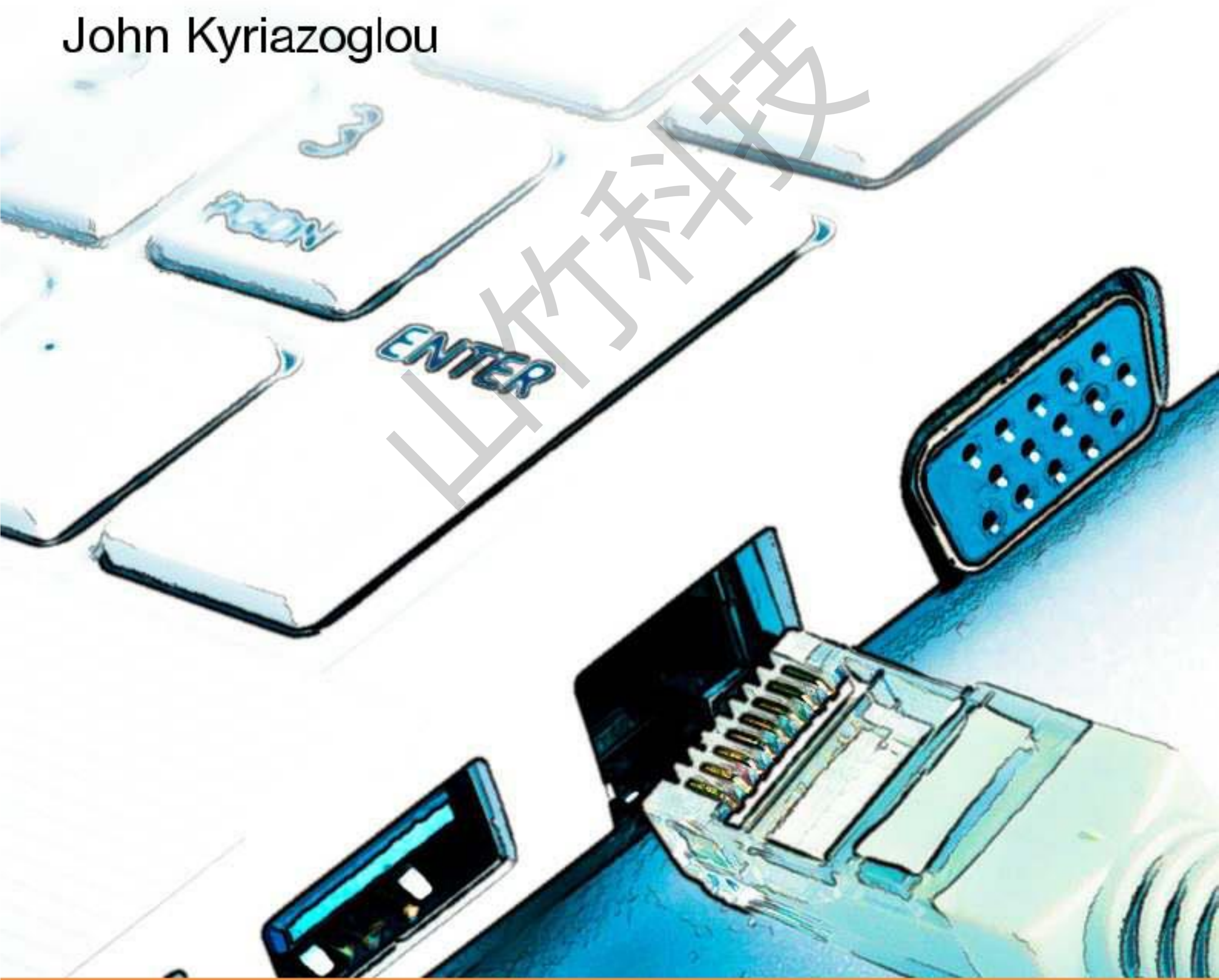
Data Protection and Privacy Management System

Data Protection and Privacy Guide – Vol I

John Kyriazoglou



bookboon.com
The eBook company

JOHN KYRIAZOGLOU

约翰·基里亚佐格卢

DATA PROTECTION AND PRIVACY MANAGEMENT SYSTEM

数据保护和隐私管理系统

DATA PROTECTION AND PRIVACY GUIDE – VOL I

资料保护及私隐指引-第一册

Data Protection and Privacy Management System:
资料保护及私隐管理系统:

Data Protection and Privacy Guide Ð Vol I
资料保护及私隐指引第一册

1st edition
第一版

ISBN 978-87-403-1540-0

2016 John Kyriazoglou & bookboon.com /
ISBN 978-87-403-1540-0

CONTENTS
内容

DEDICATIONS
献词

his book, and all the volumes that make it up, are dedicated to the glory of Ancient Greece, and to my blue-eyed, lovely grand-daughter, and princess of my life, Melina.
他的书和所有的书都献给了古希腊的荣耀，献给我的蓝眼睛，可爱的孙女，我生命中的公主，梅丽娜。

John Kyriazoglou
约翰·基里亚佐格鲁

PREFACE: DATA AND INFORMATION IN ENTERPRISES

前言:企业的数据和信息

Data and *information* are resources in both their physical and descriptive aspects, and two of the major resources of a given enterprise, apart from people and capital, least understood and controlled.
数据和信息是物理方面和描述方面的资源，也是特定企业的两大主要资源，除了人力和资本之外，人们对它们的了解和控制最少。

A small point will suffice: in most enterprises today, there are distinct functions to manage people (Human Resources Department) and capital (Finance and Accounting Department), but there is no distinct business unit or function to manage, protect, maintain and improve enterprise data and information (personal, financial, production, customer, etc.), whether manual or automated or both.
一个小问题可以证明:在今天的大多数企业中，有不同的职能来管理人员(人力资源部)和资本(财务和会计部)，但是没有不同的业务单位或职能来管理、保护、维护和改进企业的数据和信息(个人的、商业的、生产的、客户的等等)，无论是人工的还是自动的，或者两者都有。

Data is the plural of ‘datum’. It comes from Latin and means ‘given’ and this comes from Greek ‘dido’=to give (‘didomi’, ancient Greek).
数据是'datum'的复数形式。它来自拉丁语，意思是"给予"，这个词来自希腊语"dido"，意思是"给予"("didomi"，古希腊语)。

Data are typically the lowest level of abstraction of unprocessed (‘raw’) data, like characters, images, numbers and representations of physical quantities and facts, results of measurements, etc., from which information and knowledge are derived.
数据通常是未经处理("原始")数据的最低抽象层次，如字符、图像、数字、物理量和事实的表示、测量结果等，从中获得信息和知识。

In business terms these are processed by computerized systems, stored in paper filing and computerized systems as well as in computer-based devices and digital storage media, and transmitted to all authorized users, networks, computer programs, systems, stakeholders, etc., for further processing, decisions, actions, etc.
在商业方面，这些资料由计算机化系统处理，储存在纸张和计算机化系统以及基于计算机的设备和数字存储介质中，并传送给所有授权用户、网络、计算机程序、系统、利益相关者等，以供进一步处理、决定、行动等。

Information comes from Latin (‘in’ + ‘formare’) and denotes a concept, outline, or idea. Ultimately the term ‘formare’ comes from the ancient Greek term ‘morphe’=form (from the ancient Greek god Morpheus, the god of shapes).

信息来自拉丁语("in"+"formare")，表示一个概念、轮廓或想法。"formal"这个词最终来自古希腊术语"morphe"(形状之神，古希腊神)。

Information represents knowledge communicated to all interested parties. In business terms, knowledge puts shape and meaning to ‘raw’ data and it is the result of processing these data with a set of rules.
信息代表传达给所有相关方的知识。在商业术语中，知识给"原始"数据赋予形状和意义，它是用一组规则处理这些数据的结果。

Knowledge is familiarity or acquaintance with data, facts, information, principles, concepts, ideas, values, descriptions, skills, dexterities, etc., obtained through study, investigation, education, training, experience, and other methods.
知识是通过学习、调查、教育、培训、经验和其他方法所获得的对数据、事实、信息、原则、概念、想法、价值观、描述、技能、熟练程度等的熟悉或熟悉。

For the purposes of all types and forms of enterprises, business data and related information represent the ever-changing world in which private, not-for-profit and public organizations operate and survive.
就所有类型和形式的企业而言，商业数据和有关信息代表着不断变化的世界，在这个世界中，私营、非专业和公共组织在其中运作和生存。

People such as employees, customers, vendors and stakeholders, move, die and change, and therefore their data recorded in various digital resources and information systems and databases become obsolete and out of date.
员工、客户、供应商和利益相关者等人迁移、死亡和改变，因此他们在各种数字资源、信息系统和数据库中记录的数据变得过时和过时。

Vendors change their products and supplies. Standards change. Regulations change. Rules of doing business change. Market and economic forces require new types and different data which impact organizations.
供应商改变他们的产品和供应。标准改变了。规则改变了。做生意的规则改变了。市场和经济力量需要新的类型和不同的数据来影响组织。

And as information, according to Deming[1], the noted U.S. quality guru, is the second-most important resource to the organization, next to its people resources, it needs special and concentrated attention so that it remains relevant and valid, both at the data level from which information is derived as well as at the quality level which manifests its impacting and dynamic force.
根据美国著名质量大师 Deming1 的说法，信息是组织的第二重要资源，仅次于人力资源，它需要特别和集中的注意力，以保持相关性和有效性，无论是在产生信息的数据层面，还是在显示其影响力和动态力量的质量层面。

This special attention, quality and protection of your business data and information (personal, customer, financial, performance, etc.) can be effected by a process of standards and best practices and the effective use of relevant strategies, plans, policies and controls.
他对你的业务数据和信息(个人、客户、商业、业绩等)的特别关注、质量和保护，可以通过一个标准和最佳实践的过程，以及相关战略、计划、政策和控制的有效使用来反映。

These are contained in this book (with Main Title ‘**Data Protection and Privacy Guide’** and Sub-title ‘How to comply with privacy regulations more effectively’) and its five (5) parts (volumes):
本书(主标题为《资料保护及私隐指引》及副标题为《如何更有效地遵守私隐规例》)及其第(5)部分(卷):

- Volume 1: Data Protection and Privacy Management System (5 chapters);
  第一册:资料保护及私隐管理系统(五章);
- Volume 2: DP&P Policies, Plans, Checklists and Controls (6 chapters);
  第 2 卷:dp&p 策略，计划，检查表和控制(6 章);

- Volume 3: Data Protection Impact Assessment (3 chapters);
第三册:资料保护影响评估(三章);
- Volume 4: Data Protection Specialized Controls (2 chapters); and
第四册:资料保护专门控制(两章);及
- Volume 5: Security and Data Privacy Audit Questionnaires (3 chapters).
第五册:保安及资料私隐审计问卷(三章)。

he primary *AIM* of this book is to present several practical measures and controls (strategies, plans, policies, checklists, etc.) that may be used to protect better the privacy of all enterprise data and information with particular emphasis, however, on the personal data collected, processed, stored and distributed by an enterprise.
本书的主要目的是介绍几种可用于更好地保护所有企业数据和信息的隐私的实际措施和控制(策略、计划、政策、检查表等)，但特别强调企业收集、处理、储存和分发的个人数据。

his publication is intended to serve a diverse audience of senior and middle-level managers and professionals that are involved in all aspects of enterprise data governance, such as: Board members and CEOs, IT managers, Internal Audit managers and staff, Information Systems staff, Information Security officers, Compliance officers, and Data Protection and Privacy managers and staff, including:

他的出版物旨在为不同层次的高级和中级管理人员和专业人员服务，这些人员涉及企业数据治理的各个方面，例如:董事会成员和首席执行官、IT 经理、内部审计经理和管理人员、信息系统管理人员、信息安全管理人员、合规管理人员、数据保护和隐私管理人员和管理人员，包括:

1. Individuals with information system, security, and/or risk management and oversight responsibilities (e.g., authorizing officials, chief information officers, senior information security officers, information system managers, information security managers, etc.);

   具有资讯系统、保安及/或风险管理及监察职责的个人(例如，授权员工、首席资讯保安员、高级资讯保安员、资讯系统经理、资讯保安经理等);

2. Individuals with information system development responsibilities (e.g., IT managers, system designers and developers, information security engineers, systems integrators, etc.);

   负责资讯系统发展的人士(例如:资讯科技经理、系统设计师及开发人员、资讯保安工程师、系统集成商等);

3. Individuals with information security implementation and operational responsibilities (e.g., mission and business owners, information system owners, information owners and data stewards, system administrators, information system security officers, etc.);

   负责资讯保安实施及运作的人士(例如使命及业务拥有人、资讯系统拥有人、资讯拥有人及数据管理员、系统管理员、资讯系统保安员等);

4. Individuals with information security evaluation, assessment and monitoring responsibilities (e.g., auditors, data quality inspectors, information system evaluators, data quality assessors, independent system validators, business analysts, information system owners, etc.); and

   负责资讯保安评估、评估及监察工作的人士(例如:核数师、资料质素督察、资讯系统评估员、资料质素评估员、独立系统验证员、业务分析员、资讯系统拥有人等);以及

5. Commercial companies producing information technology products and systems, creating information security-related technologies, or providing information security services.

   生产信息技术产品和系统、开发信息安全相关技术或提供信息安全服务的商业公司。

SUMMARY
摘要

This volume describes the main components of a **Generalized Integrated Data Protection and Privacy Management System (DP&P System)** that may be used to manage and protect better the privacy of the personal data enterprises collect, process, store and use and to mitigate more effectively the identified data protection and privacy risks related to such personal data.
他的第卷描述了一个广义综合数据保护及私隐管理系统(dp&pSystem)的主要组成部分，该系统可用来更好地管理和保护企业收集、处理、储存和使用的个人资料的私隐，并更有效地减轻与这些个人资料有关的识别性数据保护和私隐风险。

The contents of this volume are listed below.
这本书的内容如下。

Volume 1 Contents
第一册目录

Chapter 1: Why is data protection needed?
第一章:为何需要资料保护？

This chapter describes the basic terms and reasons for data protection for enterprises.
他的章节描述了企业数据保护的基本术语和原因。

Chapter 2: Data Protection and Privacy Management System
第二章:资料保护及私隐管理系统

This chapter describes the **DP&P System** which includes: a methodology of five phases with specific steps and actions in each phase; a strategy; a set of policies and procedures; and various technical and other tools (e.g. software, checklists, quizzes, questionnaires, etc.) that may be considered, customized and used for the main purposes of providing better protection of the privacy of personal data.
他的章节描述了 dp&p 系统，其中包括:一个由五个阶段组成的方法，每个阶段都有具体的步骤和行动;一个策略;一套政策和程序;以及各种技术和其他工具(例如软件、清单、测验、问卷等)，这些工具可以被考虑、定制和使用，主要目的是为了更好地保护个人资料的私隐。

Chapter 3: Data Protection Quiz
第三章:保障资料问答游戏

This chapter contains 166 review questions and answers for a set of data protection-related issues related to: ICT Organization controls; ICT Administration Controls; IT Personnel Controls; ICT Strategic Controls; System Development Controls; ICT Security Controls; Data Center Operational Controls; IT Contingency Planning and Disaster Recovery Controls; Systems Software Controls; Computerized Application Controls; Business Data Management Controls; and

本章载有 166 个与数据保护有关的问题的审查问题和答案，这些问题涉及:信息和通信技术组织控制;信息和通信技术行政控制;信息和通信技术人事控制;信息和通信技术战略控制;系统开发控制;信息和通信技术安全控制;数据中心业务控制;信息和通信技术应急规划和灾后恢复控制;系统软件控制;计算机化应用控制;业务数据管理控制;以及

Chapter 4: Summary of the New EU General Data Protection Regulation
第四章:新欧盟一般资料保护规例概述

his chapter contains a summary of the new EU GDPR.
他的章节包含了对新欧盟反歧视政策的总结。

Chapter 5: Personal Data Checklist
第五章:个人资料核对表

his chapter identiies some common types of personal data that are linked to individuals and which (data) may be collected, processed, maintained, shared or used by enterprises in the current socio-economic, business and digital environment.
他的章节列出一些与个人有关连的常见个人资料，这些资料可供企业在现时的社会经济、商业及数码环境中收集、处理、保存、分享或使用。

Appendix 1: Components of a Data Protection and Privacy Program
附录 1:资料保护及私隐计划的组成部分

Other Related Material
其他相关资料

his volume is supplemented and supported by:
他的著作得到了以下方面的补充和支持:

- **Volume 2: DP&P Strategies, Plans and Policies**
第 2 卷:dp&p 策略、计划和政策
- Volume 3: Data Protection Impact Assessment;
第三册:数据保护影响评估;
- Volume 4: Data Protection Specialized Controls; and
第 4 卷:数据保护专门控制;以及
- Volume 5: Security and Data Privacy Audit Questionnaires.
第五册:保安及资料私隐审计问卷。

1 WHY IS DATA PROTECTION NEEDED?

为什么需要数据保护？

Summary

摘要

This chapter introduces data protection and describes the basic terms and reasons for protecting the privacy of personal data collected, processed, stored and transmitted by enterprises.
本章介绍资料保护，并阐述保护企业所收集、处理、储存及传送的个人资料私隐的基本条款及理由。

1.1 INTRODUCTION

1.1 引言

Every time you buy a product online, use a service, register for email, go to your doctor, pay your taxes and bills, or enter into any contract or service request, you have to hand over some of your personal information.
每当你在网上购买产品、使用服务、登记电子邮件、去看医生、支付税款和账单、或签订任何合同或服务要求时，你都必须交出一些个人信息。

Even without your explicit knowledge, information about you is being generated and captured by enterprises, companies, organizations of all types, and government agencies you are likely to have never knowingly interacted with.
即使没有你的外显知识，你的信息也正在被企业、公司、各种组织和政府机构产生和捕获，而你可能从未有意识地与之互动过。

The only way customers, citizens and consumers can have trust and confidence in both government and business is through strong data protection practices, with effective legislation to help minimise needless monitoring by state authorities and regulate surveillance by companies.
要让消费者、公民和消费者在政府和企业中获得信任和认同，唯一的办法就是采取强有力的数据保护措施，通过有效的立法，帮助减少国家当局不必要的监控，并规范企业的监控行为。

Since the 1960s and the expansion of information technology and communications capabilities, business and government organisations have been storing this personal information in computerized databases.
自 1960 年代以来，随着信息技术和通信能力的扩展，企业和政府机构一直将这些个人信息存储在计算机数据库中。

These databases can be quickly searched, edited, cross-referenced, summarized, profiles, etc., and data shared with other organisations and across the world. Once the management, collection and processing of data became widespread, people started asking several questions about what was happening to their information once it was turned over.

这些数据库可以被快速搜索、编辑、交叉引用、总结、汇编等，并且可以与其他组织和世界各地共享数据。一旦数据的管理、收集和处理变得普遍起来，人们就开始问一些问题，关于他们的信息一旦被移交后会发生什么。

Question 1: Who had the right to access the information and personal data?
问题 1:谁有权查阅资料及个人资料？

Question 2: Were personal data kept accurately?
问题 2:个人资料是否保存准确？

Question 3: Were they collected and disseminated without the knowledge and consent of the individuals concerned?
问题 3:是否在有关个人不知情和不同意的情况下收集和传播这些材料？

Question 4: Could personal data be used to discriminate or abuse other fundamental rights?
问题 4:个人资料是否可被用来歧视或滥用其他基本权利？

From all these, and the growing public concern, data protection principles were devised through numerous national and international consultations, standards and regulations.
从所有这些以及公众日益关注的情况出发，通过大量的国家和国际协商、标准和规章制定了数据保护原则。

1.2 WHAT IS DATA PROTECTION?

1.2 什么是资料保护？

Individuals, as consumers, citizens, customers, employees, etc., need to have the means to exercise their right to privacy and protect themselves and their personal information from abuse of any kind.
个人，作为消费者、公民、顾客、雇员等，需要有办法行使其隐私权，保护自己和个人信息不受任何形式的滥用。

Data protection is about safeguarding and protecting your fundamental right to privacy, which is enshrined in international and national laws, codes and conventions.
数据保护是保障和保护你的基本隐私权，这是国际和国家法律、法规和公约所规定的。

Data protection is commonly defined as the law designed to protect your personal data, which is collected, managed, processed and stored by computerized or ‘automated’ means or intended to be part of a manual filing system.
保障资料通常被视为保障你的个人资料的法例，而该等资料是以电脑化或「自动化」方式收集、管理、处理及储存，或拟作为人工申报系统的一部分。

In modern 21st century societies and economies, to empower you to control your information and to protect you from abuses, it is essential that data protection laws restrain and shape the activities of enterprises, organizations, companies and governments. All these institutions have shown repeatedly that unless rules and laws restrict their actions, they will possibly endeavour to collect personal data, manage them, keep them, etc., while telling us nothing at all, in many, many cases.
在 21 世纪的现代社会和经济中，为了让你有能力控制你的信息，保护你免受滥用，数据保护法律必须约束和塑造企业、组织、公司和政府的活动。所有这些机构一再表明，除非规则和法律限制他们的行动，他们可能会努力收集个人数据，管理它们，保存它们，等等，而在许多情况下，什么也不告诉我们。

1.3 DATA PROTECTION BASIC TERMS

1.3 数据保护基本术语

Some of the basic terms of data protection for your consideration are presented next.
下面将介绍一些供您考虑的数据保护的基本术语。

These terms are:
这些术语是:

1) **‘Personal Data’:** ‘Personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic,

cultural or social identity of that natural person (see example in 'Chapter 5: Personal Data Checklist');

"个人资料":"个人资料"是指任何与可识别的或可识别的自然人('数据主体')有关的信息;可识别的自然人是指能够直接或间接地被识别的人，特别是通过姓名、识别号码、位置数据、在线识别人或与该自然人的身体、生理、遗传、精神、经济、文化或社会身份有关的一个或多个因素(见'第五章:个人资料清单'中的例子);

2) **'Processing':** 'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

「处理」:「处理」指对个人资料或成套个人资料进行的任何操作或一系列操作，不论是否以自动方式进行，例如收集、记录、组织、编排、储存、改编或更改、检索、咨询、使用、透过传送、发布或以其他方式提供、排列或组合、限制、擦除或销毁;

3) **‘Controller’:** ‘Controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

"财务主任":"财务主任"是指自然人或法人、公共当局、机构或其他机构，它们单独或共同决定处理个人数据的目的和手段;如果处理个人数据的目的和手段由联盟或成员国法律决定，则联盟或成员国法律可规定财务主任或提名个人数据的具体标准;

4) **‘Processor’:** ‘Processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

"处理器":"处理器"指代表控制器处理个人数据的自然人或法人、公共机关、机构或其他机构;

5) **‘Third Party’:** ‘Third Party’ means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

「税务缔约方」:「税务缔约方」指资料当事人、控制人、处理人以外的自然人或法人、公共机关、代理机构或团体，以及在控制人或处理人直接授权下获授权处理个人资料的人士;

6) **‘Consent’:** ‘Consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

"同意":资料当事人的"同意"是指资料当事人自由给予、具体、知情和明确表示的意愿，表示同意处理与他或她有关的个人资料;

7) **‘Personal Data Breach’:** ‘Personal Data Breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed; and

「个人资料外泄」:「个人资料外泄」指违反保安规定，导致传送、储存或以其他方式处理的个人资料遭意外或非法毁坏、遗失、更改、未经授权披露或查阅;以及

Thank you!

