relevant departments, industry organizations, enterprises, educational and scientific research institutions, and relevant professional institutions in data security risk assessment, prevention, and disposal. **第十八条 -** 国家促进数据安全检测评估、认证等服务的发展，支持数据安全检测评估、认证等专业机构依法开展服务活动。国家支持有关部门、行业组织、企业、教育和科研机构、有关专业机构等在数据安全风险评估、防范、处置等方面开展协作。
The Expectation on Data Governance	**Article 11:** The state is to actively carry out international exchanges and cooperation in the sectors of data security governance and data development and use, participate in the formulation of international rules and standards related to data security, and promote the safe and free flow of data across borders. **第十一条** - 国家积极开展数据安全治理、数据开发利用等领域的国际交流与合作，参与数据安全相关国际规则和标准的制定，促进数据跨境安全、自由流动。 **Article 13:** The state is to make overall plans for development and security, persisting in unsighted development and use of data and industry development to promote data security, and using data security to ensure the development and use of data and industry development. **第十三条** - 国家统筹发展和安全，坚持以数据开发利用和产业发展促进数据安全，以数据安全保障数据开发利用和产业发展。

iBDG Big Data Governance Certification Programme
– Alignment with the Requirements of Data Security Law

Area	Data Security Law
The Expectation on Data Governance	**Article 14:** The state is to implement a big data strategy, advancing the establishment of data infrastructure, and encouraging and supporting innovative applications of detain each industry and field. **第十四条** - 国家实施大数据战略，推进数据基础设施建设，鼓励和支持数据在各行业、各领域的创新应用。 **Article 17:** The state is to advance the establishment of a system of standards for data development and exploitation technologies and data security. Within the scope of their respective duties, the State Council departments in charge of standardization and other relevant State Council departments are to organize the formulation and appropriate revision of standards related to technology and products for the development and use of data and to data security. The state is to support enterprises and social groups, educational or research bodies, and so forth, participating in drafting standards. **第十七条** - 国家推进数据开发利用技术和数据安全标准体系建设。国务院标准化行政主管部门和国务院有关部门根据各自的职责，组织制定并适时修订有关数据开发利用技术、产品和数据安全相关标准。国家支持企业、社会团体和教育、科研机构等参与标准制定。

iBDG Big Data Governance Certification Programme
– Alignment with the Requirements of Data Security Law

No.	Control Domains	Data Security Law
A	Asset Management	**Article 21:** The state is to establish a categorical and hierarchical system for data protection and carry out categorized and graded data protections based on the importance of the data in economic and social development as well as the extent of harm to national security, the public interest, or the lawful rights and interests of citizens or organizations that would be caused once the data is altered, destroyed, leaked, or illegally obtained or used. The national data security coordination mechanism coordinates the relevant departments to determine a catalog of important data and strengthen protections of the important data. Data related to national security, the lifeblood of the national economy, important people's livelihood, major public interests, and others belong to the national core data, shall apply to a more stringent management system. Each region and department shall determine the catalog of important data within that region and department and corresponding industries and sectors on the basis of the categorical and hierarchical protection system and conduct key protection for data entered in the catalog. **第二十一条** – 国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。 关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度。 各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。

iBDG Big Data Governance Certification Programme
– Alignment with the Requirements of Data Security Law

No.	Control Domains	Data Security Law
A	Asset Management	**Article 27:** The carrying out of data handling activities shall be in accordance with laws and regulations, establishing and completing data security management systems for the entire process, organizing, and carrying out education entraining data security, and employing corresponding technical measures and other necessary measures to safeguard data security. The carrying out of data handling activities through information networks, i.e., the Internet, shall fulfill the duties to protect data security on the basis of the multi-level protection system for cybersecurity. Those processing important data shall clearly designate persons responsible for data security and data security management bodies to implement responsibilities for data security protection. **第二十七条** – 开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。 重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。 **Article 30:** Those handling important data shall follow periodically carry out risk assessments of their data handling activities as provided, and send risk assessment reports to the relevant regulatory departments. Risk assessment reports shall include the types and amounts of important data being handled; the circumstances of the data handling activities; the data risks faced, methods for addressing them, and so forth. **第三十条** – 重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。 风险评估报告应当包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等。

iBDG Big Data Governance Certification Programme
– Alignment with the Requirements of Data Security Law

No.	Control Domains	Data Security Law
E	Data Processing and Exchange Security	**Article 27:** The carrying out of data handling activities shall be in accordance with laws and regulations, establishing and completing data security management systems for the entire process, organizing, and carrying out education entraining data security, and employing corresponding technical measures and other necessary measures to safeguard data security. The carrying out of data handling activities through information networks, i.e., the Internet, shall fulfill the duties to protect data security on the basis of the multi-level protection system for cybersecurity. Those processing important data shall clearly designate persons responsible for data security and data security management bodies to implement responsibilities for data security protection. **第三十一条** – 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定；其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。
F	Monitoring, Logging and Auditing	**Article 33:** When institutions engaged in data transaction intermediary services provide services, they shall require the party providing data to explain the sources of the data, verify the identities of both parties to the transcation, and store a record of the review and transaction. **第三十三条** – 从事数据交易中介服务的机构提供服务，应当要求数据提供方说明数据来源，审核交易双方的身份，并留存审核、事务历史记录。

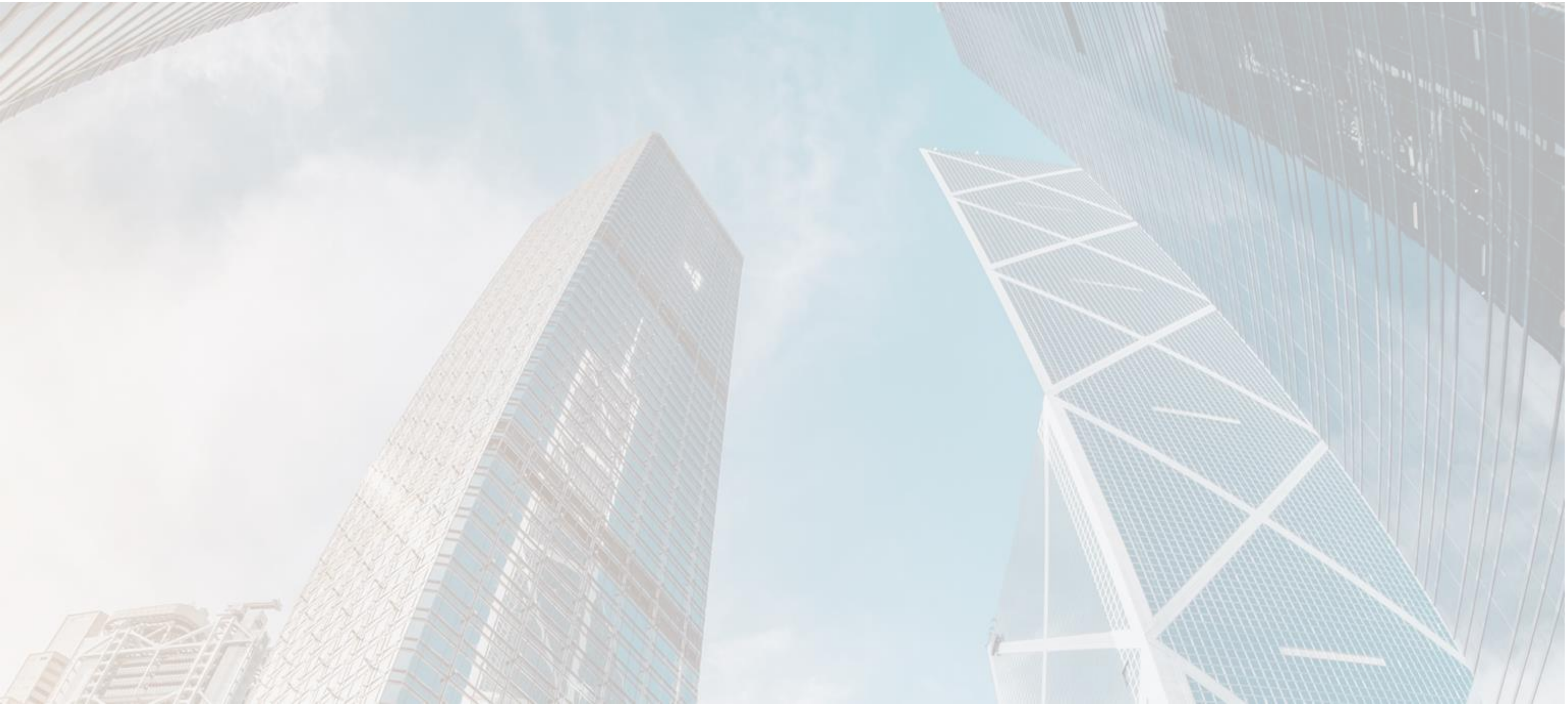
iBDG Big Data Governance Certification Programme
– Alignment with the Requirements of Data Security Law