谢谢！

8) **‘Enterprise’:** ‘Enterprise’ means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;
"企业":"企业"是指从事经济活动的自然人或法人，不论其法律形式如何，包括经常从事经济活动的合伙企业或协会;

More terms are included in Article 4 of the EU General Data Protection Regulation.
更多的条款包括在欧盟一般数据保护条例第 4 条。

For more on EU Data Protection Directive, see:
有关欧盟数据保护指令的更多信息，请参见:

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1462359521758&from=EN.
Http://eur-lex.europa.eu/legal-content/EN/txt/pdf/?uri=celex:32016r0679&qid=1462359521758& 来自 EN。

1.4 HOW DATA PROTECTION WORKS
1.4 资料保护如何运作

Where a comprehensive data protection law exists, organisations, public or private, that collect and use your personal information have the obligation to handle this data according to the data protection law.
如果存在全面的数据保护法，收集和使用您的个人信息的公共或私人机构有义务根据数据保护法处理这些数据。

This law is based on a number of general principles that require that:
他的法律基于若干一般原则，这些原则要求:

1. There should be limits to what personal data are collected;
此处应对收集个人资料作出限制;
2. Personal information should be obtained by lawful and fair means, with the consent of the individual (data subject);
个人资料应在个人(资料当事人)同意下，以合法及公平的方式取得;
3. The personal information should be correct, relevant to the purposes for which it is used, accurate, complete and up to date, etc.
个人资料必须正确、与使用目的相关、准确、完整和最新等。

More details about how data protection works in a business environment are included in this book and its various parts.
关于数据保护在业务环境中如何工作的更多细节包括在本书及其各个部分中。

1.5 THE IMPORTANCE OF DATA PROTECTION TO ENTERPRISES
1.5 保护资料对企业的重要性

There are five main reasons for allocating resources, spending money, time, and effort and taking preventive measures and implementing controls to protect enterprise data: Regulatory

compliance; Financial and other losses; Around the clock operation; Employee productivity; and Management decision-making.
以下是分配资源、花费金钱、时间和精力以及采取预防措施和实施控制以保护企业数据的主要原因:守规、财务和其他损失、全天候运营、员工生产力和管理决策。

1.6 REGULATORY COMPLIANCE

1.6 守规
he irst most important reason to implement data protection strategies is fear of ines due to non-compliance. his is because governments throughout the world[2] are implementing new privacy regulations on electronic communications and stored data of all types.
实施数据保护策略的第一个重要原因是由于不遵守引起的对 ines 的恐惧。这是因为世界各地的政府正在对电子通信和各种类型的存储数据实施新的隐私条例。

As of now (August 2016), over 100 countries around the world have enacted comprehensive data protection legislation, and several other countries are in the process of passing such laws[3, 4].
截至目前(2016 年 8 月)，世界上已有 100 多个国家颁布了全面的数据保护立法，还有几个国家正在通过此类立法 3、4。

The strongest and most comprehensive laws are in the countries of the European Union and European Economic Area that have implemented the 1995 Data Protection Directive. This is currently changing into the **General Data Protection Regulation (GDPR)** (Regulation (EU) 2016/679) by which the European Commission intends to strengthen and unify data protection for individuals within the European Union (EU).
欧盟和欧洲经济区的国家实施了1995年的数据保护指令，这些国家的法律是最有力和最全面的。欧洲委员会现正修订《一般数据保护规例》(《规例》(欧盟)2016/679)，以加强和统一对欧洲联盟(欧盟)内个人的数据保护。

The GDPR will replace the official Directive 95/46/EC from 1995 and will go into force on 25 May 2018 after a two-year transition period and, unlike a directive it does not require any enabling legislation to be passed by governments. The new law will replace a patchwork of 28 different sets of national privacy laws by creating a single set of rules for the protection of data within the EU.
该公约将从1995年起取代第95/46/ec号官方指令，经过两年的过渡期后，将于2018年5月25日生效，而且与指令不同的是，该指令不要求政府通过任何授权立法。新法律将通过创建一套单一的欧盟内部数据保护规则，取代拼凑而成的28套不同的国家隐私法。

Enterprises therefore face huge consequences and fines for noncompliance. Some countries hold company executives criminally liable for failure to comply with laws regarding electronic communications and documents. These privacy regulations often define what information must be retained, for how long, and under what conditions and circumstances. Other laws are designed to ensure the privacy of the information contained in documents, files, and databases. Loss of critical electronic communications can be construed as a violation of these regulations and may subject the enterprise to large fines and the managers to legal action.
因此，企业面临着巨大的后果和不遵守的原因。一些国家要求公司高管对未遵守有关电子通信和文件的法律承担刑事责任。这些隐私条例通常规定哪些信息必须保留，保留多长时间，以及在什么条件和情况下保留。其他法律旨在确保文件、文件和数据库中所包含信息的隐私。关键电子通信的丢失可被解释为违反了这些条例，并可能使企业受到大型公司和管理人员的法律诉讼。

1.7 FINANCIAL AND OTHER LOSSES
1.7 财务及其他损失

The second most important reason to implement data protection strategies is fear of financial and other losses. This is because enterprise data are recognized as an important corporate asset that needs to be safeguarded and protected against insider and external threats.
实施数据保护策略的第二个重要原因是害怕财务和其他损失。这是因为企业数据被认为是重要的企业资产，需要得到保护和保护，以免受到内部和外部威胁。

In the past, senior executives and boards of directors may have been complacent about the risks posed by data breaches, data errors, data quality issues, and cyber attacks executed by all types of attackers (insider, external) and ineffective staff.

过去，高级管理人员和董事会可能对数据泄露、数据错误、数据质量问题、各类攻击者(内部人员、外部人员)实施的网络攻击和无效防御所带来的风险感到自满。

However, there is a growing concern about the potential damage to reputation, class action lawsuits and costly downtime that is motivating executives to pay greater attention to the security practices of their organizations.
然而，人们越来越担心对声誉的潜在损害，集体诉讼和昂贵的停机时间，这促使管理人员更加关注他们组织的安全实践。

In their 2014 global data breach study[5] IBM and Ponemon Institute reported that the average cost for each lost or stolen record containing sensitive and conidential enterprise information increased from U.S. $188 to U.S. $201 and the total average cost paid by organizations increased from U.S. $5.4 million to U.S. $5.9 million.
在 2014 年的全球数据泄露研究中，IBM 和波耐蒙研究所报告称，包含敏感和同类企业信息的每条丢失或被盗记录的平均成本从 188 美元增加到 201 美元，各组织支付的总平均成本从 540 万美元增加到 590 万美元。

Loss or alteration of enterprise information and personal data can also lead to direct financial losses, such as lost sales, fines, or bad monetary judgments as well as other incorrect board, senior executive or management decisions.
企业信息和个人数据的丢失或变更也可能导致直接的财务损失，如销售损失、信用卡损失、错误的货币判断以及其他不正确的董事会、高级管理人员或管理层决定。

In addition to these, loss or alteration of enterprise information and personal data can cause indirect losses from the effects of a drop in investor confidence or customers fleeing to competitors, or financial effects or other consequential damages that are not known to the specific enterprise or organization until much later.
此外，企业信息和个人数据的丢失或变更可能造成间接损失，包括投资者认同度下降、客户向竞争对手投降、财务损失或其他直到很久以后才为特定企业或组织所知的间接损失。

1.8 AROUND THE CLOCK OPERATION

1.8 全天候运作

The third most important reason to implement data protection strategies is the fear of not responding adequately to the requirements for enterprise operations around the clock.
实施数据保护策略的第三个重要原因是担心不能充分响应企业 24 小时运营的需求。

This is because in an increasingly interdependent global economy, downtime is not accepted or tolerated by consumers and customers, who can readily and quickly take their business elsewhere. They expect and demand that the particular enterprise operates effectively and efficiently at all times (24 hours a day, seven days a week).
他的理由是，在一个日益相互依赖的全球经济中，停工期既不为消费者所接受，也不为消费者所容忍，他们可以随时迅速地将业务转移到其他地方。他们希望并要求特定的企业在任何时候(每天 24 小时，每周 7 天)都能够有效而安全地运作。

The inability of an enterprise to operate because of a data loss or operational malfunction caused by an attack, even a temporary one, is driving many businesses to deploy extensive data protection strategies and implement various measures and controls.
由于一次攻击(即使是暂时的攻击)导致数据丢失或操作故障，使企业无法正常运行，从而迫使许多企业部署广泛的数据保护策略，并实施各种措施和控制。

It is not only the e-commerce enterprises that experience this situation. All types of businesses (including wellness, health care, financial, manufacturing, and service, etc.) operate around the clock or at least their computer systems and IT operations do.
不仅仅是电子商务企业遇到了这种情况。所有类型的企业(包括健康、医疗保健、商业、制造和服务等等)都是昼夜不停地运转，或者至少他们的计算机系统和 IT 操作是这样的。

Even when no enterprise staff are present, computers and computerized application systems are instructed accordingly and available to take, execute and place orders, send orders to the

warehouse, run marketing campaigns, promote sales, record business transactions, manage inancial and other transactions and generally complete all types of business transactions.
即使没有企业存在，计算机和计算机化应用系统也会得到相应的指示，可以接受、执行和下订单、向仓库发送订单、开展营销活动、促进销售、记录商业交易、管理金融交易和其他交易以及一般完成所有类型的商业交易。

Enterprises, therefore, need to take all these 24/7 operational demands and requirements into account for designing and implementing better protection for their enterprise data.
因此，企业需要考虑到所有这些 24/7 的操作需求和需求，以便为其企业数据设计和实现更好的保护。

1.9 EMPLOYEE PRODUCTIVITY

1.9 员工生产力

he fourth most important reason to implement data protection strategies is fear of lower employee productivity. his is because loss and errors of important enterprise data lessens overall productivity, as employees have to deal with time-consuming operational issues (customer support, sales, accounting, production, inventory, procurement, etc.) without the aid and support of IT application systems and computer databases.
实施数据保护策略的第四个重要原因是担心员工生产率下降。这是因为企业重要数据的丢失和错误降低了整体生产力，因为员工不得不在没有 IT 应用系统和计算机数据库的帮助和支持下，处理耗时的业务问题(客户支持、销售、会计、生产、库存、采购等)。

Data losses and errors also result in IT application failures and similar system problems, making it diicult for people to do their jobs at any level of efectiveness.
数据丢失和错误还会导致 IT 应用程序故障和类似的系统问题，使人们难以在任何级别上有效地完成自己的工作。

A poor data protection strategy may leave customers waiting for long periods of time for systems to be restored after a failure. During that time, employees may be idle or able to work only in a reduced capacity, further diminishing overall productivity and increasing employee frustration.
一个糟糕的数据保护策略可能会让客户在系统故障后等待很长时间才能恢复。在此期间，员工可能处于闲置状态，或者只能在生产能力下降的情况下工作，从而进一步降低整体生产力，增加员工的挫折感。

1.10 MANAGEMENT DECISION-MAKING

1.10 管理决策

he ifth most important reason to implement data protection strategies is fear of incorrect management decision-making. his is because incorrect data, processing logic errors and data quality aspects of data lead to incorrect management decision-making at all levels of managing the enterprise operations, functions, systems and transactions[6].
实施数据保护策略的最重要原因是害怕错误的管理决策。这是因为不正确的数据、处理逻辑错误和数据质量方面的数据导致在企业运营、功能、系统和事务管理的各个层次上作出不正确的管理决策。

he Data Warehouse Institute (https://tdwi.org/Home.aspx) has estimated that more than U.S.
美国数据仓库研究所(DataWarehouseInstitute)估计，美国的 https://tdwi.org/home.aspx 超过 100 亿美元。
$600 billion are lost annually due to data quality issues.
由于数据质量问题，每年损失 6000 亿美元。

Data quality is one discipline that is important for all companies to get right, yet few currently are. According to Experian's Data Quality Global Report for 2016[7], 92 per cent of

respondents worried that their data was incorrect on some level, up from 86 per cent the previous year.
数据质量是所有公司都必须正确处理的一个重要原则，但目前很少有公司能做到这一点。根据益百利(Experian)的《2016 年全球数据质量报告》(DataQualityGlobalReportfor20167)，92%的受访者担心自己的数据在某种程度上有误，高于前一年的 86%。

To improve data quality and lessen decision-making errors, it’s important for enterprises to look at how data is treated across the whole business. his includes making sure that data is being collected, processed and stored correctly and that the right information is being entered in the irst place, etc.
为了提高数据质量和减少决策错误，企业必须了解如何在整个业务中处理数据。他的工作包括确保数据被正确地收集、处理和存储，以及正确的信息被输入到正确的地方等等。

Enterprise managers must not only protect personal and other company data against privacy and security aspects (losses, errors, damage, fraud, communicating data to criminals, etc.) but also ensure that the quality of all data (personal, inancial, production, performance, etc.) is maintained and improved in the process of running enterprise operations.
企业管理者不仅必须保护个人和其他公司数据的隐私和安全方面(损失、错误、损坏、欺诈、向犯罪分子通报数据等)，而且还必须确保所有数据的质量(个人、财务、生产、绩效等)在企业运营过程中得到维护和改进。

1.11 HOW TO IMPROVE THE PROTECTION OF YOUR ENTERPRISE DATA
1.11 如何加强企业数据的保护

The increasing use of information and communications technologies along with the internet ensure that laws and regulations related to data protection, data security and data privacy remain most important and relevant to all enterprises and which all business entities and organizations across the globe are required to comply with.
信息和通信技术以及互联网的使用日益增加，确保与数据保护、数据安全和数据隐私有关的法律法规对所有企业来说仍然是最重要和最相关的，全球所有商业实体和组织都必须遵守这些法律法规。

Your specific enterprise must look now at how it collects, manages, stores and uses personal data and how best to comply with the relevant data protection and privacy laws and regulations.
您的专业企业现在必须考虑如何收集、管理、存储和使用个人数据，以及如何最好地遵守相关的数据保护和隐私法律法规。

In order to help, support, and enable all enterprises managers in implementing the most effective controls to resolve the issues of data protection of personal data, a difficult and complex task, I have written this book with the: **Main Title 'Data Protection and Privacy Guide'** and Sub-title 'How to comply with privacy regulations more effectively'.
为了帮助、支持和帮助所有企业管理者实施最有效的控制，解决个人数据的数据保护问题，这是一个棘手而复杂的任务，我写了这本书，主标题为"数据保护和隐私指南"，副标题为"如何更有效地遵守隐私法规"。

The contents of this book, in summary, are:
总而言之，这本书的内容是:

- Volume 1: Data Protection and Privacy Management System (5 chapters);
第一册:资料保护及私隐管理系统(五章);
- Volume 2: DP&P Policies, Plans, Checklists and Controls (6 chapters);
第 2 卷:dp&p 策略，计划，检查表和控制(6 章);
- Volume 3: Data Protection Impact Assessment (3 chapters);
第三册:资料保护影响评估(三章);
- Volume 4: Data Protection Specialized Controls (2 chapters); and
第四册:资料保护专门控制(两章);及
- Volume 5: Security and Data Privacy Audit Questionnaires (3 chapters).
第五册:保安及资料私隐审计问卷(三章)。

These are detailed in the following volumes and chapters of this book.
这些在这本书的后续章节中都有详细说明。

2 DATA PROTECTION AND PRIVACY MANAGEMENT SYSTEM

数据保护和隐私管理系统

Summary
摘要

his chapter describes the proposed **Integrated Data Protection and Privacy Management System (DP&P System)** and its parts**:** methodology; phases and steps; strategy; actions; and policies, procedures and various technical and other tools (e.g. software, checklists, quizzes, questionnaires, etc.).
他的章节介绍建议的综合数据保护及私隐管理系统(dp&pSystem)及其部分:方法、阶段及步骤、策略、行动、政策、程序，以及各种技术及其他工具(例如软件、清单、测验、问卷等)。

he objective of this system is to manage better the enterprise data and to mitigate the usual data protection and privacy risks of collecting and processing personal data.
该系统的目的是更好地管理企业数据，减少收集和处理个人数据时常见的数据保护和隐私风险。

2.1 INTRODUCTION

2.1 引言

Most private companies, non-proit organizations, business entities established for various purposes, large conglomerates, pubic organizations, small and medium-size companies, retail stores, etc., collectively termed ‘enterprises’ in this book, are not be fully aware of the data protection and privacy as well as other cyber risks facing their data and information systems. hese risks are caused by malicious attackers: insiders and external entities or people.
本书中统称为「企业」的大部分私营公司、非营利组织、为各种目的而设立的商业实体、大型企业集团、公众组织、中小型公司、零售商店等，都没有充分认识到其数据和信息系统所面临的数据保护、隐私和其他网络风险。这些风险是由恶意攻击者引起的:内部人员和外部实体或个人。

Both of these types of attackers alike love to steal the enterprise’s sensitive information and data such as customer records, employee health records, research data, intellectual property, inancial records, and personal information, etc., because these data have a very high value.
这两种类型的攻击者都喜欢窃取企业的敏感信息和数据，如客户记录、员工健康记录、研究数据、知识产权、商业记录和个人信息等，因为这些数据具有非常高的价值。

In addition to this, enterprise data are also at risk due to careless and negligent employees and other trusted users with elevated levels of access such as partners and consultants.
除此之外，企业数据也面临风险，因为粗心和疏忽的雇员和其他访问级别较高的受信任用户，如合作伙伴和顾问。

Also all enterprise face the risks of very high ines if they do not comply with the various data protection and privacy regulations across the world..
此外，如果不遵守世界各地的各种数据保护和隐私规定，所有企业都面临着非常高的风险。.

All these make it paramount for the enterprise to design, develop and implement its own **Integrated Data Protection and Privacy Management System (DP&P System)** to manage better its data and to mitigate the above-mentioned risks.
所有这些都使企业设计、开发和实施自己的综合数据保护和隐私管理系统(dp&pSystem)以更好地管理数据并减轻上述风险变得至关重要。

his **DP&P System** will include a methodology**,** a strategy and a set of policies, procedures and various technical and other tools (e.g. software, checklists, quizzes, questionnaires, etc.), as presented in this book and its various parts (Volume 1 to xxx).
他的 dp&p 系统将包括一个方法论，一个策略和一套政策，程序和各种技术和其他工具(如软件，清单，测验，问卷等)，正如本书及其各个部分(第一卷至第三十卷)所介绍的。

2.2 DP&P SYSTEM PHASES
2.2dp&p 系统阶段

he above-prosed **DP&P System** consists of the following 5 phases:
发展伙伴关系及计划系统由以下五个阶段组成:

- Phase 1: Data Protection and Privacy Preparation
第一阶段:资料保护及私隐准备
- Phase 2: Data Protection and Privacy Organization
第二阶段:资料保护及私隐组织
- Phase 3: Data Protection and Privacy Development and Implementation
第三阶段:资料保护及私隐发展及推行
- Phase 4: Data Protection and Privacy Governance
第四阶段:资料保护及私隐管治
- Phase 5: Data Protection and Privacy Evaluation and Improvement
第五阶段:资料保护及私隐评估及改善

Each phase contains several steps and each step one or more actions.
每个阶段包含几个步骤，每个步骤包含一个或多个操作。

hese are presented next.
接下来是他们的表演。

2.2.1 PHASE 1: DATA PROTECTION AND PRIVACY PREPARATION
2.2.1 第一阶段:资料保护及私隐准备

Goal and Objectives
目标及宗旨

he general goal of this phase (**Phase 1-DP&P Preparation**) is to prepare your company or organization for privacy.
这个阶段(阶段 1-DP&p 准备)的总体目标是为您的公司或组织的隐私做好准备。

he more speciic objectives of this phase are: to analyze the data protection and privacy requirements and needs impacting your company; to collect the relevant laws, standards and regulations related to data protection and privacy; and to establish an action plan with the requisite resources so that you prepare your company to manage its personal data, activities, transactions and operations better taking into full consideration the data protection and privacy rules and regulations in existence.
这个阶段更具体的目标是:分析数据保护和隐私要求以及影响公司的需要;收集有关数据保护和隐私的相关法律、标准和规章;以及制定一个具备必要资源的行动计划，以便在充分考虑到现行的数据保护和隐私规则和规章的情况下，为公司管理其个人数据、活动、交易和业务做好准备。

he steps and actions required to be executed to complete this phase are:
为了完成这一阶段的工作，他需要采取以下步骤和行动:

- Step AP# 1: Conduct Privacy Analysis

步骤 1:进行隐私分析

- Step AP# 2: Collect Privacy Laws

步骤 2:收集隐私法

- Step AP# 3: Analyze Privacy Impact

步骤三:分析隐私影响

- Step AP# 4: Perform Initial Data Audits and Assessments

步骤 AP#4:执行初始数据审计和评估

- Step AP# 5: Establish Data Governance Organization

步骤 AP#5:建立数据治理组织

- Step AP# 6: Establish Data Flows and Personal Data Inventory

步骤 AP#6:建立数据流和个人数据清单

- Step AP# 7: Establish Data Protection and Privacy Program

步骤 AP#7:建立数据保护和隐私计划

- Step AP# 8: Craft DP& P Implementation Action Plans

步骤 AP#8:编制 DP&p 实施行动计划

hese are detailed next.
接下来是详细内容。

Phase 1-DP Preparation: Steps and Actions
第 1 阶段-dp 准备:步骤和行动

Step AP# 1: Conduct Privacy Analysis
步骤 1:进行隐私分析

1.1. Carry out an analysis of the data protection and privacy landscape of your company and the statutes, laws and regulations afecting all functions of the business the company is involved in and the countries or states (provinces if you also operate in Canada) it operates in.

1.1.对贵公司的数据保护和隐私状况进行分析，分析涉及该公司业务所涉及的所有职能的法规、法律和规章，以及该公司业务所在的国家或州(如果您也在加拿大经营，则为各省)。

1.2. Carry out an analysis of the readiness and awareness of your company (board, management staf, etc.) regarding data protection and privacy. *You may use the ‘Data Protection Quiz’ contained in chapter 3 of this volume for this purpose.*

1.2.对公司(董事会、管理层等)在数据保护和隐私方面的准备情况和意识进行分析。为此，你可以使用本卷第三章所载的「资料保护问答游戏」。

1.3. Record the results in a report (data protection and privacy analysis report).

1.3.将结果记录在报告中(数据保护和隐私分析报告)。

1.4. You may also use the following checklist to support your analysis:
1.4.你也可以使用下面的检查表来支持你的分析:

Action 1: Note who sends sen sitive personal information to your company or organization. Customers; Credit card companies; Banks or other inancial institutions; Credit bureaus; Job applicants; and Other companies or organizations.

行动 1:注意谁向你的公司或组织发送了有用的个人信息。客户;信用卡公司;银行或其他金融机构;征信机构;求职者;和其他公司或组织。

Action 2: Document how your company or organization receives personal data.
行动 2:记录你的公司或组织如何接收个人数据。

hrough a website; By email; hrough the normal mail; hrough cash registers
使用网站;通过电子邮件;使用普通邮件;使用收银机

in stores; and any other way.
以及任何其他方式。

Action 3: Note what kind of personal data (see also an example in ‘Chapter 5: Personal Data Checklist’) you collect at each entry point: Credit card information online; Accounting department staf keep information about customers, etc.

行动三:注意你在每个入口点收集的个人资料种类(另见「第五章:个人资料清单」的例子):网上信用卡资料;会计部门保存客户资料等。

Action 4: Record where you keep the data you collect at each entry point. In a central computer database; On individual laptops; On employees’ smartphones, tablets, or other mobile devices; On disks or tapes; In ile cabinets; In branch oices; At the homes of employees, etc.

行动 4:记录你在每个入口点收集的数据放在哪里。中央计算机数据库;个人笔记本电脑;员工智能手机、平板电脑或其他移动设备;磁盘或磁带;文件柜;分支机构;员工家庭等。

Action 5: Note who has (or could have) access to the personal data collected: Which of your employees have permission to access the data; he reason they need access; Other users; Vendors who supply and update software you use to process credit card transactions; and Contractors operating your call center, etc.

行动 5:注意谁有权(或可能有权)访问所收集的个人数据:你的哪些雇员有权访问这些数据;他们需要访问这些数据的理由;其他用户;供应商提供和更新你用来处理信用卡交易的软件;以及承包商运营你的呼叫中心等。

Step AP# 2: Collect Privacy Laws

步骤 2:收集隐私法

2.1. Collect all data protection and privacy rules, regulations and standards afecting your company or organization, both at the local or national level, as well as, at the international level.