No.	Control Domains	Data Security Law
G	Policies and Procedures	**Article 27:** The carrying out of data handling activities shall be in accordance with laws and regulations, establishing and completing data security management systems for the entire process, organizing, and carrying out education entraining data security, and employing corresponding technical measures and other necessary measures to safeguard data security. The carrying out of data handling activities through information networks, i.e., the Internet, shall fulfill the duties to protect data security on the basis of the multi-level protection system for cybersecurity. Those processing important data shall clearly designate persons responsible for data security and data security management bodies to implement responsibilities for data security protection. **第二十七条** - 开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。 重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。
H	Personnel Management	**Article 20:** The state is to support education, research institutions, enterprises, and so forth, in carrying out education and training related to data use and development and data security, employing diverse methods to cultivate professional data use and development and data security talent, and promote talent exchanges. **第二十条** - 国家支持教育、科研机构和企业等开展数据开发利用技术和数据安全相关教育和培训，采取多种方式培养数据开发利用技术和数据安全专业人才，促进人才交流。

iBDG Big Data Governance Certification Programme
– Alignment with the Requirements of Data Security Law

No.	Control Domains	Data Security Law
J	Incident Management	**Article 23:** The state is to establish data security emergency response mechanisms. Relevant regulatory departments shall initiate emergency response plans in accordance with law when data security incidents occur, employing the corresponding emergency response and handling measures to prevent the harm from increasing and eliminate security risks, and promptly issue relevant alerts to the public. **第二十三条** – 国家建立数据安全应急处置机制。发生数据安全事件，有关主管部门应当依法启动应急预案，采取相应的应急处置措施，防止危害扩大，消除安全隐患，并及时向社会发布与公众有关的警示信息。
M	Operation	**Article 29:** The carrying out of data handling activities shall strengthen risk monitoring, and when data security flaws, vulnerabilities, or other risks are discovered, remedial measures shall be immediately employed; and when data security incidents occur, methods for addressing them shall be immediately employed, users are to be promptly notified as provided, and reports are to be made to the relevant regulatory departments. **第二十九条** – 开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。

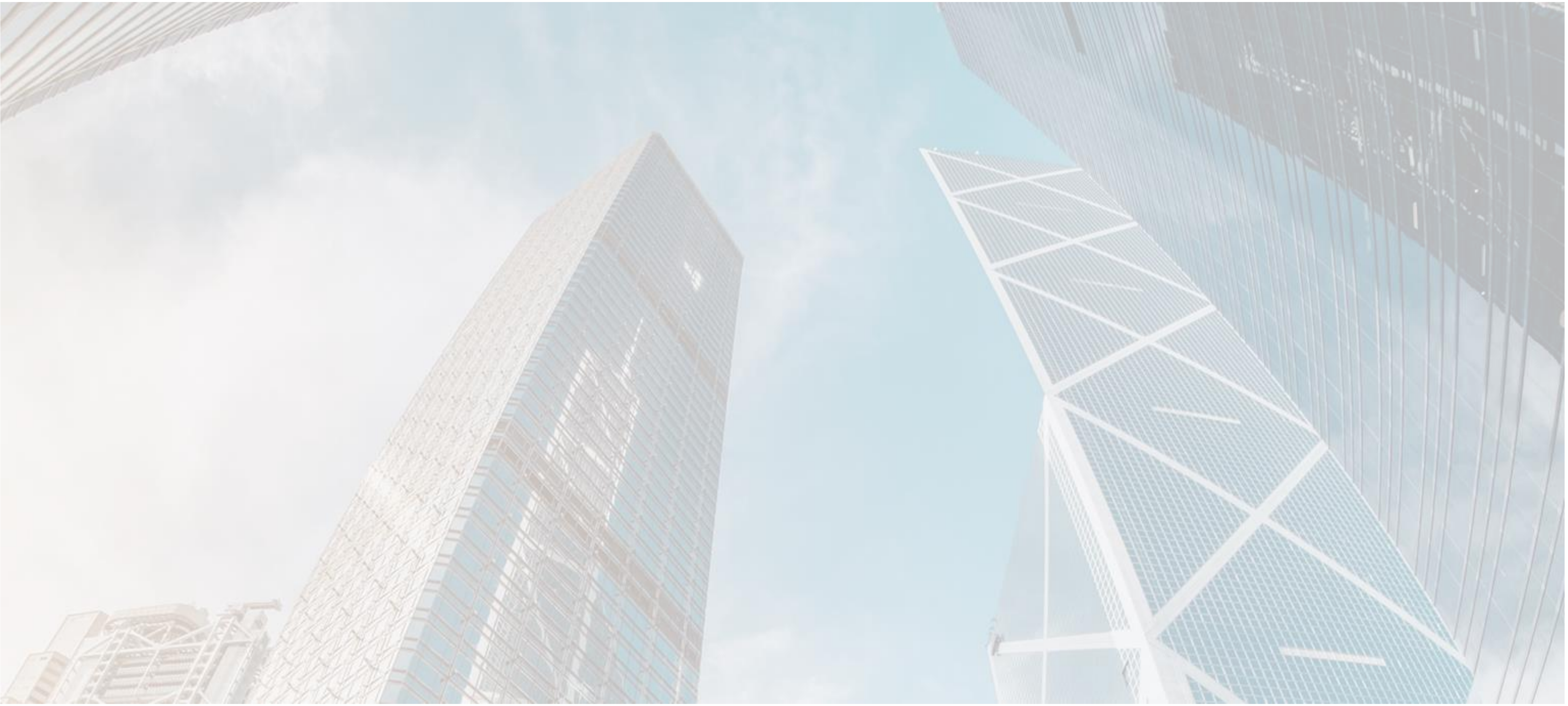
Part V -
Questions & Answer Session



Appendix:

iBDG Big Data Governance Assessment Criteria

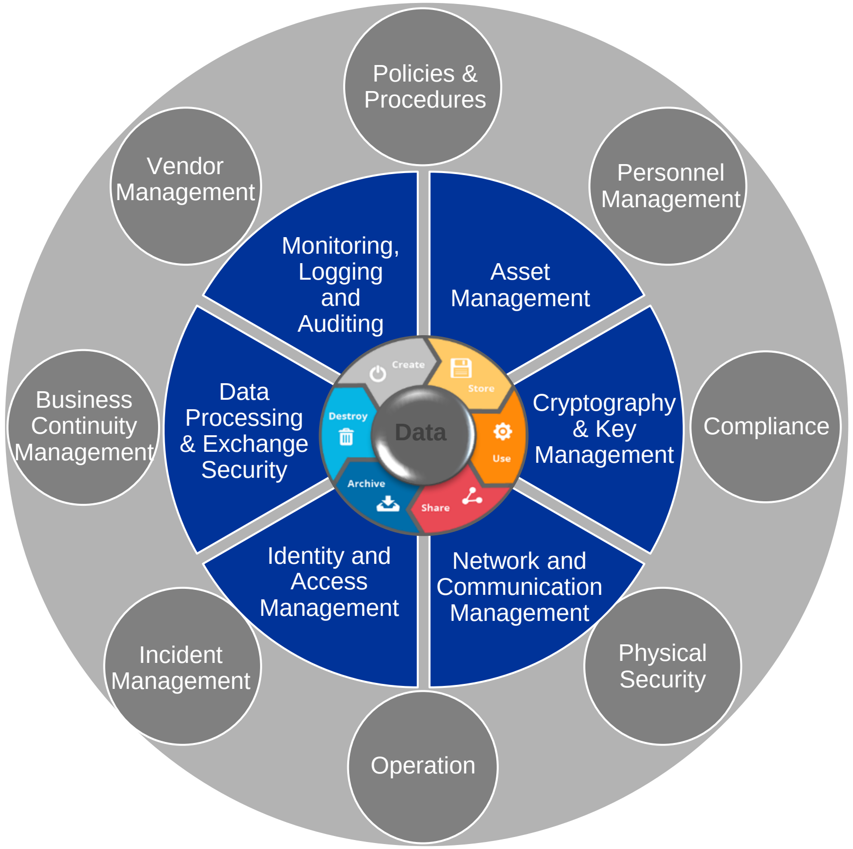
- A closer look



iBDG Big Data Governance Assessment Criteria
– Data Protection Domains

Data Protection Domains

The Data Protection Domains are intended to be used for assessment of control measures and safeguards when the data were created, stored, used, shared, archived or destroyed, as shown in the diagram below:

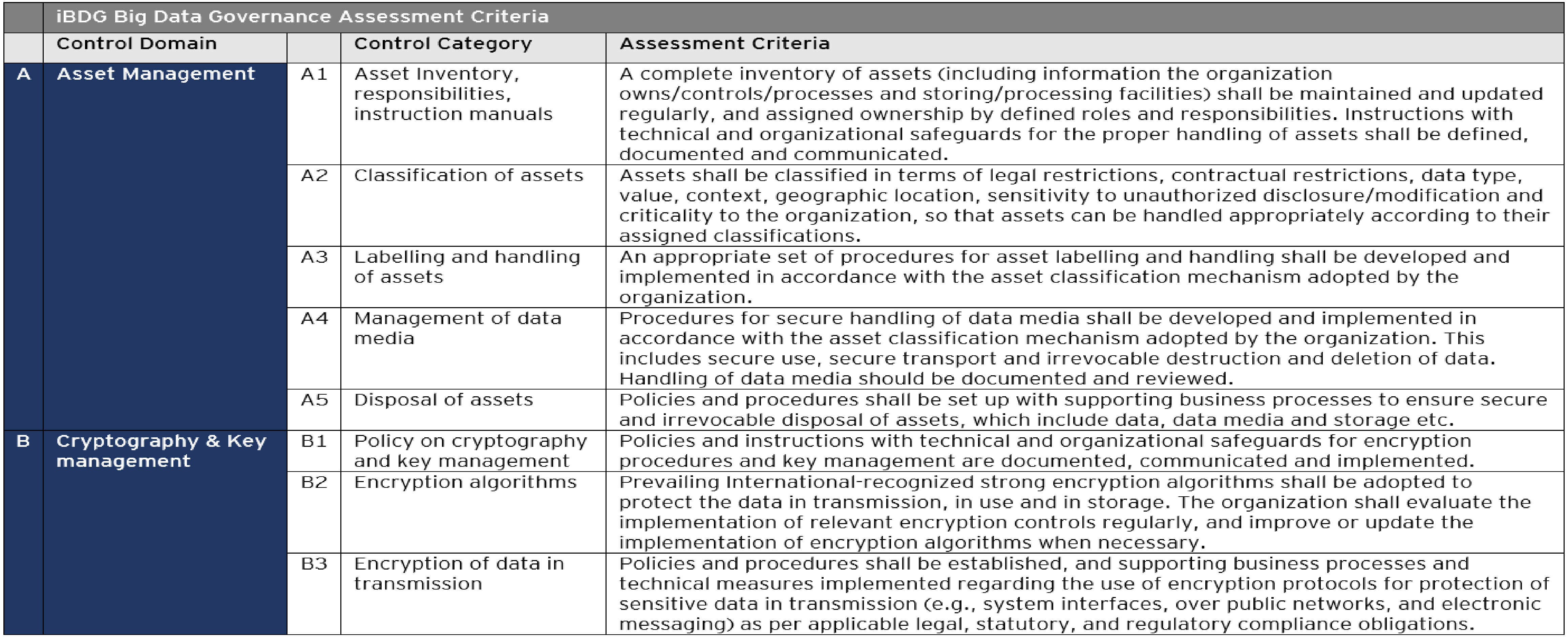


Policies & Procedures
Vendor Management
Personnel Management
Monitoring, Logging and Auditing
Asset Management
Business Continuity Management
Data Processing & Exchange Security
Cryptography & Key Management
Compliance
Create
Store
Use
Share
Archive
Destroy
Data
Identity and Access Management
Network and Communication Management
Incident Management
Physical Security
Operation

The Data Protection Domains are structured into the following sections:

A. Asset Management
B. Cryptography and Key Management
C. Network and Communication Management
D. Identity and Access Management
E. Data Processing and Exchange Security
F. Monitoring, Logging and Auditing