2.1.收集所有与你的公司或组织相关的数据保护和隐私规则、法规和标准，不论是在地方或国家层面，还是在国际层面。

2.2. As long as you operate in the EU (European Union) or your activities relate to the ofering of goods and services to individuals in the EU (i.e. most companies in the world) you need to review, study and understand the new EU Data Protection Directive[8] paying more emphasis on the following data protection principles:

2.2.只要你在欧盟(欧盟)经营业务，或你的业务涉及为欧盟的个人(即世界上大部分公司)提供货品和服务，你便需要检讨、研究和了解新的欧盟数据保护指引 8，并更加重视以下的数据保护原则:

Principle 1: Lawful Processing. Personal data shall be processed fairly and lawfully;
原则 1:依法处理。个人资料应当公正、合法地处理;

Principle 2: Purpose Speciication. Personal data shall be obtained only for one or more speciied and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;
原则 2:目的的特殊化。个人资料只能为一个或多个具体和合法的目的而获取，不得以与该目的或这些目的不符的任何方式进一步处理;

Principle 3: Data Relevancy. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
原则 3:数据相关性。就处理个人资料的目的或目的而言，个人资料必须足够、相关及不过份;

Principle 4: Data Accuracy. Personal data shall be accurate and, where necessary, kept up to date;
原则 4:资料准确性。个人资料必须准确，并在有需要时保持最新;

Principle 5: Limited Data Retention. Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes;
原则 5:有限度的数据保留。为任何目的或目的而处理的个人资料的保存期限不得超过该目的或该等目的所需的时间;

Principle 6: Fair Processing. Personal data shall be processed in accordance with the rights of data subjects under this Act;
原则 6:公平处理。个人数据应根据本法规定的数据主体的权利进行处理;

Principle 7: Accountability. Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data; and
原则 7:责任。应采取适当的技术和组织措施，防止未经授权或非法处理个人资料，防止意外遗失、毁坏或损坏个人资料;以及

Principle 8: Transferring personal data overseas. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory

ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.
原则 8:将个人资料移交海外。个人资料不得转移到欧洲经济区以外的国家或地区，除非该国确保并充分保护数据当事人在处理个人资料方面的权利和自由。

You may also review the summary of this law in 'Chapter 4: Summary of the New EU General Data Protection Regulation'.
你也可以在"第四章:新欧盟一般数据保护条例概述"中审阅这项法律的概述。

For a guide to implement the required controls for complying with the EU European Data Protection Directive, see 'Chapter 1: EU Data Protection and Privacy Controls' in Volume 4.
有关实施遵守欧盟数据保护指令所需控制的指南，请参阅第 4 卷中的'第 1 章:欧盟数据保护和隐私控制'。

Step AP# 3: Analyze Privacy Impact
步骤三:分析隐私影响

3.1. Review, study and understand the impact these data protection and privacy rules, regulations and standards may have to your business operations.
3.1.回顾、研究和理解这些数据保护和隐私规则、法规和标准可能对您的业务运作产生的影响。

3.2. Create a ile for all these and assign a company oicer to maintain it according to your company procedures (Privacy Laws Manual).
3.2.为所有这些创建一个文件，并指定一个公司专家根据您的公司程序(隐私法手册)进行维护。

Step AP# 4: Perform Initial Data Audits and Assessments
步骤 AP#4:执行初始数据审计和评估

4.1. Execute an initial personal data audit and a data protection assessment for your company.
4.1.为公司进行初步的个人数据审计和数据保护评估。

4.2. Draft and issue your personal data audit report.
4.2.起草并发布您的个人数据审计报告。

4.3. When conducting initial personal data audits and data protection assessments each company or organization should identify any data protection and privacy risks to individuals, compliance risks and any related risks for the company or organization so that they can avoid ines for non-compliance, potential litigation procedures from individuals for damages and reputational damage leading to loss of business.
4.3.在进行初步的个人数据审计和数据保护评估时，每个公司或组织应确定个人的任何数据保护和隐私风险、合规风险以及公司或组织的任何相关风险，以便避免个人因不合规行为、可能提起的损害赔偿和声誉损害导致业务损失的诉讼程序。

4.4. Companies and organizations might also be able to refer to industry standards and guidance produced by trade bodies, regulators or other organizations working in their sector.
4.4.公司和组织也可以参考行业机构、监管机构或在其部门工作的其他组织制定的行业标准和指南。

思考。

More details on how to do these are included in ‘Volume 3: Data Protection Impact
关于如何做到这些的更多细节包括在'第 3 卷:数据保护影响

Assessment’ (Chapter 1: Data Protection Impact Pre-Assessment Survey; Chapter 2: Data
评估(第一章:资料保护影响预先评估调查;第二章:资料

Protection Impact Risk Assessment; and Chapter 3: Data Protection Risk Resolution Actions).
保护影响风险评估及第三章:数据保护风险解决行动)。

Step AP# 5: Establish Data Governance Organization
步骤 AP#5:建立数据治理组织

5.1. Create a data governance oversight committee. he role of this oversight committee is to review the potential privacy and data protection impacts and risks of structured and unstructured data and ensure appropriate measures and controls are designed and implemented to mitigate the identiied issues and risks.
5.1.创建一个数据治理监督委员会。该监督委员会的作用是审查结构化和非结构化数据化对隐私和数据保护的潜在影响和风险，并确保制定和实施适当的措施和控制，以减轻已查明的问题和风险。

2. Appoint data governance roles. Develop the responsibilities, appoint and train data governance oicers to ensure proper governance and management of structured and unstructured data.
指定数据治理角色。制定职责，任命和培训数据治理专家，以确保结构化和非结构化数据的正确治理和管理。

hese roles include:
这些角色包括:

2.1. A Data Protection Oicer (described in Step OS#2: Assign and maintain Data Protection and Privacy responsibility);
1.一个数据保护器(在步骤 OS#2 中描述:分配和维护数据保护和隐私责任);

2.2. An Information Security Manager; and
图 2。资讯保安经理;及

2.3. Other Data Quality Roles and Responsibilities (for Managers, ICT Personnel, Data Quality Oicers, Administrative staf, a Business Data Librarian, a Business Data Steward, etc.), as described in Volume 2.
图 3。其他数据质量角色和职责(管理人员、信息和通信技术人员、数据质量管理人员、行政管理人员、业务数据库管理员、业务数据管理员等)，如第 2 卷所述。

Step AP# 6: Establish Data Flows and Personal Data Inventory
步骤 AP#6:建立数据流和个人数据清单

6.1. Data Flows System
6.1.数据流系统

1) Knowing the data lows within the organization will help implement and monitor data protection and privacy in a more efective way.
了解组织内部的数据流将有助于以更有效的方式实施和监控数据保护和隐私。

2) For this purpose the company develops and implements a system to document and maintain flow charts for data flows inside and outside the company (between systems, between processes, between countries, between locations or regions, between the company and various outside services providers, etc.).

为此目的，该公司开发并实施了一个系统，用于记录和维护公司内外的低位数据图表(系统之间、流程之间、国家之间、地点或地区之间、公司与各种外部服务提供商之间等)。

3) The company Data Protection and Privacy Office monitors this system and is continuously aware of all in data flows that impact data protection and privacy.

公司的数据保护和隐私 Office 监控着这个系统，并不断关注所有影响数据保护和隐私的数据低点。

6.2. Personal Data Inventory

6.2.个人资料清单

1) The Data Protection and Privacy Office creates and maintains an inventory of personal data held by the various departments and IT systems of the company. This is done by:
资料保护及私隐办公室建立及备存公司各部门及资讯科技系统所持有的个人资料清单。他的工作是由

   a) Locating all types of data (structured and unstructured), both paper as well as electronic, digital, optical, etc., especially as they may reside in your systems, files, storage media and hardware, backup systems, cloud service providers, etc.; and
   定位所有类型的数据(结构化和非结构化)，包括纸张数据、电子数据、数字数据、光学数据等，特别是它们可能存在于你的系统、芯片、存储媒体和硬件、备份系统、云服务提供商等;以及

   b) Identifying which employees (at all levels of the organization) possess these data (structured and unstructured, both paper as well as electronic, digital, optical, etc.).
   确定哪些员工(在组织的所有级别)拥有这些数据(结构化和非结构化，包括纸张以及电子、数字、光学等)。

2) The inventory would address the different types of personal data held (such as: employee data, customer data, client-owned data, and data co-owned with another organization, etc.); where the personal data are held (e.g., servers, mobile devices, desktops, in the cloud, and geographic location, etc.); and responsibility and ownership of these personal data.
个人资料存放地点(例如:雇员资料、客户资料、客户资料及与另一机构共同拥有的资料等);个人资料存放地点(例如:伺服器、流动装置、云端电脑、地理位置等);以及这些个人资料的责任和拥有权。

3) The company establishes a process to ensure that the data inventory is updated regularly to reflect changes related to the personal data maintained.
公司建立一个程序，以确保资料清单定期更新，以反映与所保存的个人资料有关的更改。

4) *More details on how to do this are included: (a) in Volume 2, Chapter 5 (Registers:*
(a)第二册第五章(登记册:
DP&P Register # 1: Business Data Elements Register; DP&P Register # 2: Data Subjects Register; and
Dp&p 登记册#1:业务数据元素登记册;dp&p 登记册#2:数据主体登记册;以及
DP&P Register # 3: Personal Data Elements Dictionary).
Dp & p Register # 3: Personal Data Elements Dictionary).

6.3. Also the Data Protection and Privacy Office of the company writes an effective Data Privacy Policy, explaining how the company collects, uses and discloses personal data.
6.3.同时，公司的数据保护和隐私保护办公室制定了有效的数据隐私政策，解释了公司如何收集、使用和披露个人数据。

For an example of a Data Protection Policy, see Volume 2.
有关数据保护策略的示例，请参阅第 2 卷。

Step AP# 7: Establish Data Protection and Privacy Program

步骤 AP#7:建立数据保护和隐私计划

7.1. Companies and organizations, for better protection and privacy results, implement data protection and privacy through a training plan, a program and a data protection and privacy strategy.

7.1.公司和组织，为了更好的保护和隐私结果，通过培训计划、项目、数据保护和隐私策略来实施数据保护和隐私。

7.2. Privacy Training Plan

7.2.私隐训练计划

1) Carry out an analysis of the communication and training aspects required for your company staf regarding data protection and privacy.

对贵公司在数据保护和隐私方面所需的沟通和培训进行分析。

2) Create your training plan (privacy training plan). More details are included in the Privacy Awareness, Communication and Training Strategy and in the Privacy Awareness, Communication and Training Plan (see Volume 2 for examples).

创建您的培训计划(隐私培训计划)。更多详情载于《私隐关注、沟通及培训策略》及《私隐关注、沟通及培训计划》(例子见第二册)。

7.3. Data Protection and Privacy Strategy

7.3.资料保护及私隐策略

1) The data protection and privacy strategy is based on the Data Protection Risk Assessment and will: Reflect the nature of the organization and its mission; Develop a vision for the company’s data protection and privacy program; Define the data protection and privacy program scope; Establish the Data Protection Officer function; and Detail strategies for achieving the organization’s data protection and privacy priorities.

数据保护和隐私战略是基于数据保护风险评估，并将:重申组织的性质及其使命;为公司的数据保护和隐私计划制定远景规划;确定数据保护和隐私计划范围;建立数据保护 Officer 功能;以及实现组织的数据保护和隐私优先级的详细战略。

7.4. Data Protection and Privacy Program

7.4.资料保护及私隐计划

1) The data protection and privacy program (DP &P Program) is also enabled by the company’s privacy mission statement which: Emphasizes the value the organization places on data protection and privacy; Identifies key objectives of the data protection and privacy program; and Details data protection and privacy strategies and governance controls for achieving those privacy objectives.

数据保护和隐私项目(DP&pProgram)也是通过公司的隐私使命宣言实现的，该宣言强调组织对数据保护和隐私的重视;数据保护和隐私项目的关键目标;实现这些隐私目标的详细数据保护和隐私策略及治理控制。

2) See ‘Appendix 1: Components of a Data Protection and Privacy Program’ and examples of a Data Protection and Privacy Program, a Data Protection Policy and a Data Protection Technology Strategy, an IT Security Strategy and other plans and job descriptions related to data protection, security and quality in Volume 2.

参见附录 1:数据保护和隐私计划的组成部分和数据保护和隐私计划的实例，数据保护政策和数据保护技术战略，IT 安全战略和与数据保护、安全和质量有关的其他计划和职务说明。

Step AP# 8: Craft DP& P Implementation Action Plans

步骤 AP#8:编制 DP&p 实施行动计划

8.1. On the basis of all previous steps (1 to 6), draft, issue and submit a report to your board containing:

8.1.根据以往的步骤(1 至 6)，草拟、发出及向董事局提交报告，内容包括:

1) The analysis and results of the above privacy analysis and preparation activities, the subsequent activities to be implemented (see Phase 2: Organization; Phase 3: Implementation; Phase 4: Governance; and Phase 5: Improvement);

对上述隐私分析和准备活动的分析和结果，以及将要实施的后续活动(见第二阶段:组织;第三阶段:实施;第四阶段:治理;以及第五阶段:改进);

2) A budget (funds, resources, systems, tools, etc.); and

预算(资金、资源、系统、工具等);

3) A set of speciic action plans for executing the complete data protection and privacy process and each phase.

执行完整的数据保护和隐私过程及每个阶段的一套特殊行动计划。

8.2. his report should be reviewed and approved so that resources and personnel are employed for designing, development and operating your data protection and privacy program for the company you manage.

8.2.他的报告应该得到审查和批准，以便使用资源和人员为你所管理的公司设计、开发和运行你的数据保护和隐私程序。

8.3. Your enterprise in now ready to go ahead and implement the data protection and privacy plans for the personal data your company collects, uses, processes and maintains.

8.3.你的企业现在已经准备好为你的公司收集、使用、处理和维护的个人数据实施数据保护和隐私计划。

Phase 1-Preparation: Products and Outcome
第一阶段-准备工作:产品及成果

The products and outcome of this phase are:
这个阶段的产品和结果是:

Product 1: Data protection and privacy analysis report (step 1);
产品 1:数据保护和隐私分析报告(步骤 1);

Product 2: Privacy Laws Manual (step 2 and 3);
产品二:私隐法例手册(第二及第三步);

Product 3: Personal Data Audit Report (step 4);
产品三:个人资料审核报告(第四步);

Product 4: Data Flows System (step 6);
产品 4:数据流系统(步骤 6);

Product 5: Personal Data Inventory (step 6);
产品五:个人资料清单(第六步);

Product 6: Data Protection Policy (step 6);
产品 6:数据保护政策(步骤 6);

Product 7: Privacy Training Plan (step 7);
产品七:私隐培训计划(第七步);

Product 8: Data Protection and Privacy Program (step 7);
产品八:资料保护及私隐计划(第七步);

Product 9: Data Protection and Privacy Organization Report and Budget (steps 1 to 8); and
产品 9:数据保护和隐私组织报告和预算(步骤 1 至 8);以及

Product 10: DP& P Implementation Action Plans (steps 1 to 8)
产品 10:DP&p 实施行动计划(步骤 1 至 8)

The **outcome** of Phase 1 is to prepare your enterprise (board, management and staff) to be more effective in dealing with the data protection and privacy risks and in managing and resolving these better so that the impact to the company's operations, brand-name and profits are minimized as much as possible.
第一阶段的成果是让你的企业(董事会、管理层和管理层)更有效地处理数据保护和隐私风险,更好地管理和解决这些风险,从而尽可能减少对公司运营、品牌和品牌形象的影响。

2.2.2 PHASE 2: DATA PROTECTION AND PRIVACY ORGANIZATION
2.2.2 阶段 2:数据保护和隐私组织

Goal and Objectives
目标及宗旨

The general goal of this phase (**Phase 2-DP&P Organization**) is to establish the organizational structures and mechanisms for the privacy needs of your enterprise.
这个阶段(阶段 2-DP&pOrganization)的总体目标是建立满足企业隐私需求的组织结构和机制。

The more specific objectives of this phase are: to design and set up the data protection and privacy program; a data protection and privacy officer; and to engage and commit all parties concerned with data protection and privacy.

这个阶段更具体的目标是:设计和建立数据保护和隐私保护程序;数据保护和隐私保护机构;以及与数据保护和隐私保护有关的所有各方进行接触和承诺。

he steps and actions required to be executed to complete this phase are:
为了完成这一阶段的工作，他需要采取以下步骤和行动:

- Step OS#1: Maintain Data Privacy Program, Policy and Governance Controls

步骤 1:维护数据隐私计划、策略和治理控制

- Step OS#2: Assign and maintain Data Protection and Privacy responsibility

步骤 OS#2:分配和维护数据保护和隐私责任

- Step OS#3: Maintain Senior Management engagement in Data Protection and Privacy

步骤 3:保持高级管理层在数据保护和隐私方面的参与

- Step OS#4: Maintain Data Protection and Privacy Commitment

步骤 4:维护数据保护和隐私承诺

- Step OS#5: Maintain regular communication for Data Protection and Privacy issues

步骤 5:为数据保护和隐私问题保持定期沟通

- Step OS#6: Maintain stakeholder engagement in Data Protection and Privacy matters

步骤 6:保持利益相关者在数据保护和隐私问题上的参与

- Step OS#7: Implement and Operate the Data Protection and Privacy Computerized System.

步骤 7:实施和操作数据保护和隐私计算机化系统。

hese are detailed next.
接下来是详细内容。

Phase 2-DP Organization: Steps and Actions
阶段 2-DP 组织:步骤和行动

Step OS#1: Maintain Data Privacy Program, Policy and Governance Controls
步骤 1:维护数据隐私计划、策略和治理控制

1.1. Companies and organizations have crafted a data protection and privacy strategy and program in the preparation phase.
1.1.公司和组织在准备阶段制定了数据保护和隐私策略和计划。

1.2. hese are also supported by a privacy policy and data governance controls which are needed to provide further specific guidance to their staf for the collection, use, processing and protection of personal information.
1.2.私隐政策及资料管治控制措施亦有助保障个人资料的收集、使用、处理及保护。

1.3. his privacy policy is based on legal, regulatory, business and data subject requirements and contains comprehensive guidance for the specific company or organization and its staf to achieve compliance with relevant laws, regulations, and contracts while reducing the risk of a data breach.
1.3.他的私隐政策是根据法律、规管、业务及资料当事人的要求而订立，并载有全面的指引，让有关的公司或机构及其注册管理人遵守有关的法例、规例及合约，同时减低资料外泄的风险。

1.4. To implement this policy the specific company will also create and implement a procedure to update the policy and the program based on changes in privacy laws or regulations, or changes in business processes (e.g., the company starts ofering health benefits and needs to collect certain medical information as a result, etc.). See an example of a Data Protection and Privacy Program in volume 2.
1.4.为了实施这一政策，专业公司还将根据隐私法律法规的变化，或业务流程的变化(例如，公司开始捐助健康基金，因此需要收集某些医疗信息等)，创建并实施一个程序来更新政策和程序。参见第 2 卷中的一个数据保护和隐私程序的例子。

1.5. he data protection and privacy program (DP &P Program) is also enabled by the company’s privacy mission statement which: Emphasizes the value the organization places on data protection and privacy; Identifies key objectives of the data protection and privacy program; and Details data protection and privacy strategies and governance controls for achieving those privacy objectives. For an example of Data Governance Controls, see ‘DP&P Plan # 6: Data Quality Improvement Plan’ in Volume 2 and in ‘Chapter 1: EU Data Protection and Privacy Controls’ in Volume 4.
1.5.数据保护和隐私项目(DP&pProgram)也是通过公司的隐私使命宣言实现的，该宣言强调组织对数据保护和隐私的重视;数据保护和隐私项目的关键目标;实现这些隐私目标的详细数据保护和隐私策略及治理控制。有关数据治理控制的例子，请参阅第 2 卷中的"dp&p 计划#6:数据质量改进计划"和第 4 卷中的"第 1 章:欧盟数据保护和隐私控制"。

Step OS#2: Assign and maintain Data Protection and Privacy responsibility
步骤 OS#2:分配和维护数据保护和隐私责任

2.1. Companies and organizations assign responsibility for the operational aspects of a data protection and privacy program to an individual. his individual may sit in a designated data protection or privacy function, or may be part of the legal, compliance, IT, security or information governance or other management departments. Data protection and privacy may be the individual's full-time position (e.g., Data Protection or Privacy Officer) or may be part of the duties of the Compliance Officer, etc.

2.1.公司和组织将数据保护和隐私计划的操作方面的责任分配给个人。个人可能担任指定的资料保护或私隐职能，或可能是法律、合规、资讯科技、保安或资讯管治或其他管理部门的一部分。资料保护及私隐可能是个人的全职工作(例如:资料保护或私隐专员)，或可能是遵从专员的部分职责等。

2.2. Design the duties, roles and responsibilities of a Data Protection and Privacy Officer.
2.2.设计资料保护及私隐专员的职责、角色及责任。

For more details, see 'Data Protection Officer' in Volume 2.
有关更多细节，请参阅第 2 卷中的"数据保护器"。

2.3. Select and appoint the Data Protection or Privacy Officer.
2.3.选择及委任资料保护或私隐专员。

2.4. Ensure that this officer performs his or her duties effectively.
2.4.确保此人有效地履行其职责。

Step OS#3: Maintain Senior Management engagement in Data Protection and Privacy

步骤 3:保持高级管理层在数据保护和隐私方面的参与

3.1. Companies and organizations engage the senior level of the organization, e.g. Board, C-level or senior management, in data protection and privacy for better data protection and privacy results.

3.1.公司和组织聘请组织的高级管理层，如董事会、高级管理层或高级管理层参与数据保护和隐私保护，以获得更好的数据保护和隐私保护结果。

3.2. Support from the senior level can include:

3.2.来自高级别的支持可以包括:

a) Sponsoring all issues related to data protection and privacy at a board of directors' meeting;
在董事会会议上赞助所有与数据保护和隐私有关的问题;

b) Communicating the importance of data protection and privacy to company staf and subordinate management;
向公司管理层沟通数据保护和隐私的重要性;

c) Participating in data protection and privacy initiatives; and
参与资料保护及私隐措施;以及

d) Ensuring adequate funding to support the data protection and privacy function.
确保有足够的资金支持数据保护和隐私功能。

Step OS#4: Maintain Data Protection and Privacy Commitment

步骤 4:维护数据保护和隐私承诺

4.1. Managing data protection and privacy within a company requires the contribution and participation of many members of that organization.

4.1.管理公司内部的数据保护和隐私需要该组织许多成员的贡献和参与。

4.2. For this purpose companies and organizations establish a data protection and privacy network, roles and obtain staf commitment.

4.2.为此，公司和组织建立了一个数据保护和隐私网络，角色和获得的 staf 承诺。

4.3. Members of the data protection and privacy network may work in diferent business functional groups or departments in which the company operates to facilitate understanding of the data protection and privacy risks applicable to that business functional group or department.

4.3.数据保护和隐私网络的成员可以在不同的业务职能组或公司所在部门工作，以促进对适用于该业务职能组或部门的数据保护和隐私风险的了解。

4.4. Also to help the company or organization meet its data protection and privacy mission statement and legal obligations, individuals responsible for data protection and privacy have clear roles and responsibilities that are deined in job descriptions and other job-related documents (e.g. Employment Contract, etc.).

4.4.此外，为协助公司或机构履行其数据保护和隐私使命宣言及法律义务，负责数据保护和隐私的个人有明确的角色和责任，这些角色和责任在职务说明及其他与工作有关的文件(例如雇佣合约等)中有所规定。

4.5. Roles that may be defined include: The Chief Privacy Officer; Privacy Managers; Data Protection Officers (DPO); Privacy Analysts; Data Protection and Privacy Network members; and Data Breach Incident response team members, etc.

4.5.可能被挑选的角色包括:首席隐私保护员;隐私经理;数据保护员(DPO);隐私分析员;数据保护和隐私网络成员;以及数据泄露事件应对小组成员等。

4.6. To ensure corporate staff (management and employees) understand the importance of privacy to the company and hold each individual staff member accountable for their actions with respect to handling personal data, each staff member (manager or employee) acknowledges and agrees to adhere to data protection and privacy policies.

4.6.为了确保企业管理层(管理层和雇员)了解私隐对公司的重要性，并要求每位管理层成员对其处理个人资料的行为负责，每位管理层成员(经理或雇员)承认并同意遵守资料保护和私隐政策。

4.7. This acknowledgement, commitment and agreement can be a separate document (paper or electronic), or it can form part of an existing document, e.g., the Code of Conduct, an Employee Handbook or an individual copy of the Data Protection and Privacy Policy in their personnel files.

4.7.他的确认、承诺及同意书可以是单独的文件(纸张或电子文件)，也可以是现有文件的一部分，例如行为守则、雇员手册或个别人员的个人资料保障及私隐政策副本。

Step OS#5: Maintain regular communication for Data Protection and Privacy issues

步骤 5:为数据保护和隐私问题保持定期沟通

5.1. Constant and regular communication is a must in all company operations.
5.1.在所有的公司运作中，经常和有规律的沟通是必须的。

5.2. For this reason and to efectively implement the company's data protection and privacy strategy, individuals who have been appointed and are accountable and responsible for data protection and privacy must regularly communicate with each other in order to:
5.2.为此，并为了有效实施公司的数据保护和隐私战略，被任命、负责和负责数据保护和隐私的个人必须定期相互沟通，以便:

a) Learn about the use of personal data in the context of the speciic company;
了解在专业公司使用个人资料的情况;

b) Proactively assist in building data protection and privacy into all systems, services, products and ongoing projects;
积极协助建立数据保护和隐私到所有系统，服务，产品和正在进行的项目;

c) Understand the diferent perspectives about data protection and privacy throughout the company;
了解整个公司对数据保护和隐私的不同观点;

d) Enable, facilitate and support individuals to meet their objectives and targets while implementing data protection and privacy; and
协助、促进和支持个人在实施资料保护和私隐的同时，达到其目标和指标;以及

e) Integrate data protection and privacy thinking across the whole company and across all its functions.
整合整个公司及其所有职能部门的数据保护和隐私思想。

More details are included in the Privacy Awareness, Communication and Training Strategy and in the Privacy Awareness, Communication and Training Plan in Volume 2.
第二册《私隐关注、沟通及培训策略》及《私隐关注、沟通及培训计划》载有更多详情。

Step OS#6: Maintain stakeholder engagement in Data Protection and Privacy matters

步骤 6:保持利益相关者在数据保护和隐私问题上的参与

6.1. To proactively address data protection and privacy matters, as well as efectively respond to data protection and privacy issues that are relevant and impact stakeholders throughout the company, the Data Protection and Privacy Function:
6.1.为积极处理资料保护及私隐事宜，以及积极回应公司内相关及影响持份者的资料保护及私隐事宜，资料保护及私隐职能:

a) Conducts informal or ad hoc communications with individuals whose responsibilities may not include data protection and privacy;
与责任可能不包括数据保护和隐私的个人进行非正式或临时通信;

b) Participates in various corporate committees for business functions or units whose activities may have data protection and privacy impacts (e.g., information security, marketing, etc.); and

参与不同的公司委员会，负责业务职能或其活动可能对数据保护和私隐有影响的部门(例如，资讯保安、市场推广等);以及

c) Conducts formal discussions (e.g., monthly meetings) about data protection and privacy issues among partners outside the organization (e.g. cloud providers, information services providers, application maintenance vendors, etc.) who have ownership (accountability or responsibility) for data protection and privacy matters.