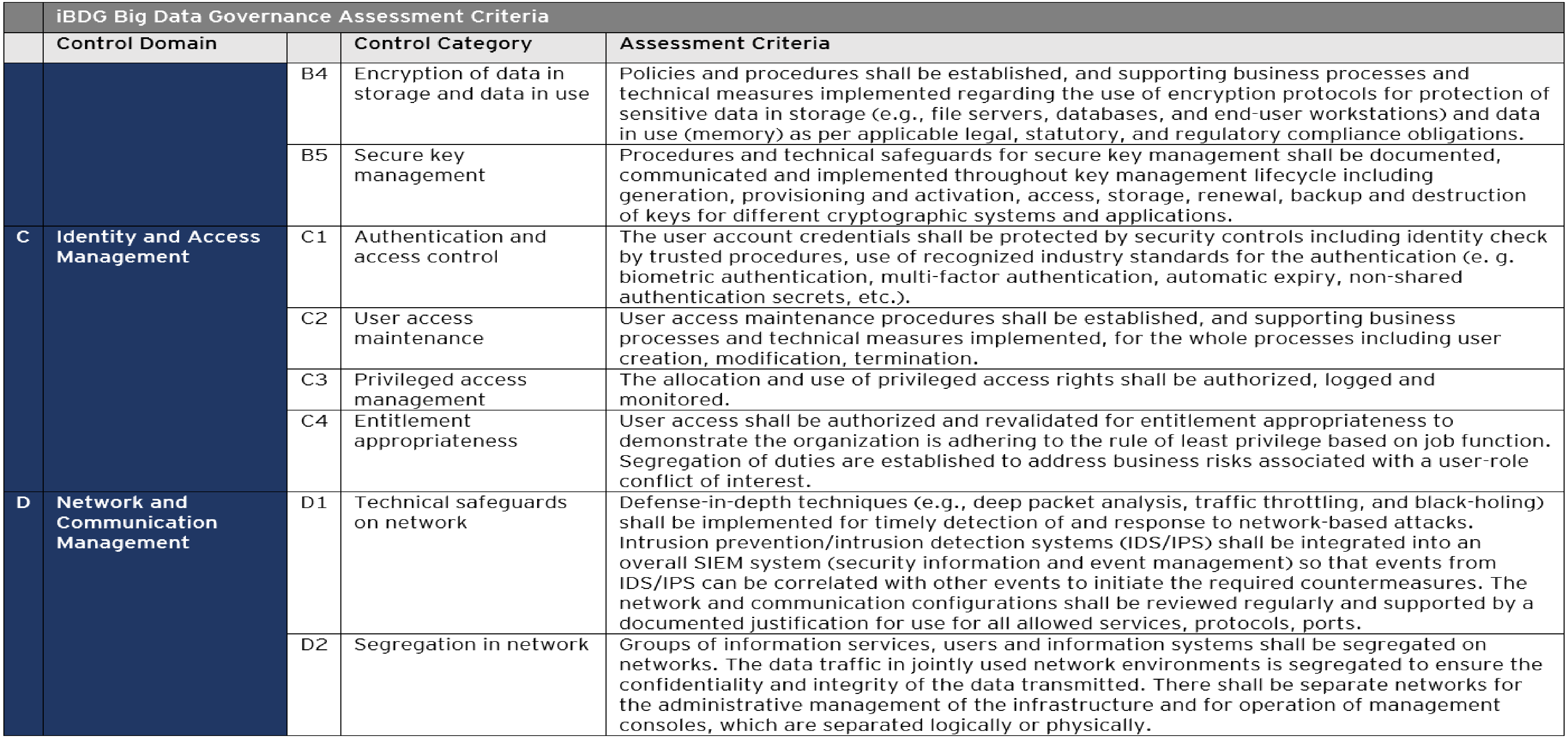
iBDG Big Data Governance Assessment Criteria
– Data Protection Domains



	iBDG Big Data Governance Assessment Criteria			
	Control Domain		**Control Category**	**Assessment Criteria**
A	**Asset Management**	A1	Asset Inventory, responsibilities, instruction manuals	A complete inventory of assets (including information the organization owns/controls/processes and storing/processing facilities) shall be maintained and updated regularly, and assigned ownership by defined roles and responsibilities. Instructions with technical and organizational safeguards for the proper handling of assets shall be defined, documented and communicated.
		A2	Classification of assets	Assets shall be classified in terms of legal restrictions, contractual restrictions, data type, value, context, geographic location, sensitivity to unauthorized disclosure/modification and criticality to the organization, so that assets can be handled appropriately according to their assigned classifications.
		A3	Labelling and handling of assets	An appropriate set of procedures for asset labelling and handling shall be developed and implemented in accordance with the asset classification mechanism adopted by the organization.
		A4	Management of data media	Procedures for secure handling of data media shall be developed and implemented in accordance with the asset classification mechanism adopted by the organization. This includes secure use, secure transport and irrevocable destruction and deletion of data. Handling of data media should be documented and reviewed.
		A5	Disposal of assets	Policies and procedures shall be set up with supporting business processes to ensure secure and irrevocable disposal of assets, which include data, data media and storage etc.
B	**Cryptography & Key management**	B1	Policy on cryptography and key management	Policies and instructions with technical and organizational safeguards for encryption procedures and key management are documented, communicated and implemented.
		B2	Encryption algorithms	Prevailing International-recognized strong encryption algorithms shall be adopted to protect the data in transmission, in use and in storage. The organization shall evaluate the implementation of relevant encryption controls regularly, and improve or update the implementation of encryption algorithms when necessary.
		B3	Encryption of data in transmission	Policies and procedures shall be established, and supporting business processes and technical measures implemented regarding the use of encryption protocols for protection of sensitive data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.