就数据保护和隐私问题与组织外的合作伙伴(如云服务提供商、信息服务提供商、应用程序维护供应商等)进行正式讨论(如每月会议)，这些合作伙伴对数据保护和隐私问题拥有所有权(责任或义务)。

Step OS#7: Implement and Operate the Data Protection and Privacy Computerized System

步骤 7:实施和操作数据保护和隐私计算机化系统

7.1. Enterprise data protection is one of the most critical priorities facing organizations today.
7.1.企业数据保护是当今组织面临的最重要的优先事项之一。

7.2. With so many potential threats and entry points, data protection solutions must take
7.2.由于存在如此多的潜在威胁和入口点，数据保护解决方案必须采取

a comprehensive, end-to-end approach that begins by identifying valuable at-risk data and devising a continuous data protection strategy that accounts for every potential threat – before threats are even identiied.

全面、端到端的方法，首先是确定有价值的风险数据，并制定持续的数据保护战略，在查明威胁之前考虑到每一个潜在威胁。

7.3. his is resolved by designing the speciications of a computerized system and software tools to support the data protection and privacy process of the organization and operate it efectively.

7.3.通过设计一个计算机化的系统和软件工具来支持组织的数据保护和隐私过程，并有效地进行操作，解决了这个问题。

7.4. A data protection and privacy computerized system software ensures data integrity by various methods, such as: verifying the original and backup iles through hash algorithms; encrypting data in transit and at rest; providing a centralized data management compliance interface; reporting of backup successes and failures; managing all aspects of the Binding Corporate Rules (BCR) process; measuring and reporting on compliance with national laws, etc.

7.4.数据保护和隐私计算机化系统软件通过各种方法确保数据的完整性，例如:通过散列算法核实原始文件和备份文件;在传输和休息时对数据进行加密;提供一个中央数据管理合规接口;报告备份的成功和失败;管理《联合公司规则》进程的所有方面;衡量和报告遵守国家法律的情况等。

Phase 2-DP Organization: Products and Outcome

第二阶段-发展阶段组织名称:产品及成果

he products and outcome of this phase are:
这个阶段的产品和结果是:

Product 1: Updated data protection and privacy strategy (step 1);
产品一:更新资料保护及私隐策略(第一步);

Product 2: Updated data protection and privacy program (step 1);
产品二:更新资料保护及私隐计划(第一步);

Product 3: Data Governance Controls (step 1);
产品 3:数据治理控制(步骤 1);

Product 4: Announcement of the appointment of the Data Protection or Privacy Oicer (step 2);
产品 4:委任资料保护或私隐专员(第二步);

Product 5: Communications related to data protection and privacy (step 3, 4, 5 and 6);

产品 5:与数据保护和隐私有关的通信(步骤 3、4、5 和 6);

Product 6: Data protection and privacy network (step 4);
产品 6:数据保护和隐私网络(步骤 4);

Product 7: Data protection and privacy role in job descriptions (step 4);
产品 7:工作描述中的数据保护和隐私角色(步骤 4);

Product 8: Updated Privacy Awareness, Communication and Training Plan (step 5); and
产品八:更新的私隐关注、沟通及培训计划(第五步);及

Product 8: Data protection and privacy computerized system (step 7);
产品 8:数据保护和隐私计算机化系统(步骤 7);

he outcome of Phase 2 is to establish the data protection and privacy organizational structures for better data protection and privacy implementation.
第二阶段的成果是建立数据保护和隐私的组织结构，以便更好地保护数据和实现隐私。

2.2.3 PHASE 3: DATA PROTECTION AND PRIVACY DEVELOPMENT
2.2.3 第三阶段:资料保护及私隐发展

AND IMPLEMENTATION
与执行

Goal and Objectives
目标及宗旨

he general goal of this phase (**Phase 3-DP&P Development and Implementation**) is to develop and implement specific data protection and privacy measures and controls for your company or organization.
这个阶段(阶段 3-DP&p 开发和实施)的总体目标是为您的公司或组织开发和实施专门的数据保护和隐私措施及控制。

he more specific objectives of this phase are: to design a data classification system; and to develop and implement all the required policies, procedures and controls (e.g., manage sensitive data, executing training plan, integrating privacy into your operations, etc.) necessary to implement the data protection and privacy laws and requirements for your company or organization.
这个阶段更具体的目标是:设计一个数据分类系统;开发和实施所有必要的政策、程序和控制(例如，管理敏感数据、执行培训计划、将隐私纳入您的操作等)，以实施公司或组织的数据保护和隐私法律及要求。

he steps and actions required to be executed to complete this phase are:
为了完成这一阶段的工作，他需要采取以下步骤和行动:

- Step DI#1: Develop and implement Data Protection and Privacy Strategies, Plans and Policies
第一步:制定和实施数据保护和隐私策略、计划和政策
- Step DI#2: Implement Approval Procedure for Processing Personal Data
第 DI#2 步骤:实施处理个人资料的审批程序
- Step DI#3: Register Databases of Personal Data
步骤 DI#3:注册个人资料数据库
- Step DI#4: Develop and Implement a Cross-Border Data Transfer System
第四步:开发和实现跨境数据传输系统
- Step DI#5: Execute DP &P integration activities
第 5 步:执行 DP&p 集成活动
- Step DI#6: Execute DP &P training plan
第 6 步:执行 DP&p 培训计划
- Step DI#7: Implement Data Security controls
步骤 DI#7:实现数据安全控制

hese are detailed next.
接下来是详细内容。

Phase 3-DP Development: Steps and Actions
阶段 3-DP 发展:步骤和行动

Step DI#1: Develop and implement Data Protection and Privacy Strategies, Plans and Policies

第一步:制定和实施数据保护和隐私策略、计划和政策

his step includes the following work tasks:
他的步骤包括以下工作任务:

Work Task 1. Data Protection and Privacy Strategies, Plans and Policies

工作任务 1。数据保护和隐私策略、计划和政策

1.1. Analyze and deine your enterprise's needs and requirements.
1.1.分析和设计您的企业的需求和要求。

1.2. Select which strategies, plans, policies and controls (see details in 'Appendix 1: Components of a Data Protection and Privacy Program' and in Volumes 2 and 4) you will implement for your enterprise.
1.2.选择您将为企业实现的策略、计划、策略和控制(详见"附录 1:数据保护和隐私计划的组成部分"和第 2 卷和第 4 卷)。

1.3. Assign responsibilities for implementing these.
1.3.分配实现这些目标的责任。

Work Task 2. Data Classiication System
工作任务 2。数据分类系统

2.1. Develop a data classiication system and use it to classify personal data as “publicly available”, “conidential”, “sensitive”, etc.
2.1.开发一个数据分类系统，并使用该系统将个人数据分类为"公开可用"、"同一性"、"敏感性"等。

2.2. his system will allow the company to narrow the scope of what needs to be protected and how.
2.2.他的系统将允许公司缩小需要保护的范围和如何保护。

2.3. Also create procedures to implement the company’s data classiication scheme, along with details about data ownership, a description of retention requirements and appropriate use and protection requirements based on the classiication level and legal requirements (e.g., certain types of data may be subject to particular legal requirements, such as health or inancial data, etc.).
2.3.同时根据分类级别和法律要求(例如，某些类型的数据可能受到特定法律要求的约束，例如健康或财务数据等)，创建实施公司数据分类计划的程序，以及有关数据所有权的详细信息、保留要求的描述以及适当的使用和保护要求。

For more details, see ‘DP&P Policy # 3: Data Classiication Policy’ in Volume 2.
有关更多细节，请参阅第 2 卷中的"dp&p 策略#3:数据分类策略"。

图 34

Step DI#2: Implement Approval Procedure for Processing Personal Data
第 DI#2 步骤:实施处理个人资料的审批程序

2.1. In certain cases or jurisdictions, companies and organizations must obtain approval from data protection and privacy regulators prior to collecting and processing personal data.

2.1.在某些情况下，公司和组织在收集和处理个人数据之前，必须获得数据保护和隐私监管机构的批准。

2.2. These situations may arise when the processing operations of the specific company are likely to present specific risks to data subjects, such as: processing sensitive personal data; processing personal data for the purpose of evaluating personal aspects of the individual or determining the individual’s eligibility for a right, benefit or contract; and collecting and processing on large scale (e.g., Big Data), etc.

2.2.当特殊公司的处理业务可能对资料当事人构成特殊风险时，便可能出现这些情况，例如:处理敏感的个人资料;处理个人资料以评估个人的个人方面，或确定个人是否有资格享有权利、受益人或合约;以及大规模收集和处理资料(例如大数据)等。

2.3. The company develops procedures to determine instances where approval is required, consult with the national or European regulator if it is unclear whether approval is required, and document the whole approval process.

2.3.公司制定程序，以确定哪些情况需要审批，如果不清楚是否需要审批，则咨询国家或欧洲监管机构，并记录整个审批过程。

Step DI#3: Register Databases of Personal Data
步骤 DI#3:注册个人资料数据库

3.1. In certain cases or jurisdictions, companies and organizations must notify the data protection and privacy regulators (national, European) of its databases containing personal data and the processing intended and register them with the authorities accordingly.

3.1.在某些情况下，公司和组织必须将其载有个人数据的数据库和打算进行的处理情况通知数据保护和隐私监管机构(国家和欧洲)，并相应地向当局登记。

3.2. The company develops procedures to determine when the company must register its databases, what information to include in registrations, how to go about registering and document the whole approval process.

3.2.公司制定程序，以确定公司何时必须注册其数据库，注册中应包括哪些信息，如何进行注册和记录整个审批过程。

Step DI#4: Develop and Implement a Cross-Border Data Transfer System
第四步:开发和实现跨境数据传输系统

4.1. Sending personal data abroad, even within the organization, can increase data protection risks and the complexity of managing them due to the differing privacy law requirements.

4.1.由于隐私法的不同要求，将个人数据发送到国外，甚至在组织内部，都会增加数据保护的风险和管理这些数据的复杂性。

4.2. For this purpose the company develops and implements a system to maintain records of the transfer mechanism used for cross-border data flows (e.g. standard contractual clauses, binding corporate rules, approvals from regulators, etc.).

4.2.为此，该公司开发并实施了一个系统，以保存用于跨境数据低位的转移机制的记录(例如标准合同条款、有约束力的公司规则、监管机构的批准等)。

4.3. Also maintains documentation regarding all cross-border lows, tracking its use of, and compliance with, cross-border transfer mechanisms, such as: Corporate codes of conduct such as Binding corporate rules (BCR) to comply with data transfer rules; model clauses in contracts; Data protection authority approvals; and Reliance on any exemption from the transfer requirements as set out in law.

4.3.还保存关于所有跨境低价的文件，跟踪跨境转移机制的使用和遵守情况，例如:公司行为守则，如遵守数据转移规则的具有约束力的公司规则;合同示范条款;数据保护当局的批准;以及依赖法律规定的转移要求的任何豁免。

4.4. he purpose of BCR is to ensure that adequate safeguards are in place to protect the rights of data subjects and must be approved by the appropriate data protection and privacy regulators.

4.4.的目的是确保有足够的保障措施保护数据当事人的权利，并且必须得到适当的数据保护和隐私监管机构的批准。

4.5. Governments and regulators create model clauses to facilitate the transfer of personal data from a privacy-protective regime to a recipient in a country that does not provide adequate protections for personal data. When disclosing personal data to third parties in a country with inadequate privacy protections, the organization uses these standard contractual clauses in its vendor contracts and processing agreements to ensure protection for personal data.

4.5.各国政府和监管机构制定了示范条款，以便于将个人数据从隐私保护制度转移到一个对个人数据没有提供充分保护的国家的收件人。在隐私保护不足的国家向第三方披露个人数据时，本组织在其供应商合同和处理协议中使用这些标准合同条款，以确保对个人数据的保护。

4.6. When transfer mechanisms such as Binding Corporate Rules (BCRs) or model contracts are not available, the company may seek the approval of the data protection/privacy regulator to legitimize the transfer for data. In transferring sensitive data, such as biometric data, the authorization of the regulator is always required.

4.6.如果没有具有约束力的公司规则或示范合同等转移机制，公司可寻求数据保护/隐私监管机构的批准，以使数据转移合法化。在传输敏感数据时，例如生物特征数据，总是需要监管者的授权。

Step DI#5: Execute DP&P integration activities
第 5 步:执行 dp&p 集成活动

5. 1. Companies and organizations include data protection and privacy into all their operations by executing a speciic set of integration activities which embed this data protection and privacy in all its aspects, such as: corporate records retention; corporate staf hiring; website access; digital marketing; social media; portable and smart devices; health and safety; system and product development, etc.

1.公司和组织将数据保护和隐私纳入他们所有的业务中，通过执行一系列特殊的集成活动，将这些数据的保护和隐私纳入其所有方面，例如:公司记录保留;公司注册雇佣;网站访问;数字营销;社交媒体;便携式和智能设备;健康和安全;系统和产品开发等。

For more details, see ‘DP&P Plan # 5: Integration Activities Plan’ in Volume 2.
有关更多细节，请参阅第 2 卷中的"dp&p 计划#5:整合活动计划"。

Step DI#6: Execute DP&P training plan
第 6 步:执行 dp&p 培训计划

6.1. Companies and organizations train their staf to better implement data protection and privacy in all their programs, systems, projects and functions.

6.1.公司和组织培训他们的技术工人，以便在他们所有的程序、系统、项目和功能中更好地实施数据保护和隐私。

6.2. his plan includes the following actions:
6.2.他的计划包括以下行动:

Action #1: Carry out ongoing data privacy training for the Privacy Oice
行动#1:为隐私办公室进行持续的数据隐私培训

Action #2: Execute basic privacy training for staf

行动#2:为 staf 执行基本的隐私培训

Action #3: Execute additional privacy training for new needs

行动#3:针对新的需求执行额外的隐私培训

Action #4: Include data privacy training into other corporate training

行动#4:将数据隐私培训纳入其他公司培训

Action #5: Maintain data privacy awareness

行动#5:保持数据隐私意识

Action #6: Maintain data privacy professional certiication for privacy personnel

行动#6:为私隐人员维护数据私隐专业认证

Action #7: Measure data privacy awareness and training activities.

行动#7:衡量数据隐私意识和培训活动。

For more details, see ‘Privacy Awareness, Communication and Training Plan’ in Volume 2.

有关详细信息，请参阅第二卷中的"隐私意识、沟通和培训计划"。

Step DI#7: Implement Data Security controls

步骤 DI#7:实现数据安全控制

7.1. Enterprises implement a set of data security controls for the better protection of personal data held in the enterprise's IT systems and data bases.

7.1.为了更好地保护企业 IT 系统和数据库中的个人数据，企业实施了一套数据安全控制。

7.2. This is effectively done via a data security plan that includes the following steps:

7.2.数据安全计划包括以下步骤:

Step 1: Include Data Privacy into the Corporate Security Policy
第一步:将资料私隐纳入公司保安政策

Step 2: Include Data Privacy into the Information Security Policy
第二步:将资料私隐纳入资讯保安政策

Step 3: Include Data Privacy into the Acceptable Use Policy
第三步:将数据隐私纳入可接受的使用策略

Step 4: Include Data Privacy into Security Risk Assessments
第四步:将资料私隐纳入保安风险评估

Step 5: Implement IT Technical Security Controls
第五步:实施资讯科技保安控制

Step 6: Implement Human Resources Security Controls
第六步:实施人力资源安全控制

Step 7: Include data privacy into business continuity planning
第七步:将数据隐私纳入商业连续性

Step 8: Develop and Implement a data-loss prevention strategy
步骤 8:制定并实施数据丢失预防策略

Step 9: Conduct regular testing of data security
步骤 9:定期测试数据安全性

Step 10: Maintain security certification
步骤 10:维护安全认证

For full details, see the 'Data Security Management Plan' in Volume 2.

有关详细信息，请参阅第 2 卷中的"数据安全管理计划"。

Phase 3-DP Implementation: Products and Outcome

阶段 3-DP 实施:产品和成果

The products and outcome of this phase are:

这个阶段的产品和结果是:

Product 1: Personal Data Classification System (step 1);
产品一:个人资料分类系统(第一步);

Product 2: Procedure for Approving the Processing of Personal Data (step 2);
产品 2:批准处理个人资料的程序(第 2 步);

Product 3: Personal Data Bases Registration document (step 3);
产品三:个人资料库登记文件(第三步);

Product 4: Step DI#4: Develop and Implement a Cross-Border Data Transfer System (step 4);
产品 4:步骤 DI#4:开发并实现跨境数据传输系统(步骤 4);

Product 5: Executed DP&P integration activities (step 5);

产品 5:执行 dp&p 集成活动(步骤 5);

Product 6: Executed DP &P training activities (step 6); and
产品 6:执行 DP&p 培训活动(步骤 6);以及

Product 7: Implemented Data Security controls (step 7);
产品 7:实现的数据安全控制(步骤 7);

he **outcome** of Phase 3 is to develop and implement a set of data protection and privacy measures to govern personal data more efectively for your enterprise.
第三阶段的成果是开发和实施一套数据保护和隐私措施，以便更有效地为企业管理个人数据。

2.2.4 PHASE 4: DATA PROTECTION AND PRIVACY GOVERNANCE
2.2.4 阶段 4:数据保护和隐私管理

Goal and Objectives
目标及宗旨

The general goal of this phase (**Phase 2-DP&P Governance**) is to establish the privacy governance mechanisms for your company or organization.
这个阶段(阶段 2-DP&p 治理)的总体目标是为您的公司或组织建立隐私治理机制。

The more specific objectives of this phase are: to design and set up the data protection and privacy governance structures (e.g., a data protection and privacy program; a data protection and privacy officer and often a data protection and privacy committee, etc.); to engage and commit all parties concerned with data protection and privacy; and to report on all data protection and privacy issues of your company or organization on a continuing basis.
这个阶段更具体的目标是:设计和建立数据保护和隐私治理结构(例如，数据保护和隐私程序;数据保护和隐私保护者，通常是数据保护和隐私委员会等);与数据保护和隐私相关的所有各方保持接触并作出承诺;以及持续报告贵公司或组织的所有数据保护和隐私问题。

The steps and actions required to be executed to complete this phase are:
为了完成这一阶段的工作，他需要采取以下步骤和行动:

- Step GR#1: Implement Practices for Managing the uses of data
步骤 GR#1:实现管理数据使用的实践
- Step GR#2: Maintain Data Privacy Notices
步骤 GR#2:维护数据隐私通知
- Step GR#3: Execute a Requests, Complaints and Rectification Plan
步骤 GR#3:执行请求、抱怨和纠正计划
- Step GR#4: Execute a Data Protection Risk Assessment
步骤 GR#4:执行数据保护风险评估
- Step GR#5: Issue Data Protection and Privacy Reports
步骤 GR#5:发布数据保护和隐私报告
- Step GR#6: Maintain Data Privacy Documentation
步骤 GR#6:维护数据隐私文档
- Step GR#7: Establish and Maintain a Data Privacy Breach Response Plan
步骤 GR#7:建立和维护数据隐私泄露应对计划

These are detailed next.
接下来是详细内容。

Phase 4-DP Governance: Steps and Actions
阶段 4-DP 治理:步骤和行动

Step GR#1: Implement Practices for Managing the uses of data
步骤 GR#1:实现管理数据使用的实践

1. Sensitive Data
敏感数据

1) Some types of personal data are considered sensitive, and require a higher standard of care and protection.

有些类型的个人资料被认为是敏感的，需要更高标准的照顾和保护。

2) Common examples of what is usually considered ‘sensitive’ include: Political opinions; Racial or ethnic origin; Data relating to sexual life; Religious or philosophical beliefs; Membership in a trade union; Physical or mental health information; Social welfare; Financial information; National or other government identifiers, e.g. Social Security numbers; Criminal charges or convictions; Biometrics; Genetic data; Location data; and Data pertaining to children.

通常被认为是'敏感'的例子包括:政治观点;种族或族裔出身;与性生活有关的数据;宗教或哲学信仰;工会成员资格;身体或心理健康信息;社会福利;财务信息;国家或其他政府身份标识，例如社会安全号码;刑事指控或定罪;生物特征识别;遗传数据;位置数据;以及与儿童有关的数据。

3) Companies and organizations maintain practices that include policies and procedures for collection and use of sensitive personal data (including biometric data, data of children, etc.).

公司和组织维护的做法包括收集和使用敏感的个人数据(包括生物特征数据、儿童数据等)的政策和程序。

4) The Data Protection or Privacy Officer ensures that these practices are implemented fully to add the additional protection required to process sensitive personal data lawfully.

资料保护或私隐专员确保这些措施得到充分执行，以加强合法处理敏感个人资料所需的额外保护。

2. Automated Decision-Making Process for Personal Data
个人数据的自动决策过程

1) Some decisions taken about individuals may have a legal or signiicant efect on them, such that they should not be made on the sole basis of automated or computerized processing.

对个人作出的一些决定可能对他们有法律或重大影响，因此不应仅仅依靠自动化或计算机化处理作出这些决定。

2) Companies and organizations have mechanisms (practices, policies and procedures) in place to evaluate the signiicance of any automated decision-making it undertakes (i.e., do the decisions have legal or signiicant efect on the individual) and take steps to introduce a manual review process where signiicant decisions are being made.

公司和组织有适当的机制(惯例、政策和程序)来评估它所进行的任何自动化决策的重要性(即这些决策对个人是否具有法律或重要影响)，并采取步骤，在作出重大决定时实行人工审查程序。

3) he Data Protection or Privacy Oicer ensures that these practices are implemented fully to avoid the potential risks of automated decision-making on these personal data.

资料保护或私隐专员确保这些措施得到充分执行，以避免就这些个人资料作出自动化决策的潜在风险。

3. Secondary Uses of Personal Data
个人资料的次要用途

1) Secondary uses of personal data are uses of personal data by an organization for that go beyond the primary purpose.

个人资料的次要用途是指组织将个人资料用于超越主要目的的用途。

2) Companies and organizations implement mechanisms (practices, policies and procedures) that deine: he purpose of personal data processing; and how to address situations when it wishes to use the personal data in ways that diverge from those deined purposes.

公司和组织实施的机制(惯例、政策和程序)符合个人资料处理的目的;以及如何处理它希望以偏离那些已经受到限制的目的的方式使用个人资料的情况。

3) he Data Protection or Privacy Oicer ensures that these practices are implemented fully to avoid the potential risks of non-authorized secondary processing on these personal data.

数据保护或隐私 Oicer 确保这些做法得到充分实施，以避免对这些个人数据进行未经授权的二次处理的潜在风险。

Step GR#2: Maintain Data Privacy Notices
步骤 GR#2:维护数据隐私通知

2.1. Enterprises maintain data privacy notices to individuals consistent with the data privacy policy, legal requirements, and operational risk tolerance.

2.1.企业维护个人数据隐私通知，这与数据隐私政策、法律要求和作业风险容忍度相一致。

2.2. hese notices identify: What personal data are is collected; How the personal data are collected, used, maintained, retained and disclosed; and What specific control the individuals' whose personal data is involved have.

2.2.个人资料如何收集、使用、保存、保留及披露，以及涉及个人资料的人士有何特别控制。

2.3. At each point where the specific enterprise collects personal data (e.g., online, via text message, phone or in person, marketing communications, employee application forms, etc.):

2.3.在专业企业收集个人数据的每一个环节(例如，在线、短信、电话或面对面、市场营销沟通、员工申请表等):

a) he individual concerned has the opportunity to review the enterprise's data privacy notice or receive information about the organization's data privacy practices prior to providing personal data ('just in time' notice);

有关个人在提供个人资料前，有机会审阅企业的资料私隐通知或接收有关机构的资料私隐措施的资料(「即时」通知);

b) he organization provides simplified information related to its privacy policies and practices to the public through visual and other means, including emails, flyers, offers, posters and signs.

该组织通过视觉和其他方式向公众提供与隐私政策和实践相关的简化信息，包括电子邮件、莱尔斯、ofers、海报和标志。

c) It also provides notices on its applications for service, receipts and bills, contracts and terms of service.

此外，本处亦会就服务申请、收据及帐单、合约及服务条款等事宜发出通知。

d) Furthermore, when personal data are collected over the phone or in person, the enterprise provides guiding instructions for use by front-line employees to provide basic explanations of the organization's privacy policies and practices, including the collection and use of these personal data.

此外，在通过电话或面对面收集个人数据时，企业提供指导说明，供一线员工使用，以便对本组织的隐私政策和做法，包括收集和使用这些个人数据作出基本解释。

e) As regards the issue of privacy notices on the enterprise's website the company ensures that privacy seals or trustmarks are displayed on the enterprise's website (s) to assure site visitors of the legitimacy of the website and to demonstrate a commitment to privacy principles defined by a third party (the seal or trustmark provider).

关于在企业网站上发布隐私通知的问题，公司确保在企业网站上展示隐私印章或信任标记，以向网站访问者保证网站的合法性，并表明对第三方(印章或信任标记提供者)所遵守的隐私原则的承诺。

Step GR#3: Execute a Requests, Complaints and Rectification Plan
步骤 GR#3:执行请求、抱怨和纠正计划

3.1. The enterprise executes the activities related to handling complaints, managing requests for access and updating of information by the individuals of their personal data held by the enterprise.

3.1.企业执行与处理投诉、管理个人查阅和更新企业持有的个人资料的请求有关的活动。

3.2. This plan contains: Personal Data Access Procedures; Personal Data Complaints Procedures; Personal Data Rectification Procedures; Personal Data Objection Procedures; Personal Data Portability Procedures; Personal Data Erasure Procedures; and Personal Data Handling Information Procedures.

3.2.他的计划包括:查阅个人资料程序;个人资料投诉程序;个人资料处理程序;个人资料反对程序;个人资料转携程序;个人资料删除程序;及个人资料处理资料程序。

3.3. For more details, see: 'Requests, Complaints and Rectification Plan' in Volume 2.

3.3.有关详细信息，请参阅第 2 卷中的"请求、投诉和整改计划"。

Step GR#4: Execute a Data Protection Risk Assessment
步骤 GR#4:执行数据保护风险评估

1. Data Protection Risk Assessment
资料保护风险评估

1) The scope of the data protection and privacy program is determined by the legal and regulatory compliance challenges and data impacted.

数据保护和隐私计划的范围取决于法律和守规挑战以及受到影响的数据。

2) The Data Protection and Privacy Office has a procedure for conducting an organizational data protection risk assessment across business units (including IT, human resources, sales, marketing, production, and product development, etc.).

资料保护及私隐 Office 有一套程序，用以进行跨业务单位(包括资讯科技、人力资源、销售、市场推广、生产及产品开发等)的组织资料保护风险评估。

3) The data protection risk assessment is a prerequisite for further development of an Organizational Data Protection and Privacy Program, in which the Data Protection and Privacy Office creates and oversees individual business unit data protection and privacy and security self-assessments, business process reviews, process improvements, communications and training, etc.

资料保护风险评估是进一步发展「组织资料保护及私隐计划」的先决条件。「组织资料保护及私隐计划」负责建立及监察个别业务单位的资料保护、私隐及保安自我评估、业务流程检讨、程序改善、通讯及培训等工作。

4) The risk assessment process enables the Data Protection and Privacy Office to identify and prioritize privacy and security gaps across the organization and manage the privacy program for risk mitigation, compliance and to increase brand reputation and customer trust.

风险评估过程使得数据保护和隐私办公室能够识别并优先处理整个组织的隐私和安全漏洞，并管理隐私项目以减少风险、合规，并增加品牌声誉和客户信任。

More details on how to do these are included in Volume 3: Data Protection Impact Assessment (Chapter 1: Data Protection Impact Pre-Assessment Survey; Chapter 2: Data Protection
第三册:资料保护影响评估(第一章:资料保护影响预先评估调查;第二章:资料保护)载有更多有关如何进行这些工作的详情

Impact Risk Assessment; and Chapter 3: Data Protection Risk Resolution Actions).
影响风险评估及第三章:数据保护及风险解决行动)。

2. hird-Party Risks
税务风险

1) he Data Protection and Privacy Oice also ensures that third party risks are properly managed. More details are included in the 'hird-Party Risks Management Plan' in Volume 2.

数据保护和隐私奥斯还确保第三方风险得到妥善管理。更多详情载于第二册的「税务风险管理计划」。

3. Privacy and Business Risk Assessment
私隐及商业风险评估

1) Companies and organizations and their risk functions usually conduct business risk assessments to identify and assess the factors and issues that may afect the success of their business operations.

公司和组织及其风险职能部门通常进行业务风险评估，以确定和评估可能影响其业务运作成功的因素和问题。

2) As part of this process and with Data Protection and Privacy Oice support, these risk functions also consider any privacy risks that may appear during this analysis as one additional element afecting the organization's business eforts.

作为这个过程的一部分，在数据保护和隐私保护的支持下，这些风险功能还考虑到在分析过程中可能出现的任何隐私风险，将其作为企业业务要塞的一个附加要素。

3) his data protection and privacy risk analysis and assessment only touches on the how data risks may be assessed. It does not address all the methods for reviewing risks and mitigating controls, nor does it list all the risks that will arise in a business risk assessment. his is the job of the data protection risk impact described in Volume 2.

他的资料保护和私隐风险分析及评估只涉及如何评估资料风险。它没有涉及审查风险和减轻控制的所有方法，也没有列出在业务风险评估中将出现的所有风险。他的工作是数据保护的风险影响描述第 2 卷。

Step GR#5: Issue Data Protection and Privacy Reports
步骤 GR#5:发布数据保护和隐私报告

5.1. he company issues a report to internal stakeholders on the status of data protection and privacy management (e.g. board of directors, management, shareholders).
5.1.公司向内部持份者发出报告，说明资料保护和私隐管理的状况(例如董事会、管理层、股东)。

5.2. Reporting on data protection and privacy is essential to accurately, comprehensively and efficiently inform those accountable for overseeing and managing the data protection and privacy program to ensure that the company achieves compliance and reduces risks related to the processing of personal data.

5.2.报告数据保护和隐私是必不可少的，这样才能准确、全面和及时地告知负责监督和管理数据保护和隐私计划的人员，以确保公司遵守规定，减少与处理个人数据有关的风险。

5.3. The status of the data protection and privacy program is communicated internally, including to management, senior executives and the board of directors, on a regular basis.

5.3.数据保护和隐私项目的状况定期在内部进行沟通，包括向管理层、高级主管和董事会进行沟通。

5.4. These communications align the data protection and privacy function with company objectives, focusing on how privacy supports the organization’s bottom line, as well as highlighting the status of compliance with legal and regulatory requirements.

5.4.这些通信使数据保护和隐私功能与公司目标相一致，重点关注隐私如何支持组织的底线，以及强调遵守法律和监管要求的状况。

5.5. The company also issues a report (generated internally, result of audits, etc.) to external stakeholders on the status of data protection and privacy management (e.g. regulators, third-parties, clients).

5.5.公司亦会向外界持份者(例如监管机构、第三者、客户等)发出报告(内部产生、审计结果等)，说明资料保护及私隐管理的情况。

5.6. External awareness of the status of the company’s data protection and privacy program builds confidence among customers, vendors, data protection and privacy regulators, and the general public.

5.6.对公司数据保护和隐私项目状况的外部意识在客户、供应商、数据保护和隐私监管机构以及公众之间建立了共识。

Step GR#6: Maintain Data Privacy Documentation
步骤 GR#6:维护数据隐私文档

6.1. The company develops, implements and maintains up-to-date documentation that reflects the status of the organization's data protection and privacy program.
6.1.公司开发，实施和维护最新的文件，反映组织的数据保护和隐私项目的状态。

6.2. This documentation is available by the company to demonstrate to regulators and authorities how it complies with privacy and data protection laws, as well as how it is accountable for the functioning of the privacy program.
6.2.该公司提供他的文件，向监管机构和有关部门展示该公司是如何遵守隐私和数据保护法的，以及该公司是如何对隐私项目的运作负责的。

6.3. Such documentation also serves as evidence when applying for 'trustmarks', seals, BCRs, certifications, and participation in other self-regulatory programs.
6.3.当申请"信任标记"、印章、BCRs、认证和参与其他自我监管项目时，这些文件也可作为证据。

Step GR#7: Establish and Maintain a Data Privacy Breach Response Plan
步骤 GR#7:建立和维护数据隐私泄露应对计划

7.1. The enterprise designs, develops, implements and maintains a data security incident or data privacy breach response plan that provides a coherent, systematic and proactive way of managing data privacy breaches and security incidents that affect personal data in a consistent way.
7.1.企业设计、开发、实施和维护一个数据安全事件或数据隐私泄漏应对计划，该计划提供一个连贯、系统和主动的方式来管理数据隐私泄漏和安全事件，以一致的方式处理个人数据。

7.2. The functions of this data privacy incident or breach response plan are:
7.2.此资料私隐事件或违反应变计划的职能如下:

a) To maintain a breach notification procedure to affected individuals;
对被怀疑的个人维持违反通知程序;

b) To report all data privacy incidents or breaches to regulators, credit agencies, law enforcement authorities, and other external third parties in a timely manner, etc.;
及时向监管机构、信贷机构、执法机关和其他外部第三方报告所有数据隐私事件或违规行为;

c) To maintain logs that record certain details regarding data privacy incidents or breaches for the purpose of achieving compliance with breach notification laws, adhering to industry best practice, and being able to demonstrate such compliance in the event of a lawsuit or other regulatory examination.
维护记录数据隐私事件或违规的某些细节的日志，以实现遵守违规通知法，遵守行业最佳做法，并能够在诉讼或其他监管审查中证明这种遵守。

d) To ensure that data privacy breach notifications and reports align with legal requirements and best practices.
确保数据隐私泄露通知和报告符合法律要求和最佳实践。

e) To monitor, document and report data privacy incident or breach metrics so that the effectiveness of data breach response policies and procedures are evaluated and the board of directors and management are aware of how breaches are being handled and allocate any new needed resources to mitigate the particular risks involved;

监测、记录和报告数据隐私事件或违规指标，以便评估数据违规应对政策和程序的效果，董事会和管理层了解如何处理违规行为，并分配任何新的所需资源，以减轻所涉及的特定风险;

f) To conduct periodic testing of the data privacy incident or breach response plan;

定期测试有关资料私隐事故或违反应变计划;

g) To engage the services of a data privacy breach response remediation provider for services that may be needed to respond to a breach, including provision of: Forensic investigations; Operation of a call center; Breach notiications; Public relations services; Identity theft resolution services, etc.; and

使用数据隐私泄露响应补救服务提供商的服务来应对泄露，包括提供:法医调查;呼叫中心运营;泄露通知;公共关系服务;身份盗窃解决服务等;以及

h) To obtain adequate data privacy breach insurance coverage for the costs associated with a privacy breach, such as mailing notiications and providing credit monitoring or other consumer services to afected individuals, costs of lawsuits, etc.

获得足够的数据隐私保险覆盖与隐私侵犯有关的费用，如邮寄通知和提供信用监测或其他消费者服务给被怀疑的个人，诉讼费用等。

For more details, see ‘Data & IT Plan # 5: Personal Data Breach Incident Response Plan’ in Volume 2.

详情请参阅第二册「资料及资讯科技计划#5:个人资料外泄事故应变计划」。

Phase 4-DP Governance: Products and Outcome

he products and outcome of this phase are:

阶段 4-DP 治理:该阶段的产品和成果及成果如下:

Product 1: Updated data protection and privacy strategy (step 1);
产品一:更新资料保护及私隐策略(第一步);

Product 2: Data protection policy (step 1);
产品 2:数据保护策略(步骤 1);

Product 3: Procedure for Maintaining Data Privacy Notices (step 2);
产品三:维持资料私隐通知的程序(第二步);

Product 4: Requests, Complaints and Rectiication Plan (step 3);
产品 4:要求、投诉和纠正计划(步骤 3);

Product 5: Data Protection Risk Assessment Process (step 4);
产品 5:数据保护风险评估程序(步骤 4);

Product 6: hird-Party Risks Management Plan (step 4);
产品六:税务风险管理计划(第四步);

Product 7: Data Protection and Privacy Report (step 5);
产品七:资料保护及私隐报告(第五步);

Product 8: Data Privacy Documentation (step 6); and
产品 8:资料私隐文件(第 6 步);及

Product 9: Data Privacy Breach Response Plan (step 7);
产品九:资料私隐泄漏应变计划(第七步);

he outcome of Phase 4 is to establish the data protection and privacy governance structures for better data protection and privacy management.
第四阶段的成果是建立数据保护和隐私治理结构，以更好地保护数据和隐私管理。

2.2.5 PHASE 5: DATA PROTECTION AND PRIVACY EVALUATION
2.2.5 阶段 5:数据保护和隐私评估
AND IMPROVEMENT
和改进

Goal and Objectives
目标及宗旨

he general goal of this phase (**Phase 5-DP&P Evaluation and Improvement**) is to evaluate and improve all the speciic data protection and privacy aspects of your corporate environment (controls, measures, policies, procedures, practices, etc.).
这个阶段(第 5 阶段-dp&p 评估和改进)的总体目标是评估和改进公司环境的所有特定数据保护和隐私方面(控制、措施、政策、程序、实践等)。

he more speciic objectives of this phase are: to monitor the operation and resolution of all privacy-related matters; to regularly assess whether your company or organization complies with internal data protection and privacy policies and operational processes; and to improve your data protection and prvacy measures and controls on the basis of internal and external audits and reviews.

这个阶段更具体的目标是:监察所有与私隐有关事宜的运作和解决方法;定期评估贵公司或机构是否遵守内部资料保护及私隐政策和运作程序;以及在内部及外部审核和检讨的基础上，改善你的资料保护及审查措施和控制。

he steps and actions required to be executed to complete this phase are:
为了完成这一阶段的工作，他需要采取以下步骤和行动:

- Step RI#1: Perform Internal Audits of Data Protection and Privacy
  步骤 RI#1:执行数据保护和隐私的内部审计
- Step RI#2: Engage an external party to perform Data Protection and Privacy assessments
  步骤 RI#2:聘请外部人员执行数据保护和隐私评估
- Step RI#3: Perform privacy assessments and benchmarks
  步骤 RI#3:执行隐私评估和基准测试
- Step RI#4: Execute Data Protection Impact Assessments
  步骤 RI#4:执行数据保护影响评估
- Step RI#5: Resolve Data Protection and Privacy (DP&P) Risks
  步骤 RI#5:解决数据保护和隐私(dp&p)风险
- Step RI#6: Report DP&P Risk Analysis and Results
  步骤 RI#6:报告 dp&p 风险分析和结果
- Step RI#7: Monitor Data Privacy Laws and Regulations
  步骤 RI#7:监控数据隐私法律法规

hese are detailed next.
接下来是详细内容。

Phase 5-DP&P Evaluation and Improvement Steps and Actions
第 5 阶段-发展大纲图及计划评估及改善步骤及行动

Step RI#1: Perform Internal Audits of Data Protection and Privacy
步骤 RI#1:执行数据保护和隐私的内部审计

1.1. he Internal Audit department regularly assesses whether the organization complies with internal data protection and privacy policies and operational processes.

1.1.内部审计部门定期评估组织是否遵守内部数据保护和隐私政策及操作流程。

1.2. he results of these privacy audits and assessments inform and guide decisions by the privacy oice to create or update policies, design or adapt procedures, conduct training, or engage in other activities to minimize risk and comply with internal or external privacy requirements.

1.2.这些私隐审核及评估的结果，为私隐办公室制定或更新政策、设计或调整程序、进行培训或从事其他活动的决定提供资料及指引，以尽量减低风险及遵守内部或外部的私隐规定。

1.3. he scope of this privacy audit activity will cover the privacy oice’s role in participating in privacy audits and responding to indings and perform audits on all personal data held in electronic format or contained within a structured manual iling system.

1.3.这项私隐审核活动的范围将包括私隐审核处在参与私隐审核及回应投诉方面所担当的角色，以及审核所有以电子形式持有或载于结构化人工程序系统内的个人资料。

1.4. In particular, but not exclusively, the audit will cover personal data held in the following systems and formats: Computer databases; Document management systems (including documents stored in standard directory structures provided by such facilities); Individual computer iles where appropriate (e.g. spreadsheets and other such analysis tools, word-processed lists, etc.); Structured e-mail directories; Structured manual iling systems that can contain personal data; Web-pages; Photographs; Microiche; Video/audio recordings, etc.

1.4.审计工作将特别但并非专门涵盖以下系统和格式保存的个人资料:电脑数据库;文件管理系统(包括储存在这些设施提供的标准目录结构中的文件);个人电脑文件(例如电子表格和其他这类分析工具、文字处理清单等);结构化电子邮件目录;可包含个人资料的结构化手册系统;网页;照片;微缩文件;录像/录音等。

1.5. he ‘Security and Data Privacy Questionnaires’ in Volume 5 may also be used to complete this audit.

1.5.第五册的「保安及资料私隐问卷」亦可用来完成审核工作。

知识工程的力量。

请访问我们的 www.skf.com/knowledge

Step RI#2: Engage an external party to perform Data Protection and Privacy assessments
步骤 RI#2:聘请外部人员执行数据保护和隐私评估

2.1. The company or organization may request an assessment to be executed by an outside service provider to validate compliance with internal privacy policies and applicable legal requirements.

2.1.公司或组织可要求外部服务供应商进行评估，以确认是否符合内部隐私政策和适用的法律要求。

2.2. The results of these assessments inform, enable and guide decisions by the data protection or privacy office to create or update privacy policies, design or adapt data protection and privacy procedures, conduct privacy training, or engage in other activities to ensure compliance with internal or external privacy requirements.

2.2.这些评估的结果为资料保护或私隐办公室的决定提供信息、支持和指导，以制定或更新私隐政策、设计或调整资料保护和私隐程序、进行私隐培训，或参与其他活动，以确保遵守内部或外部的私隐规定。

Step RI#3: Perform privacy assessments and benchmarks
步骤 RI#3:执行隐私评估和基准测试

1. Ad-hoc privacy assessments
临时私隐评估

1) The Privacy Office has procedures to conduct assessments of business unit compliance with the privacy policies on a periodic, but unannounced basis.

隐私办公室有一套程序，可以定期评估业务单位遵守隐私政策的情况，但不能事先通知。

2) Also after a privacy event (e.g., breach, complaint, inquiry), the Privacy Office has policies and procedures for conducting an ad-hoc assessment of the business unit, product, service, system or process that was the subject of the event for the purpose of: Evaluating privacy compliance; Determining privacy risks; and Identifying any gaps that should be remediated.

此外，在私隐事件(例如违反、投诉、查询)发生后，私隐专员办事处有政策及程序，对事件所涉及的业务单位、产品、服务、系统或程序进行特别评估，目的是:评估遵从私隐的情况;确定私隐风险;以及找出应予弥补的任何空白。

2. Privacy self-assessments
私隐自我评估

1) The company or organization has a procedure for evaluating the privacy practices of individual business units (e.g., customer support, sales and marketing, IT function, etc.) for the purpose of improving the data protection and privacy policies and business practices.

公司或机构有程序评估个别业务单位(例如客户支援、销售及市场推广、资讯科技职能等)的私隐措施，以改善资料保障、私隐政策及业务运作。

2) This procedure may be run by the Privacy function or by the individual business units of the company.

他的程序可以由隐私功能或由公司的个人业务单位运行。

3. Privacy benchmarks

私隐基准

1) The company or organization has implemented a practice to run benchmarks of the results of privacy audits and assessments for various reasons, such as:

公司或机构基于各种原因，实施了私隐审核及评估结果的基准测试，例如:

a) To compare the results against previous audits/assessments to identify improvements or areas that may have deteriorated within the privacy office;

将审核结果与以往的审核/评估作比较，以找出私隐范围内可能有所改善或恶化的地方;

b) To make comparisons across business units regarding privacy compliance; and

对各业务单位的隐私遵从性进行比较;以及

c) To measure the organization's privacy performance against other similar entities.

根据其他类似实体衡量组织的隐私性能。

2) Depending on these benchmark results, the Privacy office improves all aspects of the data protection and privacy practices, policies and procedures of the company.

根据这些基准测试结果，隐私保护协会改进了公司数据保护和隐私实践、政策和程序的所有方面。

Step RI#4 Execute Data Protection Impact Assessments
步骤 RI#4 执行数据保护影响评估

4.1. Initial assessments: Companies and organizations have policies, procedures and practices in place to determine when privacy impact assessments ('PIAs') or data protection impact assessments ('DPIAs') are required as part of the development process for new programs, systems and processes to ensure privacy protections are achieved.
4.1.初步评估:公司和组织制定了政策、程序和做法，以确定何时需要进行隐私影响评估或数据保护影响评估，作为新项目、系统和流程开发过程的一部分，以确保实现隐私保护。

4.2. Changes: Also companies and organizations have the corresponding policies and procedures to follow when operational units propose changes to their existing programs, systems or processes to ensure that data protection and privacy risks are measured, analyzed and privacy-protective alternatives are considered. This process also could rely on the principles of Privacy by Re-Design to ensure privacy and data protection is considered at all points of program, system and process development.
4.2.变化:各公司和组织也有相应的政策和程序，在运营单位提出对其现有方案、系统或流程的变化时可以遵循，以确保数据保护和隐私风险得到衡量、分析和考虑保护隐私的替代办法。他的过程也可以依靠隐私的原则，通过重新设计，以确保隐私和数据保护被考虑在程序，系统和过程开发的所有点。

4.3. Guidelines and templates: Organizations maintain guidelines and templates detailing how to conduct privacy impact assessments ('PIAs') or data protection impact assessments ('DPIAs') for programs, systems and processes to ensure consistency in how data protection risks are measured and analyzed. These PIAs/DPIAs would:
4.3.指导方针和模板:组织维护指导方针和模板，详细说明如何对程序、系统和流程进行隐私影响评估("PIAs")或数据保护影响评估("DPIAs")，以确保数据保护风险的衡量和分析的一致性。这些 pias/dpias 将:

a) Analyze how programs, functions, systems and processes collect, use, share and maintain personal data to ensure conformity to applicable privacy/data protection laws and policies; and
分析程序、功能、系统和程序如何收集、使用、共享和维护个人数据，以确保符合适用的隐私/数据保护法律和政策;以及

b) Determine the risks to personal data inherent in the programs, systems; functions; projects; and processes.
确定程序、系统、功能、项目和过程中固有的个人数据风险。

For more details, see Volume 3: Data Protection Impact Assessment (Chapter 1: Data
有关详情，请参阅第 3 卷:数据保护影响评估(第 1 章:数据)

Protection Impact Pre-Assessment Survey; Chapter 2: Data Protection Impact Risk Assessment;
保护影响预评估调查;第二章:数据保护影响风险评估;
and Chapter 3: Data Protection Risk Resolution Actions).
及第三章:资料保护风险解决行动)。

Step RI#5: Resolve Data Protection and Privacy (DP&P) Risks
步骤 RI#5:解决数据保护和隐私(dp&p)风险

5.1. he privacy impact assessment (‘PIAs’) or data protection impact assessment (‘DPIAs’) need to feed into planning a system’s, process’s or project’s next steps.
5.1.隐私影响评估("PIAs")或数据保护影响评估("DPIAs")需要纳入规划系统、流程或项目的下一步。

5.2. Companies and organizations implement a procedure to:
5.2.公司和组织执行一项程序，以便:

a) Evaluate the issues identiied in the PIA/DPIA;
评估在 pia/dpia 中发现的问题;

b) Assess possible protections and alternative processes to mitigate those data protection risks identiied; and
评估可能的保护措施和替代程序，以减轻已查明的数据保护风险;以及

c) Monitor how the chosen risk mitigation actions are implemented.
监控所选择的风险缓解措施是如何实施的。

For more details, see Volume 3: Data Protection Impact Assessment (Chapter 1: Data
有关详情，请参阅第 3 卷:数据保护影响评估(第 1 章:数据)

Protection Impact Pre-Assessment Survey; Chapter 2: Data Protection Impact Risk Assessment;
保护影响预评估调查;第二章:数据保护影响风险评估;
and Chapter 3: Data Protection Risk Resolution Actions).
及第三章:资料保护风险解决行动)。

Step RI#6: Report DP&P Risk Analysis and Results
步骤 RI#6:报告 dp&p 风险分析和结果

6.1. Companies and organizations report DP&P risk analysis and results to regulators, where required, and stakeholders (customers, employees, privacy advocates, etc.), as appropriate, for several reasons.

6.1.公司和组织将 dp&p 风险分析和结果报告给监管机构(如果需要的话)，以及合适的利益相关者(客户、雇员、隐私倡导者等)，原因有以下几点。

6.2. hese reasons include cases where there are privacy risks that cannot be mitigated by reasonable means by the company, or they might take additional time, etc.