iBDG Big Data Governance Assessment Criteria

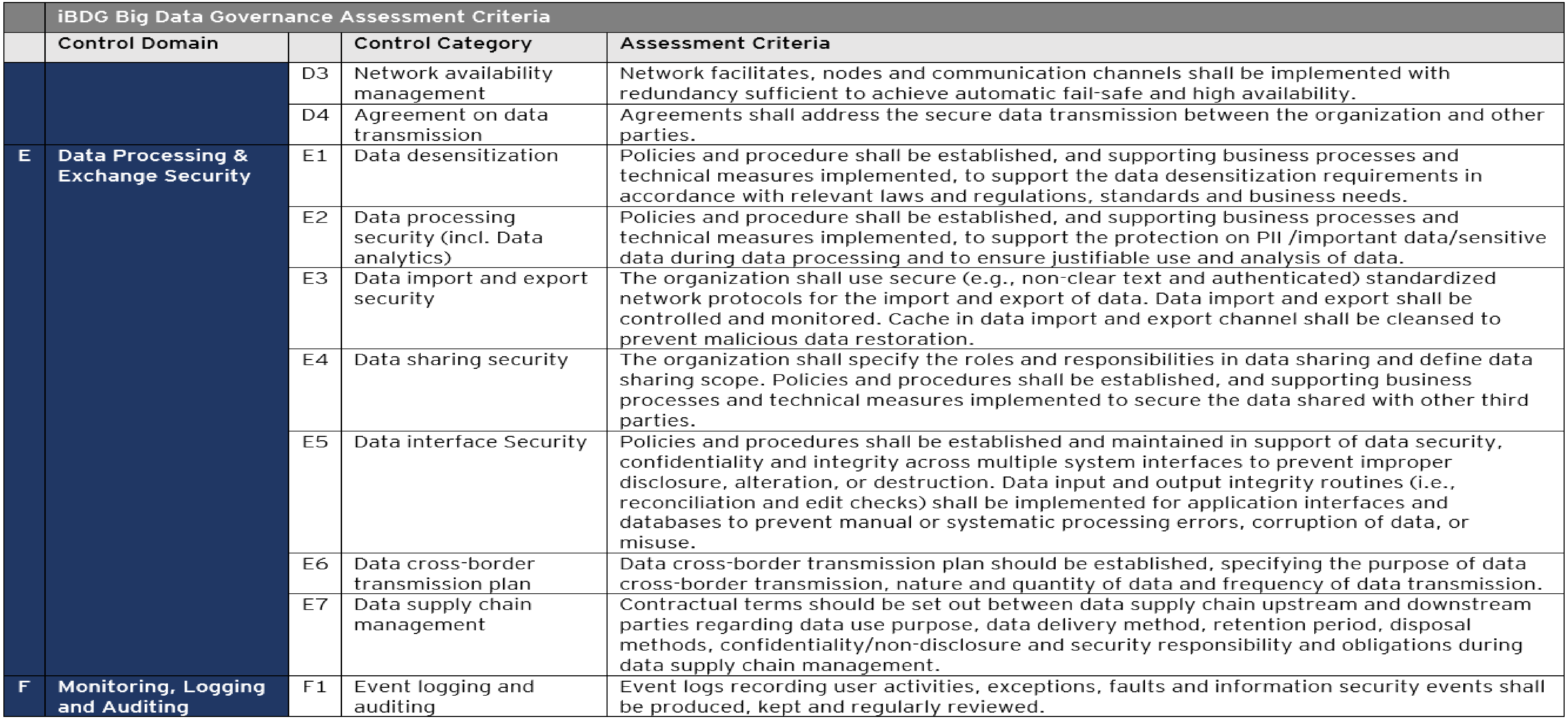
– Data Protection Domains



	iBDG Big Data Governance Assessment Criteria			
	Control Domain		Control Category	Assessment Criteria
		B4	Encryption of data in storage and data in use	Policies and procedures shall be established, and supporting business processes and technical measures implemented regarding the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations) and data in use (memory) as per applicable legal, statutory, and regulatory compliance obligations.
		B5	Secure key management	Procedures and technical safeguards for secure key management shall be documented, communicated and implemented throughout key management lifecycle including generation, provisioning and activation, access, storage, renewal, backup and destruction of keys for different cryptographic systems and applications.
C	Identity and Access Management	C1	Authentication and access control	The user account credentials shall be protected by security controls including identity check by trusted procedures, use of recognized industry standards for the authentication (e. g. biometric authentication, multi-factor authentication, automatic expiry, non-shared authentication secrets, etc.).
		C2	User access maintenance	User access maintenance procedures shall be established, and supporting business processes and technical measures implemented, for the whole processes including user creation, modification, termination.
		C3	Privileged access management	The allocation and use of privileged access rights shall be authorized, logged and monitored.
		C4	Entitlement appropriateness	User access shall be authorized and revalidated for entitlement appropriateness to demonstrate the organization is adhering to the rule of least privilege based on job function. Segregation of duties are established to address business risks associated with a user-role conflict of interest.
D	Network and Communication Management	D1	Technical safeguards on network	Defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) shall be implemented for timely detection of and response to network-based attacks. Intrusion prevention/intrusion detection systems (IDS/IPS) shall be integrated into an overall SIEM system (security information and event management) so that events from IDS/IPS can be correlated with other events to initiate the required countermeasures. The network and communication configurations shall be reviewed regularly and supported by a documented justification for use for all allowed services, protocols, ports.
		D2	Segregation in network	Groups of information services, users and information systems shall be segregated on networks. The data traffic in jointly used network environments is segregated to ensure the confidentiality and integrity of the data transmitted. There shall be separate networks for the administrative management of the infrastructure and for operation of management consoles, which are separated logically or physically.

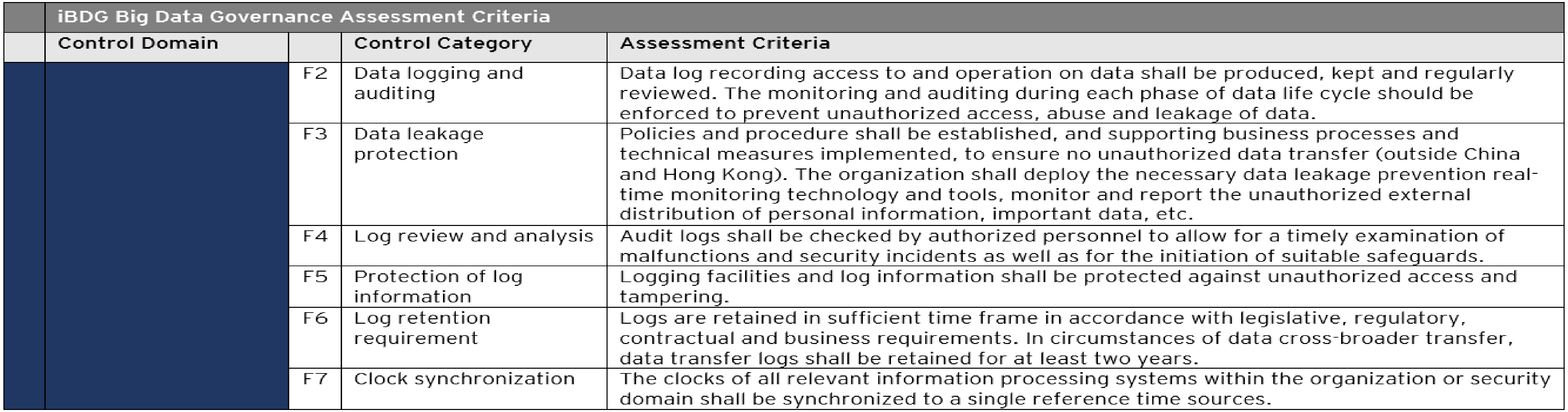
iBDG

iBDG Big Data Governance Assessment Criteria
– Data Protection Domains



	iBDG Big Data Governance Assessment Criteria			
	Control Domain		Control Category	Assessment Criteria
		D3	Network availability management	Network facilitates, nodes and communication channels shall be implemented with redundancy sufficient to achieve automatic fail-safe and high availability.
		D4	Agreement on data transmission	Agreements shall address the secure data transmission between the organization and other parties.
E	Data Processing & Exchange Security	E1	Data desensitization	Policies and procedure shall be established, and supporting business processes and technical measures implemented, to support the data desensitization requirements in accordance with relevant laws and regulations, standards and business needs.
		E2	Data processing security (incl. Data analytics)	Policies and procedure shall be established, and supporting business processes and technical measures implemented, to support the protection on PII /important data/sensitive data during data processing and to ensure justifiable use and analysis of data.
		E3	Data import and export security	The organization shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data. Data import and export shall be controlled and monitored. Cache in data import and export channel shall be cleansed to prevent malicious data restoration.
		E4	Data sharing security	The organization shall specify the roles and responsibilities in data sharing and define data sharing scope. Policies and procedures shall be established, and supporting business processes and technical measures implemented to secure the data shared with other third parties.
		E5	Data interface Security	Policies and procedures shall be established and maintained in support of data security, confidentiality and integrity across multiple system interfaces to prevent improper disclosure, alteration, or destruction. Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.
		E6	Data cross-border transmission plan	Data cross-border transmission plan should be established, specifying the purpose of data cross-border transmission, nature and quantity of data and frequency of data transmission.
		E7	Data supply chain management	Contractual terms should be set out between data supply chain upstream and downstream parties regarding data use purpose, data delivery method, retention period, disposal methods, confidentiality/non-disclosure and security responsibility and obligations during data supply chain management.
F	Monitoring, Logging and Auditing	F1	Event logging and auditing	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.