6.2.这些原因包括公司无法通过合理手段减轻隐私风险，或者可能需要更多时间等情况。

6.3. hese reports are issued to the relevant regulator or stakeholders so that these groups are made aware of the attendant data privacy risks prior to the launch of a new privacy product, program, system, process or the relocation of personal data to another jurisdiction, etc.

6.3.在推出新的私隐产品、计划、系统、程序或将个人资料迁移至其他司法管辖区等前，这些团体会知悉随之而来的资料私隐风险。

Step RI#7: Monitor Data Privacy Laws and Regulations
步骤 RI#7:监控数据隐私法律法规

7.1. he company and its Privacy Oice monitors all standards, laws and regulations related to data protection and privacy.

7.1.该公司及其隐私监控所有与数据保护和隐私有关的标准、法律和法规。

7.2. Once aware of a proposed new data protection or privacy standard, law, regulation or code, or amendments to these, it:

7.2.一旦意识到新的数据保护或者隐私标准、法律、法规或者法规，或者这些的修正案，它:

a) Tracks its progress and reports to appropriate stakeholders on the impact the development will have on the organization’s privacy program or business activities that have privacy risks;

跟踪其进展情况，并向相关利益攸关方报告开发对组织隐私项目或具有隐私风险的业务活动的影响;

b) Seeks an opinion from the organization’s legal counsel (internal or external) on the impact these new changes will have on the company’s privacy program or business activities that have privacy risks; and

就这些新变化对公司隐私项目或有隐私风险的商业活动的影响征求公司内部或外部法律顾问的意见;

c) Keeps track of how new developments in these (laws and regulations, etc.) have been handled, including making records of what has been changed and why, as well as documenting decisions to not implement any changes and the rationale behind those decisions.

跟踪如何处理这些(法律和条例等)的新发展，包括记录哪些已经改变和为什么改变，记录不执行任何改变的决定和这些决定背后的理由。

Phase 5-Improvement: Products and Outcome
第五阶段-改善:产品及成果

The products and outcome of this phase are:
这个阶段的产品和结果是:

Product 1: Data protection and privacy internal audit report (step 1);
产品 1:数据保护和隐私内部审计报告(步骤 1);

Product 2: Data protection and privacy eternal audit report (step 2);
产品 2:数据保护和隐私永久审计报告(步骤 2);

Product 3: Ad-hoc privacy assessment report (step 3);
产品三:即席私隐评估报告(第三步);

Product 4: Privacy self-assessment report (step 3);
产品四:私隐自我评估报告(第三步);

Product 5: Privacy benchmark report (step 3);
产品 5:隐私基准报告(步骤 3);

Product 6: Data Protection Impact Assessment report (step 4);
产品 6:数据保护影响评估报告(步骤 4);

Product 7: Data Protection and Privacy Resolved Risks report (step 5);
产品 7:数据保护和隐私解决风险报告(步骤 5);

Product 8: DP&P Risk Analysis and Results report (step 6); and
产品 8:dp&p 风险分析和结果报告(步骤 6);以及

Product 9: Monitoring Privacy Laws Report (step 7);
产品 9:监控隐私法报告(步骤 7);

The outcome of Phase 5 is to audit the data protection and privacy aspects of your enterprise so that you find the gaps and errors in implemented measures and controls related to data protection and privacy and schedule actions to improve them.
第五阶段的成果是审计企业的数据保护和隐私方面，以便找出与数据保护和隐私相关的实施措施和控制中的漏洞和错误，并制定改进措施的时间表。

2.3 CONCLUSION: GOOD PRACTICES
2.3 结论:良好做法

In conclusion, the following good practices to improve your data protection and privacy measures and controls are recommended for your review and consideration and potential implementation after customization to your enterprise's requirements, needs and expectations:
总而言之，我们推荐以下改进数据保护和隐私措施及控制的良好实践，供您在根据企业的需求、需求和期望进行定制之后进行审查、考虑和潜在的实施:

Recommended Good Practice 1: Security
建议的良好做法 1:保安

1.1. Develop an integrated approach to all aspects of information policy and practice for your enterprise systems and data.
1.1.为您的企业系统和数据开发信息策略和实践的所有方面的集成方法。

1.2. Always train your people to follow your security policies and procedures and engage them to report any suspected security breaches.

1.2.始终训练你的员工遵守你的安全政策和程序，并让他们举报任何可疑的数字证书认证机构。

1.3. Set up review procedures for old enterprise business records, based on a policy of destroying business records unless there is a strong reason or regulation (pension, health, etc.) for keeping them.

1.3.建立旧的企业业务记录的审查程序，基于销毁业务记录的政策，除非有强有力的理由或规章(养老金、健康等)来保存它们。

Recommended Good Practice 2: Accuracy of data

推荐的良好做法 2:数据的准确性

2.1. Your people should always give a full explanation on all forms of communication (telephone, paper, on-line, etc.) of why personal data are needed, who is going to use it, what other sources of information may be used and what choice the data subject has.

2.1.你的人员应经常就各种沟通方式(电话、纸张、网上等)作出充分解释，说明为何需要个人资料、谁会使用这些资料、可使用哪些其他资料来源，以及资料当事人有什么选择。

2.2. Your enterprise should use every opportunity to check that a data subject’s contact details are correct (e.g., address, telephone number, email address, etc.).

2.2.您的企业应该利用一切机会检查数据主体的联系方式是否正确(例如，地址、电话号码、电子邮件地址等)。

2.3. Your enterprise responsible officer should also set a schedule for checking other elements of the information held about a data subject according to the likelihood of frequent changes, etc.

2.3.您的企业负责人还应该根据频繁更改的可能性等设置一个时间表，用于检查关于数据主体的其他信息元素。

Recommended Good Practice 3: Authorization

建议的良好做法 3:授权

3.1. Instruct your enterprise people to never share personal information obtained in the course of their employment with anyone unless they have explicit authorization to do so.

3.1.指示你的企业员工，除非得到明确授权，否则绝对不要与任何人分享在工作过程中获得的个人信息。

3.2. Also to always follow security and authorization procedures, particularly when dealing with enquirers about personal data over the telephone.

3.2.此外，要经常遵守保安及授权程序，尤其是在电话联络查询个人资料的人士时。

Recommended Good Practice 4: Managing requests and complaints

建议的良好做法 4:管理请求和投诉

4.1. Your enterprise should set a timetable for dealing with a subject access request and keep a log of each stage.

4.1.您的企业应该为处理主题访问请求设置一个时间表，并保存每个阶段的日志。

4.2. Your enterprise responsible officer should make direct contact with the data subject to establish what information he or she wants and to get any information you need to process the request.

4.2.您的企业负责人应该与数据主体直接联系，以确定他或她需要哪些信息，并获得处理请求所需的任何信息。

4.3. The complaints by the data subjects should be dealt with in accordance with the normal complaints procedure.

4.3.资料当事人的投诉应按正常的投诉程序处理。

3 DATA PROTECTION QUIZ

3 保障资料问答游戏

Overview (link to the Data Protection and Privacy Management System)
概览(连结至资料保护及私隐管理系统)

This chapter provides further details of the actions defined in ‘Step AP# 1: Conduct Privacy Analysis’ of ‘Phase 1-DP Preparation’ of the Data Protection and Privacy Management System (as described in ‘Chapter 2: Data Protection and Privacy Management System’).
本章提供资料保护及私隐管理系统「第一阶段-资料保护及私隐管理系统」的「第一步:进行私隐分析」所采取行动的进一步详情(见「第二章:资料保护及私隐管理系统」)。

Summary
摘要

This chapter contains eleven questionnaires of 166 review questions and answers for a set of data protection-related issues and controls, such as: ICT Organization controls; ICT Administration Controls; IT Personnel Controls; and ICT Strategic Controls, etc.
他的章节包含了 166 个问题的十一份调查问卷，回顾了一系列与数据保护相关的问题和控制，例如:ICT 组织控制;ICT 行政控制;IT 人事控制;和 ICT 战略控制等。

The objective of these are: to enable enterprise managers to identify whether the processing operations of their company can be perceived as potentially risky to the protection of personal data of the individuals so that a full-fledged **Data Protection Impact Assessment** is executed later; and to examine the company’s knowledge-level, culture, awareness and readiness for implementing data protection and privacy measures and controls.
其目标是:使企业管理人员能够确定其公司的处理业务是否可被视为对保护个人的个人数据具有潜在风险，以便随后进行全面的数据保护影响评估;并审查该公司在执行数据保护和隐私措施及控制方面的知识水平、文化、认识和准备情况。

3.1 ICT ORGANIZATION CONTROLS

3.1 信息和通信技术组织控制

1. Question: Which is the purpose of ICT Organization controls?
1.问题:信息和通信技术组织控制的目的是什么？

1. Answer: The purpose of ICT (Information and Communications Technology) Organization Controls is to ensure, enable and facilitate:
答:ICT(信息和通信技术)组织控制的目的是确保、促成和便利:

a) The establishment of the entire I.T. control framework;
建立整个信息技术控制框架;

b) The continuous support of ICT on a formal basis by management (top, middle, lower), and ICTs enforcement with proper policies, standards and procedures, registers, tagging and locks, including internal and external audits;

管理层(高层、中层、低层)持续支持资讯及通讯科技，并透过适当的政策、标准和程序、登记册、标签和锁定，包括内部和外部审计，执行资讯及通讯科技;

c) he management of the input, processing, and output functions of computerized application systems in recording, maintaining and processing the computerized transactions of the organization;

管理计算机化应用系统的输入、处理和输出功能，记录、维护和处理组织的计算机化交易;

d) he developing, management and maintenance of ICT infrastructure and application systems; and

发展、管理及维修资讯及通讯科技基础设施及应用系统;以及

e) he protection and safeguarding of the ICT infrastructure, equipment, facilities and data of the organization.

保护和维护组织的信息和通信技术基础设施、设备、设施和数据。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

2. Question: Which are the main types of ICT Organization controls?
图 2。问题:信息和通信技术组织控制的主要类型有哪些？

2. Answer: The main types of ICT Organization Controls are: ICT Department Functional Description Controls, ICT Strategy Organization Controls, Security Organizational Controls, Monitoring and Review Controls, ICT Control Frameworks, and ICT Organization Performance Measures.
答:信息和通信技术组织控制的主要类型是:信息和通信技术部门职能说明控制、信息和通信技术战略组织控制、安全组织控制、监测和审查控制、信息和通信技术控制框架和信息和通信技术组织绩效措施。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

3. Question: Which are the main ICT Department Functional Description Controls?
图 3。问题:信息和通信技术部门的主要功能描述控制是什么？

3. Answer: The main ICT Department Functional Description Controls are: ICT Department Overall Objectives, ICT Department Overall Terms of Reference, Detail ICT Department Terms of Reference, and ICT Department Job Description Controls.
答:他主要负责信息通信技术部门的职能描述控制:信息通信技术部门的总体目标，信息通信技术部门的总体职权范围，详细的信息通信技术部门职权范围，以及信息通信技术部门的职责描述控制。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

4. Question: Which are the five departments of a typical ICT function?
图 4。问题:典型的 ICT 功能有哪些部门？

4. Answer: A typical ICT function is made up of five departments, namely: ICT management, Information Systems Development, Computer Operations, Technical Support, and ICT Quality Assurance Standards.
答:典型的信息通信技术职能由以下几个部门组成:信息通信技术管理、信息系统开发、计算机操作、技术支持和信息通信技术质量保证标准。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's ________________

______ ______

comments: ________________

5. Question: Which is the primary purpose of the ICT Committee?
5.问题:资讯及通讯科技委员会的主要目的是什么？

5. Answer: he primary purpose of the ICT Committee is to provide guidelines, review, and approve the ICT critical strategic issues (systems, plans, etc.) of the Company.
回答:ICT 委员会的主要目的是提供指导方针，审查和批准公司的 ICT 关键战略问题(系统，计划等)。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s
comments: ________________

6. Question: What is a typical deinition of a values statement for an ICT function?
图 6。问题:信息和通信技术职能的价值说明的典型定义是什么？

6. Answer: he vision and mission of the ICT services will be provided with the highest values of quality, security, integrity of data, and with the most eicient and efective application of corporate and national codes of moral and professional conduct, rules and regulations.
答复:信息和通信技术服务的愿景和使命将具有最高的质量、安全和数据完整性价值，以及最有效和最有效地应用公司和国家道德和专业行为守则、规则和条例。

7. Question: Which roles and responsibilities should be formally assigned for the management and support of ICT security?
问题:应当为信通技术安全的管理和支持正式分配哪些作用和责任？

7. Answer: For the management and support of the ICT security activities of the organization the following roles and responsibilities should be formally assigned: ICT Security Project Manager, Security Test Designer, Security Tester, Security System Test Administrator, and Security System Accounts Administrator.
答:为了管理和支持组织的信息和通信技术安全活动，应正式分配以下角色和职责:信息和通信技术安全项目经理、安全测试设计人员、安全测试人员、安全系统测试管理员和安全系统账户管理员。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

8. Question: What does the review of system logs achieve?
图 8。问题:审查系统日志有什么作用？

8. Answer: A periodic review of system-generated logs can detect security problems, including attempts to exceed access authority or gain system access during unusual hours, detect log clipping, etc.
回答:定期检查系统生成的日志可以检测安全问题，包括在非正常时间尝试超出访问权限或获得系统访问权限，检测日志剪辑等。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

9. Question: How do ICT Organization controls afect the critical issues of the EU Data
问题:ICT 组织如何控制欧盟数据的关键问题

Protection Regulation, such as: Purpose specification; Data limitation; Information and access rights; Legal basis for personal data processing and transfer; Personal data rectification and deletion; Personal data quality and accuracy; Personal data security; Personal data sharing; Personal data retention; and Personal data accountability?
保障规例，例如:目的介绍;资料限制;资料及查阅权利;处理及传送个人资料的法律基础;个人资料的整理及删除;个人资料的质素及准确性;个人资料保安;个人资料共用;个人资料保留;及个人资料问责？

9. Answer: ICT Organization controls form the first crucial component that enables the ICT function to operate effectively and efficiently so that all risks related to these data protection issues are resolved as best as possible for the personal data collected and used by the specific company or organization.

答:信息和通信技术组织的控制是使信息和通信技术职能能够有效运作的第一个关键组成部分，以便尽可能最好地解决与这些数据保护问题有关的所有风险，使专业公司或组织能够收集和使用个人数据。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

3.2 ICT ADMINISTRATION CONTROLS

3.2 资讯及通讯科技行政管理

1. Question: Which is the purpose of ICT Administration controls?
1.问题:资讯及通讯科技管理控制的目的是什么？

1. Answer: he purpose of ICT Administration Controls is to enable and facilitate:
答复:信息和通信技术行政管制的目的是促成和便利:

a) the activities that manage the input, processing, and output functions of computerized application systems in recording, maintaining and processing the computerized transactions of the organization;
管理计算机化应用系统的输入、处理和输出功能，以记录、维护和处理本组织的计算机化交易的活动;

b) he developing, management and maintenance of ICT infrastructure and application systems; and
发展、管理及维修资讯及通讯科技基础设施及应用系统;以及

c) he protection and safeguarding of the ICT infrastructure, equipment, facilities and data of the organization.
保护和维护组织的信息和通信技术基础设施、设备、设施和数据。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

2. Question: Which are the main types of ICT Administration controls?
图 2。问题:资讯及通讯科技管理控制的主要类型有哪些？

2. Answer: he main types of ICT Administration controls are: ICT Standards, Policies and Procedures, ICT Asset Controls, ICT Personnel Management Controls, ICT Personnel Job Descriptions, ICT Purchasing Controls, ICT Management Reporting, and ICT Administration Performance Measures.
答:资讯及通讯科技行政管制的主要类别是:资讯及通讯科技标准、政策及程序、资讯及通讯科技资产管制、资讯及通讯科技人事管理管制、资讯及通讯科技人事职务说明、资讯及通讯科技采购管制、资讯及通讯科技。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

3. Question: What are some of the areas the ICT standards, policies and procedures should cover?
问题:信息和通信技术标准、政策和程序应涵盖哪些领域？

3. Answer: he ICT standards, policies and procedures should cover: the full system development cycle (analysis, development, design, implementation and evaluation), the I.T. strategic process, the ICT security process, the backup and recovery process, the documentation process, the disaster recovery aspects for critical computerized applications, computer availability management, service level management, capacity management, software control and distribution, change management, etc.

答:信息和通信技术标准、政策和程序应涵盖:整个系统开发周期(分析、开发、设计、实施和评价)、信息技术战略过程、信息和通信技术安全过程、备份和恢复过程、文档过程、关键计算机应用程序的灾难恢复方面、计算机可用性管理、服务级别管理、能力管理、软件控制和分发、变更管理等。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

4. Question: What should the ICT asset controls usually include?
图 4。问题:信通技术资产控制通常应包括哪些内容？

4. Answer: The ICT asset controls should usually include: A hardware and software inventory, a consumables inventory, maintenance registers for systems and application software, and hardware, visitors logs (for both offices and computer rooms), hardware locks, and hardware tagging (property labels, serial numbers, etc.).
答:信息和通信技术资产控制通常应包括:硬件和软件库存、消耗品库存、系统和应用软件的维护登记册、硬件、来访者日志(机房和计算机房)、硬件锁和硬件标签(财产标签、序列号等)。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

5. Question: Which are the strategic objectives of the ICT Procurement function?
5.问题:信息和通信技术采购职能的战略目标是什么？

5. Answer: The strategic objectives of the ICT Procurement function are: Fast and effective processing of ICT procurement services, Highest quality in ICT products, solution and services obtained, and Best pricing arrangements.
答:信息和通信技术采购职能的战略目标是:信息和通信技术采购服务的快速有效处理、信息和通信技术产品的最高质量、获得的解决方案和服务以及最佳定价安排。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

With us you
can shape the

6. Question: Which steps is the ICT Procurement Procedure made up of?
图 6。问题:资讯及通讯科技采购程序由哪些步骤组成？

6. Answer: he ICT Procurement Procedure is made up of the following steps:
答:信息和通信技术采购程序由以下步骤组成:

PURCHASE REQUISICTION, MARKET RESEARCH, PROPOSAL EVALUATION, EXPENDICTURE APPROVAL, PLACEMENT OF ORDER, EXPEDICTING & FINAL DELIVERY, and VENDOR PAYMENT
采购申请，市场调查，建议书评估，消耗品批准，订单安排，执行和最终交货，以及卖方付款

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

7. Question: What does project scoping involve?
图 7。问题:项目范围界定包括哪些内容？

7. Answer: Appropriate project scoping involves (a) adequate speciications, well documented, agreed with the end-users and other corporate stakeholders, (b) agreed time-table for implementation, (c) agreed project milestones and deliverables,
答:适当的项目范围界定涉及:(a)充分的专业知识、良好的文件记录、与最终用户和其他公司利益攸关方商定的时间表、(b)商定的实施时间表、(c)商定的项目里程碑和交付成果、

(d) agreed quality standards, (e) agreed and well documented acceptance criteria and procedures, (f) agreed and well documented error correction and resolution procedure, (g) agreed grievance settlement procedure, and (h) top management sponsoring on behalf of the organization.
商定的质量标准、(e)商定和记录完整的验收标准和程序、(f)商定和记录完整的错误纠正和解决程序、(g)商定的冤情解决程序，以及(h)代表组织的最高管理层的赞助。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

8. Question: What items and issues should an ICT management report cover?
图 8。问题:信息和通信技术管理报告应涵盖哪些项目和问题？

8. Answer: he ICT management report should cover: Changes, problems, and backlog of requests, Help Desk related issues, Development issues of new applications, Project actual costs (against budgets), and Post-implementation review issues.

回答:信息和通信技术管理报告应该包括:变化，问题和请求的积压，服务台相关的问题，新应用程序的开发问题，项目实际成本(对照预算)，和实施后的审查问题。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s
comments: ______________

9. Question: How do ICT Administration controls afect the critical issues of the
问题:信息和通信技术管理部门如何控制

EU Data Protection Regulation, such as: Purpose speciication; Data limitation; Information and access rights; Legal basis for personal data processing and transfer; Personal data rectiication and deletion; Personal data quality and accuracy; Personal data security; Personal data sharing; Personal data retention; and Personal data accountability?

欧盟资料保护规例，例如:目的介绍;资料限制;资料及查阅权利;处理及传送个人资料的法律基础;个人资料的整理及删除;个人资料的质素及准确性;个人资料保安;个人资料共用;个人资料保留;及个人资料问责？

9. Answer: ICT Administration Organization controls form the second crucial component that enables the ICT function to operate efectively and eiciently so that all risks related to these data protection issues are resolved as best as possible for the personal data collected and used by the speciic company or organization.

答:信通技术管理组织的控制构成第二个关键组成部分，使信通技术职能能够有效和独立地运作，以便尽可能最好地解决与这些数据保护问题有关的所有风险，使专业公司或组织能够收集和使用个人数据。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

3.3 IT PERSONNEL CONTROLS

3.3 资讯科技人事管制

1. Question: What are the usual ICT personnel management controls?
1.问题:通常的信息和通信技术人事管理控制是什么？

1. Answer: he usual ICT personnel management controls are: Screening, employment contracts and job descriptions, supervision, segregation of duties, rotation of duties, vacation taking and adoption of professional ethical standards.

答:通常的信息和通信技术人员管理控制有:筛选、雇用合同和职务说明、监督、职责分工、轮换、休假和采用职业道德标准。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

2. Question: What should the IT Manager consider in reviewing segregation of duties in the ICT department?

问题:信息技术经理在审查信息和通信技术部门的职责分工时应考虑什么？

2. Answer: he following issues should be considered by the IT Manager in reviewing

回答:IT 经理在审核时应该考虑以下问题

segregation of duties in the ICT department: Responsibility for initiating or authorizing transactions, custody of valuable or moveable assets, amendments to master iles, and correction of input errors, segregation of functions (e.g.: Number of ICT staf, Systems programmers, Application programmers, Database administrator, ICT operations, Data input, Network security, Reliance on key personnel, and Reliance on contract staf), and programming expertise of the users.