iBDG Big Data Governance Assessment Criteria
– Data Protection Domains

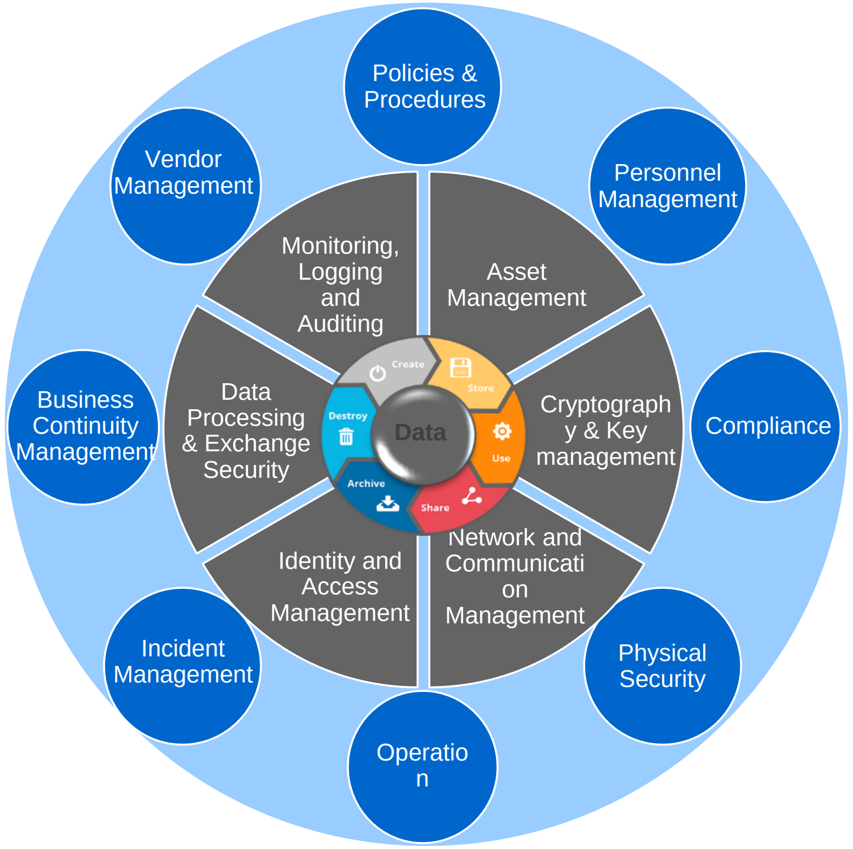


	iBDG Big Data Governance Assessment Criteria			
	Control Domain		Control Category	Assessment Criteria
		F2	Data logging and auditing	Data log recording access to and operation on data shall be produced, kept and regularly reviewed. The monitoring and auditing during each phase of data life cycle should be enforced to prevent unauthorized access, abuse and leakage of data.
		F3	Data leakage protection	Policies and procedure shall be established, and supporting business processes and technical measures implemented, to ensure no unauthorized data transfer (outside China and Hong Kong). The organization shall deploy the necessary data leakage prevention real-time monitoring technology and tools, monitor and report the unauthorized external distribution of personal information, important data, etc.
		F4	Log review and analysis	Audit logs shall be checked by authorized personnel to allow for a timely examination of malfunctions and security incidents as well as for the initiation of suitable safeguards.
		F5	Protection of log information	Logging facilities and log information shall be protected against unauthorized access and tampering.
		F6	Log retention requirement	Logs are retained in sufficient time frame in accordance with legislative, regulatory, contractual and business requirements. In circumstances of data cross-broader transfer, data transfer logs shall be retained for at least two years.
		F7	Clock synchronization	The clocks of all relevant information processing systems within the organization or security domain shall be synchronized to a single reference time sources.

iBDG Big Data Governance Assessment Criteria
– Control Environment Domains

Control Environment Domain

The Control Environment Domains are intended to be used for assessment of general controls that support the protection on data by providing a sound control environment, as shown in the diagram below:

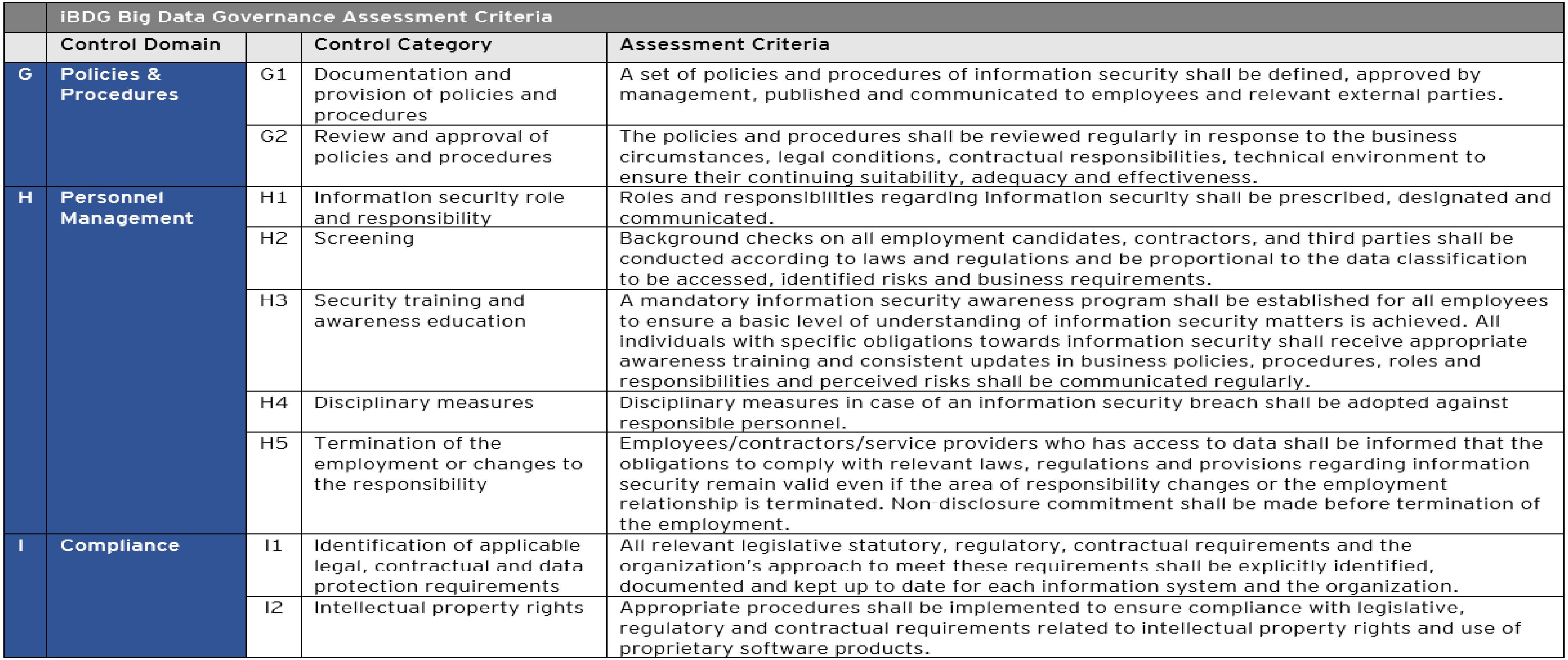


Policies & Procedures
Personnel Management
Compliance
Physical Security
Operatio n
Incident Management
Business Continuity Management
Vendor Management
Monitoring, Logging and Auditing
Asset Management
Cryptograph y & Key management
Network and Communicati on Management
Identity and Access Management
Data Processing & Exchange Security
Data
Create
Store
Use
Share
Archive
Destroy

This Control Environment Domains are structured into the following sections:

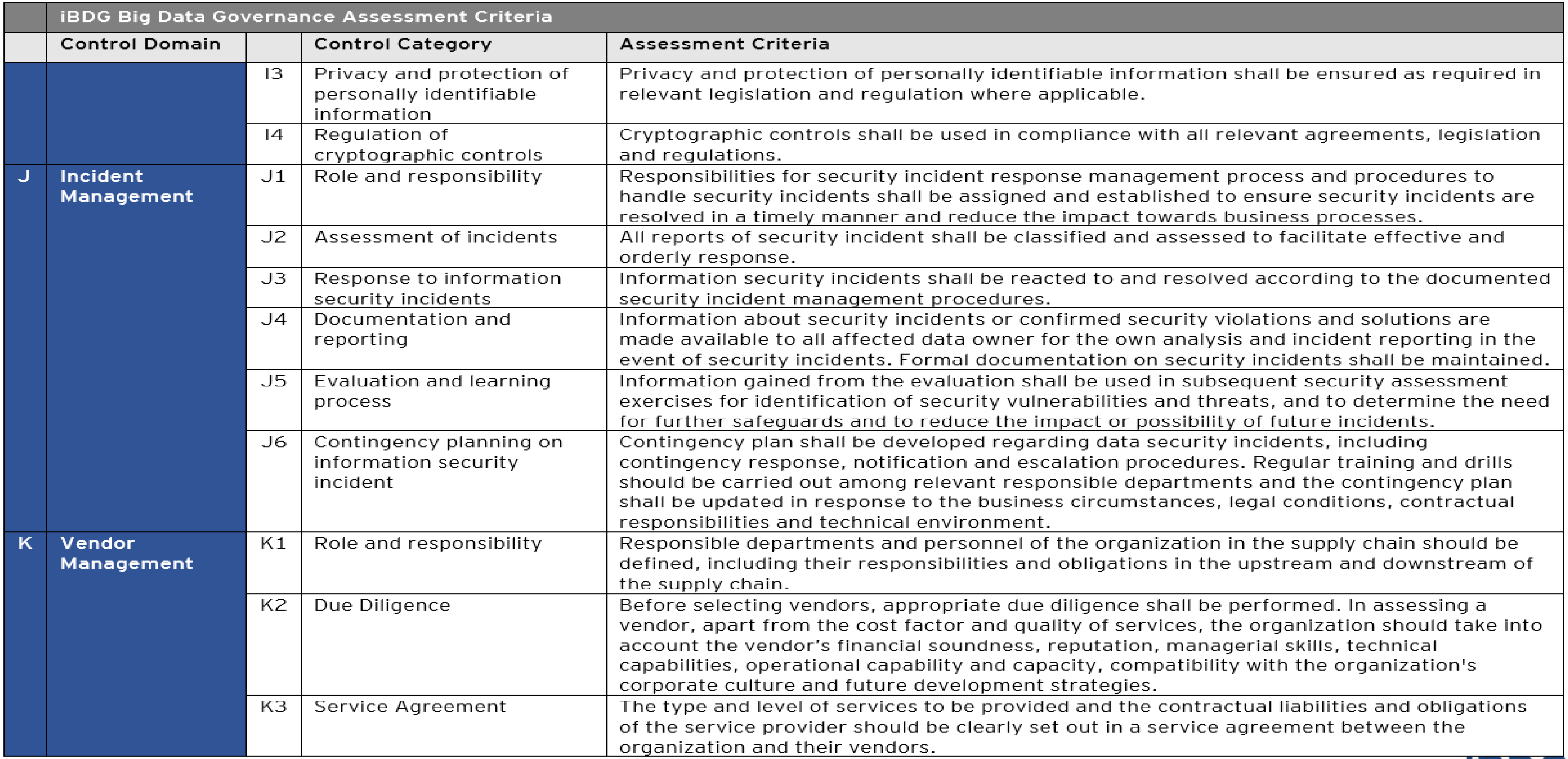
G. Policies & Procedures
H. Personnel Management
I. Compliance
J. Incident Management
K. Vendor Management
L. Business Continuity Management
M. Operation
N. Physical Security

iBDG Big Data Governance Assessment Criteria
– Control Environment Domains



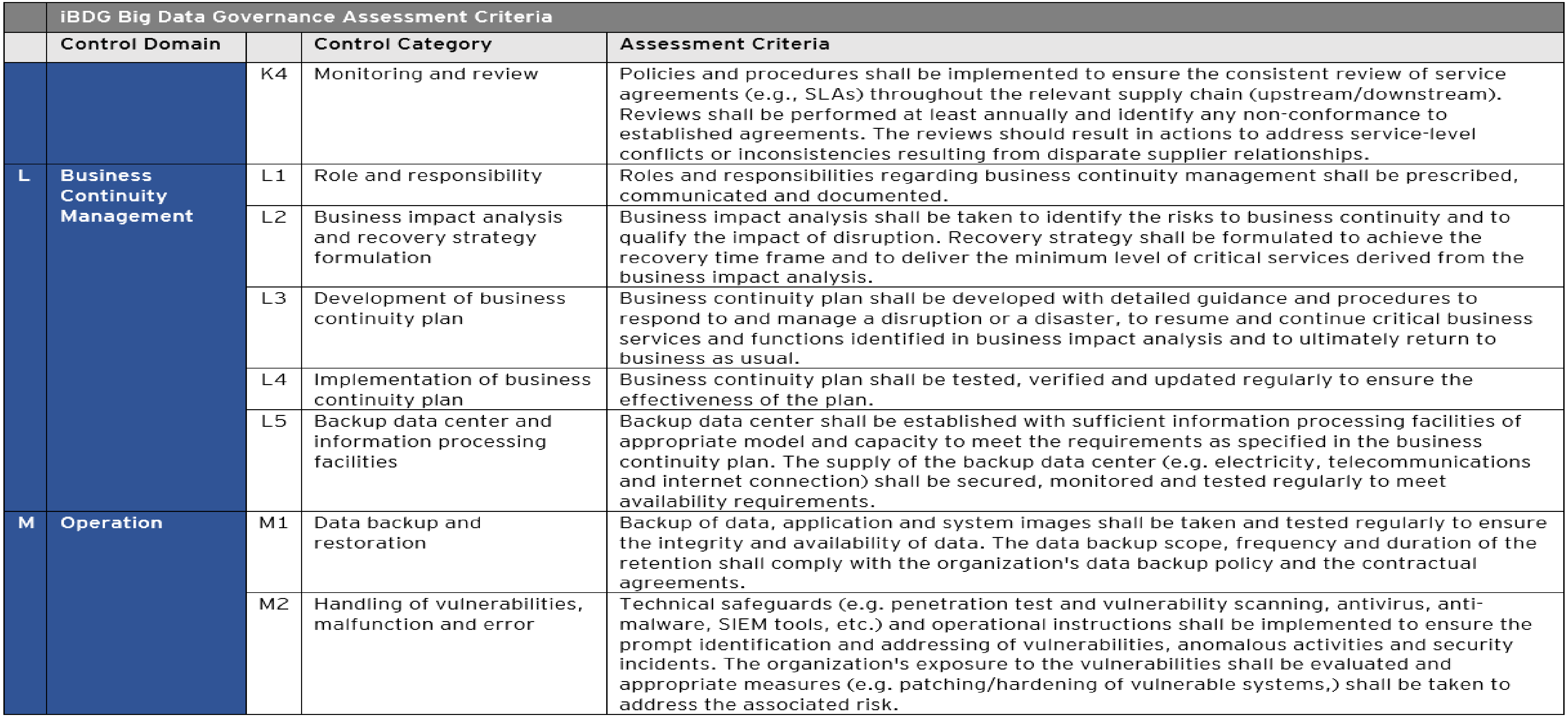
	iBDG Big Data Governance Assessment Criteria			
	Control Domain		Control Category	Assessment Criteria
G	Policies & Procedures	G1	Documentation and provision of policies and procedures	A set of policies and procedures of information security shall be defined, approved by management, published and communicated to employees and relevant external parties.
		G2	Review and approval of policies and procedures	The policies and procedures shall be reviewed regularly in response to the business circumstances, legal conditions, contractual responsibilities, technical environment to ensure their continuing suitability, adequacy and effectiveness.
H	Personnel Management	H1	Information security role and responsibility	Roles and responsibilities regarding information security shall be prescribed, designated and communicated.
		H2	Screening	Background checks on all employment candidates, contractors, and third parties shall be conducted according to laws and regulations and be proportional to the data classification to be accessed, identified risks and business requirements.
		H3	Security training and awareness education	A mandatory information security awareness program shall be established for all employees to ensure a basic level of understanding of information security matters is achieved. All individuals with specific obligations towards information security shall receive appropriate awareness training and consistent updates in business policies, procedures, roles and responsibilities and perceived risks shall be communicated regularly.
		H4	Disciplinary measures	Disciplinary measures in case of an information security breach shall be adopted against responsible personnel.
		H5	Termination of the employment or changes to the responsibility	Employees/contractors/service providers who has access to data shall be informed that the obligations to comply with relevant laws, regulations and provisions regarding information security remain valid even if the area of responsibility changes or the employment relationship is terminated. Non-disclosure commitment shall be made before termination of the employment.
I	Compliance	I1	Identification of applicable legal, contractual and data protection requirements	All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.
		I2	Intellectual property rights	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.

iBDG Big Data Governance Assessment Criteria
– Control Environment Domains



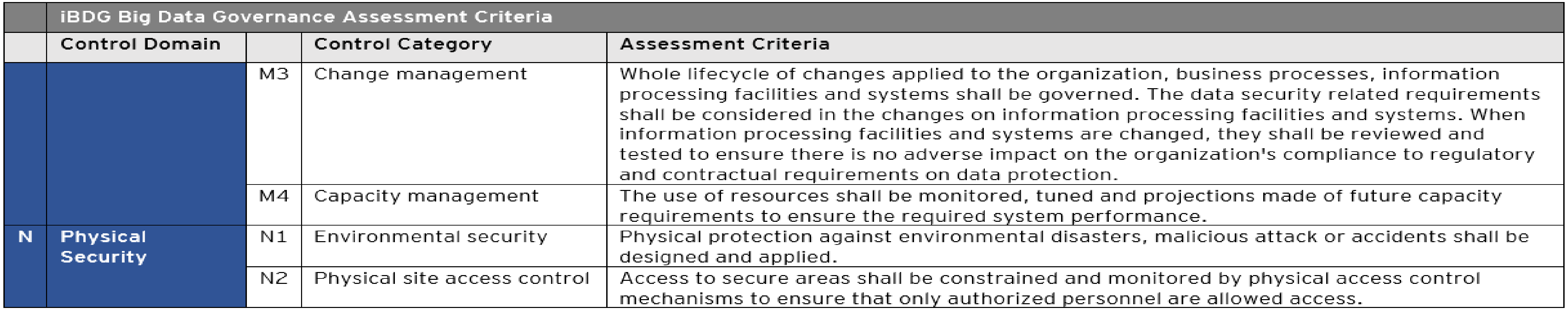
	iBDG Big Data Governance Assessment Criteria			
	Control Domain		Control Category	Assessment Criteria
		I3	Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.
		I4	Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.
J	Incident Management	J1	Role and responsibility	Responsibilities for security incident response management process and procedures to handle security incidents shall be assigned and established to ensure security incidents are resolved in a timely manner and reduce the impact towards business processes.
		J2	Assessment of incidents	All reports of security incident shall be classified and assessed to facilitate effective and orderly response.
		J3	Response to information security incidents	Information security incidents shall be reacted to and resolved according to the documented security incident management procedures.
		J4	Documentation and reporting	Information about security incidents or confirmed security violations and solutions are made available to all affected data owner for the own analysis and incident reporting in the event of security incidents. Formal documentation on security incidents shall be maintained.
		J5	Evaluation and learning process	Information gained from the evaluation shall be used in subsequent security assessment exercises for identification of security vulnerabilities and threats, and to determine the need for further safeguards and to reduce the impact or possibility of future incidents.
		J6	Contingency planning on information security incident	Contingency plan shall be developed regarding data security incidents, including contingency response, notification and escalation procedures. Regular training and drills should be carried out among relevant responsible departments and the contingency plan shall be updated in response to the business circumstances, legal conditions, contractual responsibilities and technical environment.
K	Vendor Management	K1	Role and responsibility	Responsible departments and personnel of the organization in the supply chain should be defined, including their responsibilities and obligations in the upstream and downstream of the supply chain.
		K2	Due Diligence	Before selecting vendors, appropriate due diligence shall be performed. In assessing a vendor, apart from the cost factor and quality of services, the organization should take into account the vendor's financial soundness, reputation, managerial skills, technical capabilities, operational capability and capacity, compatibility with the organization's corporate culture and future development strategies.
		K3	Service Agreement	The type and level of services to be provided and the contractual liabilities and obligations of the service provider should be clearly set out in a service agreement between the organization and their vendors.

iBDG Big Data Governance Assessment Criteria
– Control Environment Domains



	iBDG Big Data Governance Assessment Criteria			
	Control Domain		Control Category	Assessment Criteria
		K4	Monitoring and review	Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) throughout the relevant supply chain (upstream/downstream). Reviews shall be performed at least annually and identify any non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.
L	Business Continuity Management	L1	Role and responsibility	Roles and responsibilities regarding business continuity management shall be prescribed, communicated and documented.
		L2	Business impact analysis and recovery strategy formulation	Business impact analysis shall be taken to identify the risks to business continuity and to qualify the impact of disruption. Recovery strategy shall be formulated to achieve the recovery time frame and to deliver the minimum level of critical services derived from the business impact analysis.
		L3	Development of business continuity plan	Business continuity plan shall be developed with detailed guidance and procedures to respond to and manage a disruption or a disaster, to resume and continue critical business services and functions identified in business impact analysis and to ultimately return to business as usual.
		L4	Implementation of business continuity plan	Business continuity plan shall be tested, verified and updated regularly to ensure the effectiveness of the plan.
		L5	Backup data center and information processing facilities	Backup data center shall be established with sufficient information processing facilities of appropriate model and capacity to meet the requirements as specified in the business continuity plan. The supply of the backup data center (e.g. electricity, telecommunications and internet connection) shall be secured, monitored and tested regularly to meet availability requirements.
M	Operation	M1	Data backup and restoration	Backup of data, application and system images shall be taken and tested regularly to ensure the integrity and availability of data. The data backup scope, frequency and duration of the retention shall comply with the organization's data backup policy and the contractual agreements.
		M2	Handling of vulnerabilities, malfunction and error	Technical safeguards (e.g. penetration test and vulnerability scanning, antivirus, anti-malware, SIEM tools, etc.) and operational instructions shall be implemented to ensure the prompt identification and addressing of vulnerabilities, anomalous activities and security incidents. The organization's exposure to the vulnerabilities shall be evaluated and appropriate measures (e.g. patching/hardening of vulnerable systems,) shall be taken to address the associated risk.

iBDG Big Data Governance Assessment Criteria
– Control Environment Domains



	iBDG Big Data Governance Assessment Criteria			
	Control Domain		Control Category	Assessment Criteria
		M3	Change management	Whole lifecycle of changes applied to the organization, business processes, information processing facilities and systems shall be governed. The data security related requirements shall be considered in the changes on information processing facilities and systems. When information processing facilities and systems are changed, they shall be reviewed and tested to ensure there is no adverse impact on the organization's compliance to regulatory and contractual requirements on data protection.
		M4	Capacity management	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.
N	Physical Security	N1	Environmental security	Physical protection against environmental disasters, malicious attack or accidents shall be designed and applied.
		N2	Physical site access control	Access to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.