信息和通信技术部门的职责分工:负责启动或授权交易，保管有价值或可动资产，修改主文件，纠正输入错误，功能分工(例如:信息和通信技术标准的数量，系统程序员，

应用程序编程人员，应用数据库管理员，信息和通信技术操作，数据输入，网络安全，对关键人员的依赖，以及对合同标准的依赖)，以及用户的编程专长。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

3. Question: Why is rotation of duties important?
图 3。问题:为什么职责轮换很重要？

3. Answer: Rotation of duties, done periodically, prevents personnel from becoming bored and vulnerable to fraud, abuse and system tampering as a form of challenge.
回答:职责轮换，定期进行，防止人员变得无聊和易受欺诈，滥用和系统篡改作为一种挑战形式。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

4. Question: Who should develop and ratify ICT personnel job descriptions?
图 4。问题:谁应该制定和批准信息和通信技术人员的职务说明？

4. Answer: ICT personnel job descriptions should be developed by the ICT committee and ratified by the board.
答:信息和通信技术人员的职务说明应由信息和通信技术委员会制定，并由董事会批准。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

5. Question: Which are the main (summary) responsibilities of the Chief Information Officer (CIO)?
问题:首席信息官(CIO)的主要(总结)职责是什么？

5. Answer: The CIO will lead the organization in planning and implementing enterprise information systems to support both distributed and centralized production and business operations and achieve more effective and cost beneficial enterprise-wide ICT operations.
答:首席信息干事将领导组织规划和实施企业信息系统，以支持分散和集中的生产和业务运作，并实现更有成效和成本效益的全企业信通技术运作。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

6. Question: Which are the main responsibilities of a business system analyst?
图 6。问题:业务系统分析师的主要职责是什么？

6. Answer: The main responsibilities of a business systems analyst are: (a) Study the overall business and information needs of the organization, in order to develop solutions to business and related ICT technology problems (b) Work closely with users to identify business needs and the costs and benefits of implementing computerized solutions, (c) Build information technology (ICT) definitions based on identified needs of the organisation, and (d) Work with other ICT experts to address application software and hardware needs of the organization.
答:业务系统分析员的主要职责是:(a)研究组织的整体业务和信息需求，以便为业务和相关的信息和通信技术问题制定解决方案;(b)与用户密切合作，确定实施计算机化解决方案的业务需求和成本及利益;(c)根据组织的明确需求建立信息和通信技术设施;(d)与其他信息和通信技术专家合作，解决组织的应用软件和硬件需求。

Is reply satisfactory? or NO

YES ______ ______

Reviewer's comments: ________________

7. Question: Which are some of the main responsibilities of a computer programmer?
问题:程序员的主要职责是什么？

7. Answer: Some of the main responsibilities of a computer programmer are:
答:程序员的一些主要职责是:

a) Perform a variety of programming assignments requiring knowledge of established programming procedures and data processing requirements,
执行各种编程任务，要求熟悉既定的编程程序和数据处理要求,

b) Code, test, maintain, modify and troubleshoot programs utilizing the appropriate hardware, database, and programming technology , and
利用适当的硬件、数据库和编程技术对程序进行编码、测试、维护、修改和故障排除

c) Make approved changes by amending flow charts, etc.
通过修改低位图表等获得批准的更改。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ______________

8. Question: Which are some of the main responsibilities of a system programmer?
图 8。问题:系统程序员的主要职责是什么？

8. Answer: Some of the main responsibilities of a system programmer are: (a) Provide system-level support of multi-user operating systems, hardware and software tools, including installation, configuration, maintenance, and support of these systems,
答:系统程序员的一些主要职责是:(a)为多用户操作系统、硬件和软件工具提供系统级支持，包括安装、配置、维护和支持这些系统

(b) Identify alternatives for optimizing computer and network resources, (c) Research, plan, install, configure, troubleshoot, maintain and upgrade operating systems, network and data base software, etc.
(b)确定优化计算机和网络资源的替代方案，(c)研究、计划、安装、调试、故障排除、维护和升级操作系统、网络和数据库软件等。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ______________

9. Question: What does the 'Security Test Designer' do?
图 9。问题:"安全性测试设计器"是做什么的？

9. Answer: The Security Test Designer produces, categorizes and files security test scenaria.
答:安全测试设计器生产、分类和编写安全测试场景。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s
comments: ________________

10. Question: What does the ‘Security Tester’ do?
图 10。问题:"安全测试人员"是做什么的？

10. Answer: he Security Tester executes security test scenaria, documents the results and documents any required changes.
答:安全测试人员执行安全测试场景，记录测试结果并记录所需的任何更改。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s
comments: ________________

11. Question: How do IT Personnel controls afect the critical issues of the EU Data
问题:IT 人员如何控制欧盟数据的关键问题

Protection Regulation, such as: Purpose speciication; Data limitation; Information and access rights; Legal basis for personal data processing and transfer; Personal data rectiication and deletion; Personal data quality and accuracy; Personal data security; Personal data sharing; Personal data retention; and Personal data accountability?
保障规例，例如:目的介绍;资料限制;资料及查阅权利;处理及传送个人资料的法律基础;个人资料的整理及删除;个人资料的质素及准确性;个人资料保安;个人资料共用;个人资料保留;及个人资料问责？

11. Answer: IT Personnel controls form the third crucial component that enables the ICT function to operate efectively and eiciently so that all risks related to these data protection issues are resolved as best as possible for the personal data collected and used by the speciic company or organization.
答:信息技术人员控制构成了第三个关键组成部分，使信息和通信技术职能能够有效和独立地运作，以便尽可能最好地解决与这些数据保护问题有关的所有风险，使专业公司或组织能够收集和使用个人数据。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ______________

3.4 ICT STRATEGIC CONTROLS

3.4 资讯及通讯科技策略控制

1. Question: What is the purpose of ICT Strategic Controls?
1.问题:信息和通信技术战略控制的目的是什么？

1. Answer: he purpose of ICT Strategic Controls is to deine and establish the future ICT vision and mission for the for the ICT eforts (infrastructure and systems) of the organization and prepare the whole ICT environment to accommodate such requirements and needs of the ICT systems of the organization.
答:信息和通信技术战略控制的目的是为本组织的信息和通信技术要塞(基础设施和系统)制定和确立未来的信息和通信技术愿景和任务，并为满足本组织信息和通信技术系统的这些要求和需要而准备整个信息和通信技术环境。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ______________

2. Question: Which are the main types of ICT Strategic Controls?
图 2。问题:信息和通信技术战略控制的主要类型有哪些？

2. Answer: The main types of ICT Strategic Controls are: ICT Strategy Organization Controls, ICT Strategic Process Controls, ICT Strategy Implementation and MonICToring Controls, and ICT Strategic Performance Management Controls.

答:主要的信息和通信技术战略控制类型是:信息和通信技术战略组织控制、信息和通信技术战略过程控制、信息和通信技术战略执行和监测控制以及信息和通信技术战略性能管理控制。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

3. Question: What is the primary purpose of the Information Technology (ICT) Committee?
问题:资讯及通讯科技委员会的主要目的是什么？

3. Answer: he primary purpose of the ICT Committee is to provide guidelines, review, and approve the ICT crICTical strategic issues (systems, plans, etc.) of the Company.
答:信息技术委员会的主要职责是提供指导方针，审查和批准公司的信息技术战略问题(系统、计划等)。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s comments: ______________

4. Question: Who develops and ratiies the Information Technology (ICT) Policy?
图 4。问题:谁发展和推行资讯及通讯科技政策？

4. Answer: Developing the ICT policy should be done by the ICT committee and ratiied by the board.
答:制定信息和通信技术政策应由信息和通信技术委员会负责，并由委员会批准。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s comments: ______________

5. Question: How is a typical ‘ICT Mission Statement’ described?
5.问题:如何描述典型的"信通技术任务说明"？

5. Answer: he mission of the department is to manage the eicient low of data and electronic information throughout the organization as well as to and from external (customers), parties (banks, vendors, suppliers, etc.) and government authorICTies and regulatory agencies.
答:部门的任务是管理整个组织内部以及与外部(客户)、各方(银行、供应商、供应商等)和政府部门及监管机构之间的数据和电子信息的流通。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s comments: ______________

6. Question: What are the main steps of the ICT strategic process?
图 6。问题:信息和通信技术战略进程的主要步骤是什么？

6. Answer: The main steps of the ICT strategic process are: Getting Ready, Articulating Mission and Vision, Assessing the existing organizational context and current ICT systems and infrastructure, Developing ICT Strategies, Goals, and Objectives, Defining the future I.T. architecture and data to support the business environment of the organization, and completing the written action plan, Implementing the ICT Strategy, and Evaluating the ICT Strategy (at least annually).

答:信息和通信技术战略进程的主要步骤是:做好准备，阐明任务和愿景，评估现有的组织环境和当前的信息和通信技术系统和基础设施，制定信息和通信技术战略、目标和目的，规划未来的信息和通信技术架构和数据，以支持组织的业务环境，完成书面行动计划，执行信息和通信技术战略，以及评价信息和通信技术战略(至少每年一次)。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s comments: ________________

7. Question: Which are some of the objectives of the ICT strategic plan?
图 7。问题:信通技术战略计划的一些目标是什么？

7. Answer: Some of the objectives of the ICT Strategic Plan are: Align information systems with the competitive strategy of the enterprise to enhance the company's performance, ensure that ICT delivers efective solutions to business problems, make certain that ICT provides strategic advantage to company through cost or price beneits, innovation, value to products or services ofered, target the customer, supplier, and competitor needs, and accurately target the corporate success factors to achieve, through the use of ICT, the given business objectives.

答:信息和通信技术战略计划的一些目标是:使信息系统与企业的竞争战略保持一致，以提高公司的业绩;确保信息和通信技术为企业提供有效的业务问题解决方案;确保信息和通信技术通过成本或价格收益、创新、产品或服务的价值为企业提供战略优势;针对客户、供应商和竞争对手的需求，并通过使用信息和通信技术准确定位企业的成功因素，以实现既定的业务目标。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

8. Question: How is monitoring the implementation of the ICT Strategic Plan carried out?
问题:如何监测信息和通信技术战略计划的执行情况？

8. Answer: Monitoring the actual detail implementation of the ICT strategic plan must be done by the ICT corporate committee, or the functional managers or a combination of both, sometimes with external support, overviewed by the Chief Executive Oicer, and ratiied by the board.

答:监测信通技术战略计划的实际细节执行情况必须由信通技术公司委员会或职能管理人员或两者结合进行，有时得到外部支持，由首席执行官监督，并由董事会批准。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

9. Question: Why is a strategic commitment for ongoing information management and data quality required?
问题:为什么需要对持续的信息管理和数据质量作出战略承诺？

9. Answer: A strategic commitment to continuous ongoing information management and data quality is required because an organization's data, due to changes in the

internal and external environment, quickly becomes incorrect or invalid as incorrect or contaminated data reach mission-critical business applications.

答:需要对持续不断的信息管理和数据质量作出战略承诺，因为由于内部和外部环境的变化，一个组织的数据很快就会变得不正确或无效，因为不正确或受污染的数据送达关键任务的业务应用程序。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

10. Question: Which are the three major phases of a typical data quality improvement methodology?
问题:典型的数据质量改进方法的三个主要阶段是什么？

10. Answer: The three major phases of a typical data quality improvement methodology
答:他提出了三个主要阶段的典型数据质量改进方法

are: analyze the problem, fix the problem, and control the problem.
分析问题，解决问题，控制问题。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

11. Question: How do ICT Strategic controls affect the critical issues of the EU Data
问题:ICT 战略控制如何影响欧盟数据的关键问题

Protection Regulation, such as: Purpose specification; Data limitation; Information and access rights; Legal basis for personal data processing and transfer; Personal data rectification and deletion; Personal data quality and accuracy; Personal data security; Personal data sharing; Personal data retention; and Personal data accountability?
保障规例，例如:目的介绍;资料限制;资料及查阅权利;处理及传送个人资料的法律基础;个人资料的整理及删除;个人资料的质素及准确性;个人资料保安;个人资料共用;个人资料保留;及个人资料问责？

11. Answer: ICT Strategic controls form the fourth crucial component that enables the ICT function to operate effectively and efficiently so that all risks related to these data protection issues are resolved as best as possible for the personal data collected and used by the specific company or organization.
答:信息和通信技术战略控制构成第四个关键组成部分，使信息和通信技术职能能够有效和独立地运作，以便尽可能最好地解决与这些数据保护问题有关的所有风险，使专业公司或组织能够收集和使用个人数据。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

3.5 SYSTEM DEVELOPMENT CONTROLS

3.5 系统开发控制

1. Question: What is the purpose of system development controls?
1.问题:系统开发控制的目的是什么？

1. Answer: The purpose of system development controls is to ensure the safe and secure development of computerized information systems and the protection from harm or

other potential damage of the organization’s information and data maintained by these systems.

答:系统开发控制的目的是确保计算机化信息系统的安全可靠开发，以及保护这些系统所维护的组织信息和数据不受损害或其他潜在损害。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s
comments: ________________

2. Question: Which are the main types of system development controls?
图 2。问题:系统开发控制的主要类型是什么？

2. Answer: he main types of system development controls are: Application Development Controls, IT Systems Testing Methodology, End User Application Development Controls, Audit Trails, Software Package Controls, System Development Quality Controls, and System Development Performance Measures.
答:系统开发控制的主要类型是:应用程序开发控制、IT 系统测试方法、最终用户应用程序开发控制、审计跟踪、软件包控制、系统开发质量控制和系统开发性能测量。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ____________

3. Question: Which are the major stages of a typical IT systems development project?
图 3。问题:典型的 IT 系统开发项目的主要阶段是什么？

3. Answer: A typical IT Systems Development Project can be divided into seven major
答:一个典型的 IT 系统开发项目可以分为七大类

stages: IT Project Proposal, IT Project Initiation, IT Project Planning, IT Project Execution, IT Project Management, IT Project Termination, and IT Project Closure.
阶段:IT 项目建议书、IT 项目启动、IT 项目计划、IT 项目执行、IT 项目管理、IT 项目终止及 IT 项目结束。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ____________

4. Question: Which are the usual system development products?
图 4。问题:通常的系统开发产品是什么？

4. Answer: he usual system development products are: Feasibility Study, Systems Analysis, Systems Design, Software Code, and Application Documentation.
答:他通常的系统开发产品是:可行性研究、系统分析、系统设计、软件代码和应用程序文档。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ____________

5. Question: Which are the main contents of the IT system feasibility document?
5.问题:IT 系统可行性文件的主要内容是什么？

5. Answer: he main contents of the IT system feasibility document are: Executive summary, problem description, solution speciications, feasibility, I.T. system development plan, recommendations and appendices.

答:IT 系统可行性文件的主要内容有:执行摘要、问题描述、解决方案说明、可行性、IT 系统开发计划、建议和附录。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

6. Question: What are the main steps to create the systems analysis and design document?
图 6。问:创建系统分析和设计文档的主要步骤是什么？

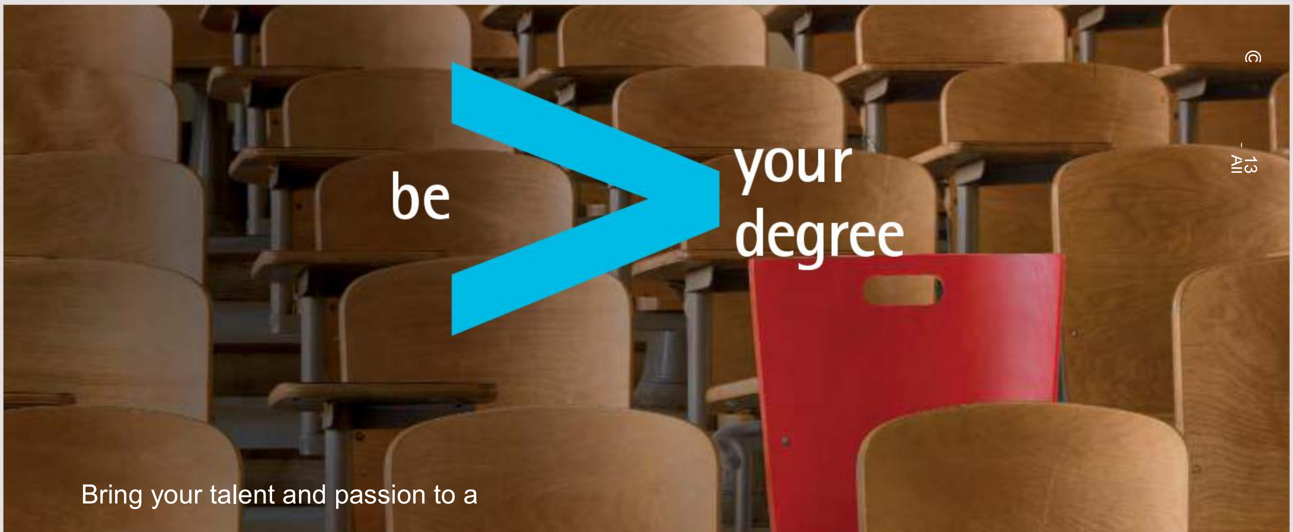
6. Answer: he main steps to create the systems analysis and design document are: gathering the user needs, extracting the requirements from the existing information systems, deriving the requirements from the business functions, describing the future “logical” and “physical” system, documenting the data volumes, the interfaces, and the outputs and the control requirements of the system.
答:创建系统分析和设计文档的主要步骤是:收集用户需求，从现有信息系统中提取需求，从业务功能中得出需求，描述未来的"逻辑"和"物理"系统，记录系统的数据量、接口、输出和控制需求。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s comments: ________________

7. Question: Which are the main contents of the systems analysis and design document?
图 7。问题:系统分析和设计文档的主要内容是什么？

7. Answer: he main contents of the systems analysis and design document are: Executive summary, systems analysis and design summary, user requirements of the proposed system, future “logical” system description, future “physical” system description, system constraints, programming phase budget, and appendices.
答:系统分析和设计文件的主要内容有:执行摘要、系统分析和设计摘要、拟议系统的用户要求、未来"逻辑"系统描述、未来"物理"系统描述、系统约束、编程阶段预算和附录。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s comments: ________________



8. Question: Which are the contents of end user documentation?
图 8。问题:最终用户文档的内容是什么？

8. Answer: he contents of end user documentation are: Application description, procedures for completing source documents, input screens, and how to do manual and automated processing, description of manual and computerized iles, data and report descriptions, explanation of controls, error handling instructions and procedures for distributing output data and reports.
答:最终用户文件的内容有:应用说明，完成原始文件的程序，输入屏幕，以及如何进行人工和自动处理，手工和计算机文件的说明，数据和报告说明，控制说明，错误处理指示和分发输出数据和报告的程序。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s
comments: ________________

9. Question: Which basis should be used for testing an IT system?
图 9。问题:测试资讯科技系统应采用哪个基准？

9. Answer: Testing an IT system should be performed on the basis of an IT testing standard and methodology, an IT application test plan, and a set of testing tools.
答:测试 IT 系统应该基于 IT 测试标准和方法、IT 应用程序测试计划和一组测试工具进行。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s
comments: ________________

10. Question: Which are the contents of a typical application test plan?
图 10。问题:典型应用程序测试计划的内容是什么？

10. Answer: he contents of a typical application test plan are: Testing strategy, detailed testing design plan for each unit, clear deinition of testing responsibilities and organization, components to be tested, expected deliverables of tests, formalized test procedures, test cases and test data, and post implementation review details.
答:典型应用程序测试计划的内容包括:测试策略、每个单元的详细测试设计计划、明确的测试职责和组织、待测试的组成部分、测试的预期交付成果、形式化的测试程序、测试用例和测试数据，以及实施后评审细节。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s
comments: ________________

11. Question: Which data ields should a test case execution log form include?
图 11。问题:测试用例执行日志表单应该包括哪些数据场？

11. Answer
回答

he test case execution log form should include data, such as: Test case number, project, tester name, date, pass/fail comment, actual results (for fail), error log number (for fail) and approval.
测试用例执行日志表单应该包括数据，例如:测试用例编号、项目、测试人员名称、日期、通过/失败注释、实际结果(失败)、错误日志编号(失败)和批准。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ______________

12. Question: Which is the main purpose of end user application development controls?
图 12。问题:最终用户应用程序开发控制的主要目的是什么？

12. Answer: The main purpose of end user application development controls is to ensure that the end users, especially when they are using personal computers to do their daily business tasks, are protected from harm, damage and errors.

答:最终用户应用程序开发控制的主要目的是确保最终用户，尤其是当他们使用个人电脑完成日常业务任务时，免受伤害、损害和错误的侵害。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

13. Question: What is the definition of an end-user?
图 13。问题:最终用户的需求是什么？

13. Answer: An end-user is any person who interacts directly with a computer or a network system. This includes both those persons who are authorized to interact with the system and those people who interact without authorization. Note that "end-users" do not include "operators," "system programmers," "technical control officers," "system security officers," and other system support personnel.

最终用户是指任何直接与计算机或网络系统进行交互的人。其中既包括那些被授权与系统互动的人，也包括那些未经授权互动的人。请注意,"最终用户"不包括"操作员"、"系统程序员"、"技术控制员"、"系统安全员"和其他系统支持人员。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

14. Question: What are the usual spreadsheet applications controls?
图 14。问题:通常的电子表格应用程序控制什么？

14. Answer: The usual spreadsheet applications controls are: standard spreadsheet design template for all spreadsheets of the organization, testing rules and strategies for each spreadsheet used, documentation for each spreadsheet, and complete list of spreadsheets used for management decision making.

回答:他通常的电子表格应用程序控制是:组织所有电子表格的标准电子表格设计模板，每个电子表格的测试规则和策略，每个电子表格的文档，以及用于管理决策的完整电子表格列表。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's ________________

comments: ______________

15. Question: Which are the various Audit trail types?
图 15。问题:各种审计跟踪类型有哪些？

15. Answer: The various Audit trail types are: System software and hardware logs, application journal logs for updating data bases and classical files, security monitoring logs for network traffic, etc.
答:各种审计跟踪类型有:系统软硬件日志、用于更新数据库和经典文件的应用日志日志、网络传输的安全监控日志等。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s
comments: ______________

16. Question: What are the minimum contents of an Audit trail record?
图 16。问题:审计跟踪记录的最小内容是什么？

16. Answer: The minimum contents of an Audit trail record are: Type of event, when the event or transaction occurred (time and day), user id associated with the event or transaction, program or command used to initiate the event or transaction, copy of the transaction, and copy of the database record before and after the update process.
答:审计跟踪记录的最小内容是:事件类型、事件或事务发生的时间和日期、与事件或事务相关的用户 id、用于启动事件或事务的程序或命令、事务的副本以及更新过程前后的数据库记录的副本。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s
comments: ______________

17. Question: Which are the main objectives of software package controls?
图 17。问题:软件包控制的主要目标是什么？

17. Answer: The main objective of software package controls is to ensure that software packages to serve business applications are selected on the basis of approved pre-defined standards and to prevent the potential case of fraud and misuse of resources in the purchase process.
答:软件包控制的主要目的是确保服务于商业应用程序的软件包是根据已批准的事先确定的标准选择的，并防止在采购过程中可能发生欺诈和滥用资源的情况。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s
comments: ______________

18. Question: Which are the main controls for software package purchases?
图 18。问题:软件包购买的主要控制是什么？

18. Answer: The main controls for software package purchases are: Project plan, feasibility study, evaluation of vendor proposals, business requirements document, technical ICT requirements document, and post-Implementation review.
回答:软件包采购的主要控制是:项目计划、可行性研究、供应商提案评估、业务需求文件、技术 ICT 需求文件和实施后评审。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s
comments: ______________

19. Question: What is included in the dimension of ‘integrity’ of the system development quality controls?

问题:系统开发质量控制的"完整性"维度包括什么？

19. Answer: he dimension of ‘integrity’ of the system development quality controls

答:系统开发质量控制的"完整性"维度

includes: he inputs, processes, interactions, processing rules, logical conditions, and information presentations of the said information system, so that it is designed and executed in a systemic way so as to minimize the possibility of human and machine errors, and produce, always, the same results.

信息系统包括:信息系统的输入、过程、交互、处理规则、逻辑条件和信息表示，以便系统地设计和执行信息系统，从而最大限度地减少人机错误的可能性，并始终产生相同的结果。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s comments: ________________

20. Question: Which are some of the usual system development performance measures?
图 20。问:哪些是通常的系统开发性能度量？

20. Answer: Some of the usual system development performance measures are: Delivered lines of code, development time per application, average time to deliver an application, no. of listed requirements not delivered on time, % of users satisied with the delivered application, % of users trained in new application, etc.
答:一些常见的系统开发性能指标是:交付的代码行数、每个应用程序的开发时间、交付应用程序的平均时间、没有。未按时交付所列要求的百分比、对交付的应用程序满意的百分比、受过新应用程序培训的百分比等。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ______________

21. Question: How do System Development controls afect the critical issues of the
问题:系统开发如何控制

EU Data Protection Regulation, such as: Purpose speciication; Data limitation; Information and access rights; Legal basis for personal data processing and transfer; Personal data rectiication and deletion; Personal data quality and accuracy; Personal data security; Personal data sharing; Personal data retention; and Personal data accountability?
欧盟资料保护规例，例如:目的介绍;资料限制;资料及查阅权利;处理及传送个人资料的法律基础;个人资料的整理及删除;个人资料的质素及准确性;个人资料保安;个人资料共用;个人资料保留;及个人资料问责？

21. Answer: System Development controls form the ifth crucial component that enables the ICT function to develop, maintain and operate systems, efectively and eiciently, so that all risks related to these data protection issues are resolved as best as possible for the personal data collected and used by the speciic company or organization.
答:系统开发控制是使信息和通信技术部门能够有效地开发、维护和操作系统的关键组成部分，以便尽可能最好地解决与这些数据保护问题有关的所有风险，使专业公司或组织能够收集和使用个人数据。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ______________

3.6 ICT SECURITY CONTROLS

3.6 资讯及通讯科技保安控制

1. Question: What is the purpose of ICT Security controls?
1.问题:资讯及通讯科技保安管制的目的为何？

1. Answer: he purpose of ICT security controls is to ensure that all I.T. assets, systems, networks, facilities, hardware, media, data and iles are protected against unauthorized access, potential damage and improper or illegal use, and that they are operable, safe and secure at all times.

答:信息和通信技术安全控制的目的是确保所有信息技术资产、系统、网络、设施、硬件、媒体、数据和文件不受未经授权的访问、潜在的损害、不当或非法使用的影响，并确保它们在任何时候都是可操作的、安全和可靠的。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s
comments: ________________

2. Question: How is ICT security achieved?
图 2。问题:如何实现信息和通信技术安全？

2. Answer: ICT security is achieved by implementing a suitable set of measures and controls, which may include policies, practices, procedures, organizational structures and software systems and functions.
答:信通技术安全是通过实施一套适当的措施和控制来实现的，这些措施和控制可能包括政策、做法、程序、组织结构以及软件系统和功能。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

3. Question: Which are the main types of ICT security controls?
图 3。问题:信息和通信技术安全控制的主要类型有哪些？

3. Answer: he main types of ICT Security Controls are: ICT Security Policies and Plans, Computer Operations Controls, Personnel Security Management Controls, End User Security Administration Controls, Password Controls, ICT Technical Protection Controls, Other Management Controls, and ICT Security Performance Measures.
答:资讯及通讯科技保安控制的主要类别是:资讯及通讯科技保安政策及计划、电脑运作控制、人事保安管理控制、最终用户保安管理控制、密码控制、资讯及通讯科技技术保安控制、其他管理控制及资讯及通讯科技保安表现措施。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

4. Question: Which are the usual ICT Security Policies and Plans?
图 4。问题:通常的信息和通信技术安全政策和计划是什么？

4. Answer: he usual ICT Security Policies and Plans are: ICT Security Policy, Privacy of Information Policy, Information Sensitivity Policy, ICT Security Management Plan, and System Development Security Plan.
答:他通常的 ICT 安全政策和计划是:ICT 安全政策，信息隐私政策，信息敏感度安全政策，ICT 安全管理计划，系统开发安全计划。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

5. Question: What should the ICT Security Policy cover?
5.问题:资讯及通讯科技保安政策应涵盖甚么？

5. Answer: he ICT Security Policy should cover: Access control standards, Accountability, Audit trails, Backups, Business Continuity Planning, Disposal of Media, Disposal of printed matter, Downloading from the Internet, Information Ownership, Management responsibilities, Modems and Analog Lines, Of-Site Repairs to Equipment, Physical Security, Portable Devices, Staf Responsibilities, Use of E-Mail, Viruses, Workstation Security, Privacy, Noncompliance, Legislation, etc.
答:信息和通信技术安全政策应包括:访问控制标准，责任，审计跟踪，备份，商业连续性，媒体处理，印刷品处理，从互联网下载，信息所有权，管理责任，调制解调器和模拟线路，设备的现场维修，物理安全，便携式设备，国家责任，电子邮件的使用，病毒，工作站安全，隐私，不遵守，立法等。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

6. Question: What is the primary purpose of the Privacy of Information Policy?
图 6。问题:资讯保密政策的主要目的是什么？

6. Answer: The primary purpose of the Privacy of Information Policy is to provide guidelines for the privacy issues of information activities (collection, use, disclosure, monitoring, etc.) of the organization.
答:信息隐私政策的主要目的是为组织的信息活动(收集、使用、披露、监控等)的隐私问题提供指导方针。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ______________

7. Question: What is the purpose of the Information Sensitivity Policy?
图 7。问:信息敏感度货币政策的目的是什么？

7. Answer: The purpose of the Information Sensitivity Policy is to help employees determine what data and information can be disclosed to non-employees, as well as the relative Sensitivity of data and information that should not be disclosed outside of the organization without proper authorization.
答:信息敏感度政策的目的是帮助员工决定哪些数据和信息可以向非员工披露，以及数据和信息的相对敏感性，这些数据和信息在未经适当授权的情况下不应在组织外披露。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ______________

8. Question: Which major actions should the ICT Security Management Plan include?
图 8。问题:信息和通信技术安全管理计划应包括哪些主要行动？

8. Answer: The major actions that an ICT Security Management Plan should include
答复:信息和通信技术安全管理计划应包括的主要行动

are: Establishment of the I.T. security management steering committee, formulation of the ICT security strategy, examining the various options and deciding on the security model of the organization, establishment and implementation of security policies and procedures, establishment of the I.T. security organization, etc.
设立资讯科技保安管理指导委员会、制订资讯科技保安策略、研究各种方案及决定组织的保安模式、制订及执行保安政策及程序、设立资讯科技保安组织等。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ______________

9. Question: What is a ‘cookie’?

9. Answer: A cookie is a piece of information that is stored on a personal computer hard drive and which records the navigation of a website by a user so that, when the user revisits that website, it can present tailored options to him or her, based upon the stored information about his or her last visit.

答:cookie 是一种存储在个人电脑硬盘上的信息，它记录了用户浏览网站的过程，当用户再次访问该网站时，它可以根据用户最近一次访问的信息，向用户提供量身定制的选项。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s comments: ________________

10. Question: Which are the main activities of a computer security awareness and training program?
问题:计算机安全意识和培训计划的主要活动是什么？

10. Answer: The main activities of a computer security awareness and training program
答:他的主要活动是一个计算机安全意识和培训方案

are: Identify security awareness and training program scope, set goals and objectives, identify training staff, identify target audiences, motivate management and employees, administer the program, maintain the program, and evaluate the program.
确定安全意识和培训项目范围，设定目标和目的，确定培训阶段，确定目标受众，激励管理层和员工，管理项目，维护项目，评估项目。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

11. Question: Which is the primary objective of the System Development Security Plan?
图 11。问题:系统开发保安计划的主要目标是什么？

11. Answer: The primary objective of the System Development Security Plan is to provide guidelines for security issues for all phases of an IT system development life cycle for the information systems implemented in an organization.
答:系统开发安全计划的主要目标是为组织中实施的信息系统的 IT 系统开发生命周期的所有阶段提供安全问题的指导方针。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

12. Question: What does separation or segregation of duties mean in an IT function?
图 12。问题:在 IT 职能中，职责的分离或隔离意味着什么？

12. Answer: Separation or segregation of duties refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process. For example, in IT systems, the system programmer should not write application software and should not have access, without explicit authorization, to production data. The operators also should not be allowed to maintain application software, etc.
回答:分离或职责分离指的是划分角色和职责，以便单个个人不能颠覆一个关键过程。例如，在 IT 系统中，系统程序员不应该编写应用软件，并且在没有明确授权的情况下不应该访问生产数据。操作人员也不得维护应用软件等。

Is reply satisfactory?
YES or NO

______ ______

Reviewer's comments: ________________

13. Question: What steps does the process of end user account management include?
图 13。问题:最终用户帐户管理流程包括哪些步骤？

13. Answer: he end user account management process includes: requesting, establishing, issuing, and closing user accounts, tracking users and their respective access authorizations, and managing these functions.
答:最终用户帐户管理过程包括:请求、建立、发布和关闭用户帐户，跟踪用户及其各自的访问授权，以及管理这些功能。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

14. Question: What does ‘friendly termination’ of end users include?
图 14。问题:最终用户的友好终止包括什么？

14. Answer: Friendly terminations of end users includes: (a) removal of access privileges, computer accounts, and authentication tokens, (b) the control of keys, (c) the brieing on the continuing responsibilities for conidentiality and privacy, (d) return of property, and (e) documenting where the data are stored on the hard disk, iles, systems or media, and how they are backed up.

答:最终用户的友好终止包括:(a)取消访问权限、计算机帐户和认证令牌;(b)密钥控制;(c)继续承担保密和隐私责任的授权;(d)归还财产;(e)记录数据存储在硬盘、文件夹、系统或媒体上的位置，以及如何备份这些数据。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s comments: ______________

15. Question: What is the reason why the password must not contain dictionary words from any language?
问:为什么密码不能包含任何语言的字典词汇？

15. Answer: he password must not contain dictionary words from any language because numerous password-cracking programs exist that can run through millions of possible word combinations in seconds.

答:密码不能包含来自任何语言的字典单词，因为存在大量破解密码的程序，可以在几秒钟内运行数百万个可能的单词组合。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s comments: ______________

16. Question: How should default passwords be controlled for system, data base software and standard packages?
问题:如何控制系统、数据库软件和标准软件包的默认密码？

16. Answer: Default passwords for operating systems, systems software, and other systems (data base, data communications, etc.) should be changed to ‘strong’ passwords to minimize the high risk of compromise as these are sometimes installed with a standard set of default accounts and associated very easy to break standard passwords.

答:操作系统、系统软件和其他系统(数据库、数据通信等)的默认密码应该更改为"强"密码，以尽量减少泄露的高风险，因为这些密码有时会安装一组标准的默认帐户，并且很容易破解标准密码。

Is reply satisfactory? or NO

YES ______ ______
Reviewer's
comments: ________________

17. Question: How often should a password change?
图 17。问题:密码多久更改一次？

17. Answer: he passwords should be changed every 30, 60, or 90 days, etc., depending on the time limit set by the speciic organization.
答:密码应该每 30 天、60 天或 90 天更换一次，具体时间取决于专业机构设置的时限。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

18. Question: How can a computer security incident result?
图 18。问题:电脑保安事故如何导致？

18. Answer: A computer security incident can result from a computer virus, other malicious code (e.g. malware), or a system intruder, either from inside or outside of the organization.
答:电脑保安事故可能由电脑病毒、其他恶意程式码(例如恶意程式码)或系统入侵者所引致，不论是来自机构内部或外部。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ______________

19. Question: Which are some of the hardware and software mechanisms for implementing security at the technical level?
问题:在技术层面实现安全性的一些硬件和软件机制是什么？

19. Answer: Some hardware and software mechanisms for implementing security at the
答:一些硬件和软件机制用于在

technical level are: Firewalls, Virtual Private Networks, DMZ, IDS/IPS systems, Web site content filtering, gateway antivirus, Email Server, DNS, VLAN, BACKUP lines, WEB URL filtering, URL keyword blocking, data base management system security parameters setting, Database password profiles, digital certificates, honey pots and honey nets, etc.
技术层次包括:防火墙、虚拟专用网络、DMZ、ids/ips 系统、网站内容分类、网关防病毒、电子邮件服务器、DNS、VLAN、备份线路、WebURL 分类、URL 关键字封锁、数据库管理系统安全参数设置、数据库密码保护、数字证书、蜜罐和蜜网等。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ______________

20. Question: Which are some of the usual ICT Security Performance Measures?
图 20。问题:通常的资讯及通讯科技保安表现措施有哪些？

20. Answer: Some of the usual ICT Security Performance Measures are: Number and types of incidents, number and types of violations, number and types of viruses eliminated, number of developed and deployed systems where security requirements were not met, etc.
答:通常的信息和通信技术安全性能计量包括:事件的数量和类型、违规的数量和类型、消除的病毒的数量和类型、开发和部署的系统中未满足安全要求的数量等。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

21. Question: How do ICT Security controls afect the critical issues of the EU Data
问题:信息和通信技术安全控制如何影响欧盟数据的关键问题

Protection Regulation, such as: Purpose speciication; Data limitation; Information and access rights; Legal basis for personal data processing and transfer; Personal data rectiication and deletion; Personal data quality and accuracy; Personal data security; Personal data sharing; Personal data retention; and Personal data accountability?
保障规例，例如:目的介绍;资料限制;资料及查阅权利;处理及传送个人资料的法律基础;个人资料的整理及删除;个人资料的质素及准确性;个人资料保安;个人资料共用;个人资料保留;及个人资料问责？

21. Answer: ICT Security controls form the sixth crucial component that enables the IT function to operate systems, software and networks efectively and eiciently so that all risks related to these data protection issues are resolved as best as possible for the personal data collected and used by the speciic company or organization.
答:信息和通信技术安全控制是第六个关键组成部分，它使信息技术职能能够有效和安全地操作系统、软件和网络，以便尽可能最好地解决与这些数据保护问题有关的所有风险，使专业公司或组织能够收集和使用个人数据。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s comments: ____________

3.7 DATA CENTER OPERATIONAL CONTROLS

3.7 数据中心操作控制

1. Question: What is the purpose of Data Center operational controls?
1.问题:数据中心操作控制的目的是什么？

1. Answer: ICT operational controls ensure that the facilities and equipment can remain in good operational status, and ensure the safe and successful operation of the ICT infrastructure and systems for serving the business purposes of the organization.

答:信通技术业务控制确保设施和设备保持良好的运行状态，并确保为本组织的业务目的服务的信通技术基础设施和系统的安全和成功运行。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

2. Question: Which are the main data centre controls?
图 2。问题:主要的数据中心控制是什么？

2. Answer: he main data centre controls in this area are: Environmental Controls, Fire Security Controls, Radiation Prevention Controls, Emergency Power Controls, Data Centre Physical Access Controls, Failure of Supporting Utilities, Structural Collapse, Data Centre Infrastructure Controls, Operations Personnel Controls, Hardware and Software Maintenance Controls, Surveillance and Eavesdropping Detection Controls, and Daily Activities Controls.

答:这个领域的主要数据中心控制是:环境控制，消防安全控制，辐射防护控制，紧急电源控制，数据中心物理访问控制，支持设施故障，结构倒塌，数据中心基础设施控制，操作人员控制，硬件和软件维护控制，监视和窃听探测控制，以及日常活动控制。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

3. Question: What is the role of radiation prevention controls of computer equipment, wiring, and computer rooms?
问:计算机设备、线路和机房的辐射防护控制起什么作用？

3. Answer: Computer equipment, the wiring and computer rooms themselves should be shielded to contain the radiation emanated by computers in order to avoid some external party from picking up all the critical communications and data transmitted from a distance from the data center.

答:计算机设备、线路和计算机房本身应该屏蔽，以防止计算机发出的辐射，从而避免某些外部部分接收到从数据中心远距离传输的所有关键通信和数据。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

4. Question: What types of utility failures will cause service interruptions?
图 4。问题:什么类型的公用事业故障会导致服务中断？

4. Answer: Failures of electric power, heating and air-conditioning systems, water, sewage, and other utilities will usually cause a service interruption and may damage hardware.
答:电力、供暖和空调系统、水、污水和其他设施的故障通常会造成服务中断，并可能损坏硬件。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s
comments: ______________

5. Question: Which usual elements and actions are included in data center infrastructure controls?
问题:数据中心基础设施控件中包含哪些通常的元素和操作？

5. Answer: he usual elements and actions of data center infrastructure controls
答:数据中心基础设施控件的常用元素和动作

include: Spare circuit boards and components for UPS units, Checking of electrical circuits (once a year), Locating equipment not under sprinkler heads or water pipes, Storing of extra computer motherboards, disks and controllers, Testing the fuel levels of standby generators (once every six months), Testing of smoke detectors (once a year), etc.
包括:UPS 单元的备用电路板和元件、检查电路(每年一次)、定位不在洒水头或水管下的设备、储存额外的电脑主板、磁盘和控制器、测试备用发电机的燃料水平(每六个月一次)、测试烟雾探测器(每年一次)等。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s
comments: ______________

6. Question: Which are the three routes of data interception?
图 6。问题:数据截获的三种途径是什么？

6. Answer: here are three routes of data interception: direct observation, interception of data transmission, and electromagnetic interception.
答:这里有 3 种截取数据的途径:直接观测、截取数据传输和电磁截取。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s
comments: ______________

7. Question: Which are the main daily activities controls?
图 7。问题:哪些是主要的日常活动控制？

7. Answer: he main daily activities controls are: Visitors log, daily work activities log, problem log, computer jobs schedule.
答:他主要的日常活动控制有:访客日志、日常工作活动日志、问题日志、计算机作业日程表。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ______________

8. Question: What data should be recorded in an IT visitors Log?
图 8。问题:IT 访问者日志中应该记录哪些数据？

8. Answer: he following data should be recorded on a standard form designed by
答:他以下的数据应该记录在一个标准的形式设计

the organization: <date of entry>, <time of entry>, <date of exit>, <time of exit>, <location visited>, <visitor's particulars (name, identiication no., etc.), <escort's name and phone no.>, <visitor's signature>, and <escort's signature>.
机构名称:入境日期、入境时间、出境日期、出境时间、到访地点、访客资料(姓名、身份证号码等)、陪同人员姓名及电话号码，访客的签名，和护卫的签名。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

9. Question: What is the objective of hardware controls?
图 9。问:硬件控制的目标是什么？

9. Answer: he objective of hardware controls is to use the components of the computer hardware itself in order to protect the computerized application systems from unwanted, abrupt and not scheduled shut-downs.
答:硬件控制的目的是使用计算机硬件本身的组成部分，以保护计算机化的应用系统免受不必要的、突然的和计划外的关闭。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

10. Question: Which are some of the contents of a personal computers policy?
图 10。问:个人电脑政策的一些内容是什么？

10. Answer: Some of the contents of personal computers policy are: Terms of acceptable use of personal computers, use of personal computers for personal reasons, access to various unethical or illegal web sites, access to personal "friendship" type social networks, iling of electronic messages, committing the organization via the use of e-mail messages, use of passwords for daily access to personal computers, etc.
答:个人计算机政策的一些内容是:个人计算机的可接受使用条款、出于个人原因使用个人计算机、访问各种不道德或非法的网站、访问个人"友谊"类型的社交网络、隐藏电子信息、通过使用电子邮件信息向该组织作出承诺、每天使用密码访问个人计算机等。

Is reply satisfactory?
YES or NO

Reviewer’s comments: ________________

11. Question: Which are some safe operation tips for personal computers?
图 11。问题:个人电脑的安全使用贴士有哪些？

11. Answer: A list of safe operation tips for personal computers includes: Turn of personal computer, Do not share any passwords, Maintain currency of anti-virus software, Maintain currency of operating system and application software, Protect System Administrator account, and Lock personal computer upon leaving.
答:个人电脑安全操作提示清单包括:转动个人电脑、不共享任何密码、维护防毒软件的货币、维护操作系统和应用软件的货币、保护个人系统管理员帐户、离开时锁定个人电脑。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s comments: ________________

12. Question: Which are some of the usual ICT Operational Performance Measures?
图 12。问题:通常的信息和通信技术业务绩效衡量标准有哪些？

12. Answer: Some of the usual ICT Operational Performance Measures are: Online response time, number of pages printed, number of operational hours, number of idle hours, number of transactions processed, etc.
答:一些通常的信息和通信技术业务绩效指标是:在线响应时间、打印页数、运行时数、空闲时数、处理的交易数等。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s comments: ________________

13. Question: How do Data Center operational controls affect the critical issues of the
问题:数据中心操作控制如何影响

EU Data Protection Regulation, such as: Purpose specification; Data limitation; Information and access rights; Legal basis for personal data processing and transfer; Personal data rectification and deletion; Personal data quality and accuracy; Personal data security; Personal data sharing; Personal data retention; and Personal data accountability?
欧盟资料保护规例，例如:目的介绍;资料限制;资料及查阅权利;处理及传送个人资料的法律基础;个人资料的整理及删除;个人资料的质素及准确性;个人资料保安;个人资料共用;个人资料保留;及个人资料问责？

13. Answer: Data Center operational controls form the seventh crucial component that enables the ICT function to operate systems and networks effectively and efficiently so that all risks related to these data protection issues are resolved as best as possible for the personal data collected and used by the specific company or organization.
答:数据中心业务控制是第七个关键组成部分，它使信通技术职能能够有效和安全地操作系统和网络，以便尽可能最好地解决与这些数据保护问题有关的所有风险，使专业公司或组织能够收集和使用个人数据。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s comments: ________________

3.8 IT CONTINGENCY PLANNING AND DISASTER RECOVERY CONTROLS

3.8 资讯科技应变计划及灾后复原控制

1. Question: How is IT Resilience defined?
1.问题:IT 韧性如何受到影响？

1. Answer: IT resilience is an organization’s ability to maintain acceptable service levels, regardless of the service disruptions, hardware failures, natural disasters, malicious attacks, operator or other errors that may be caused.

答:IT 弹性是一个组织维持可接受的服务水平的能力，不管服务中断、硬件故障、自然灾害、恶意攻击、操作员或其他可能引起的错误。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s
comments: ________________

2. Question: Which is the purpose of controls in the area of I.T. Contingency Planning?
图 2。问:信息技术应急计划领域的控制目的是什么？

2. Answer: The purpose of controls in the area of I.T. Contingency Planning and Disaster recovery is to ensure that critical I.T. assets, such as data center facilities, computer hardware, operating system and database management system software, telecommunications lines, application systems (software and data), etc., can be recovered within a pre-defined time frame in order to resume critical business operations after a disaster.

答:it 应急计划和灾难恢复领域控制的目的是确保关键的 it 资产，如数据中心设施、计算机硬件、操作系统和数据库管理系统软件、电信线路、应用系统(软件和数据)等，能够在预先设定的时间框架内恢复，以便在灾难后恢复关键的业务运作。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s
comments: ________________

3. Question: How is a ‘disaster’ defined in ICT terms?
图 3。问题:如何用信息和通信技术术语来描述"灾难"？

3. Answer: A disaster is deemed to be a disruption to normal ICT operations due to
答:灾害被认为是由于以下原因而对正常的信通技术业务造成的干扰:

various events, malfunctions, omissions and errors to: Buildings (fire, flood, storm, other weather conditions, etc., electrical power, telephony (PBX), networking systems, equipment, availability of personnel, information systems, computer hardware and software, business functions, documentation and supplies (forms, consumables, etc.), and technology (manufacturer, software developments, etc.).

各种事件、故障、遗漏和错误:建筑物(fire、flood、storm、其他天气状况等)、电力、电话(PBX)、网络系统、设备、人员可用性、信息系统、计算机硬件和软件、业务功能、文件和用品(表格、消耗品等)，以及技术(制造商、软件开发等)。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s
comments: ________________

4. Question: What is a definition of the term ‘hot site’ in terms of disaster recovery?
图 4。问:就灾难恢复而言,"热点"一词的定义是什么？

4. Answer: A ‘hot site’ is a fully operational disaster recovery center completely equipped with hardware, software, communications and on-site technical support personnel. This is a contingency alterative that may be used to recover from disaster,

depending on the organization’s needs and requirements for resuming its business operations based on I.T. systems.

答:"热点"是一个全面运作的灾难恢复中心，完全配备了硬件、软件、通信和现场技术支持人员。这是一个可能用于从灾难中恢复的应急替代方案，取决于组织恢复基于 it 系统的业务运营的需求和要求。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s
comments: ________________

5. Question: What is a deinition of the term ‘cold site’ in terms of disaster recovery?
5.问:就灾难恢复而言,"冷场"一词的定义是什么？

5. Answer: A ‘cold site’ is a contingency alternative to recovering from disaster, depending on the needs of the organization. A cold site facility is wired and set up to operate computer and peripheral equipment supplied by the organization recovering ICTs I.T. Systems.

答:根据组织的需要，冷场是从灾难中恢复过来的一种应急替代方案。一个冷站设施是有线的，用于操作该组织提供的计算机和外部设备，恢复信息通信技术系统。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s
comments: ________________

6. Question: What is a deinition of the term ‘warm site’ in terms of disaster recovery?
图 6。问:就灾难恢复而言,"温暖场所"这个术语的定义是什么？

6. Answer: A ‘warm site’ is a contingency alternative to recovering form disaster, depending on the needs of the organization. A warm site is set up in such a way, as to facilitate the remote processing of the I.T. Systems of the organization under recovery, at the recovery site.

答:根据组织的需要,"温暖场所"是从灾难中恢复过来的一种应急替代方案。一个温暖的站点以这样的方式设置，以便于远程处理恢复中的组织的 it 系统，在恢复站点。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s
comments: ________________

7. Question: What is a deinition of the term ‘dual data centre’ in terms of disaster recovery?
图 7。问题:"双重数据中心"一词在灾难恢复方面的定义是什么？

7. Answer: A ‘dual data centre’ is a contingency alternative to recovering from disaster, depending on the needs of the organization. A dual data center is set up in such a way as to always have available a fully functioning data center at a safe distance from the primary data center.

答:根据组织的需要,"双重数据中心"是从灾难中恢复的一种应急备选方案。双重数据中心的设置方式是，始终在与主数据中心保持安全距离的情况下拥有一个功能齐全的数据中心。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s
comments: ________________

8. Question: How do IT Contingency Planning and Disaster Recovery Controls
问题:如何进行 IT 应急计划和灾难恢复控制

afect the critical issues of the EU Data Protection Regulation, such as: Purpose speciication; Data limitation; Information and access rights; Legal basis for personal data processing and transfer; Personal data rectiication and deletion; Personal data quality and accuracy; Personal data security; Personal data sharing; Personal data retention; and Personal data accountability?

解决欧盟资料保护规例的关键问题，例如:目的性传播;资料限制;资料及查阅权利;处理及传送个人资料的法律基础;个人资料的处理及删除;个人资料的质素及准确性;个人资料保安;个人资料共用;个人资料保留;及个人资料问责？

8. Answer: IT Contingency Planning and Disaster Recovery Controls form the eighth crucial component that enables the ICT function to plan for emergencies and recover systems when a disaster occurs so that all risks related to these data protection issues are resolved as best as possible for the personal data collected and used by the speciic company or organization.

答:信息技术应急规划和灾后恢复控制是第八个关键组成部分，使信息和通信技术职能能够在发生灾害时规划应急和恢复系统，以便尽可能最好地解决与这些数据保护问题有关的所有风险，使专业公司或组织能够收集和使用个人数据。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

3.9 SYSTEMS SOFTWARE CONTROLS

3.9 系统软件控制

1. Question: Which components is a typical Web (Internet) Application made up of?
1.问:典型的 Web(Internet)应用程序由哪些组件组成？

1. Answer: A typical Web (Internet) Application System is made up of several
答:一个典型的 Web(Internet)应用系统由几个部分组成

components, such as: Web clients (hardware and software) transport mechanisms (communications software, telecommunications lines, HTTP software), Web servers (hardware and software), Web applications (business software), and Data Base Repositories (corporate internal and external data).

组件，例如:Web 客户机(硬件和软件)传输机制(通信软件、电信线路、HTTP 软件)、Web 服务器(硬件和软件)、Web 应用程序(业务软件)和数据库(公司内部和外部数据)。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

2. Question: What do systems software controls ensure?
图 2。问题:系统软件控制确保什么？

2. Answer: Systems software controls ensure that the operating system, data base and data communications software can remain in good operational status, and ensure the safe and successful operation of the ICT infrastructure and systems for serving the business purposes of the organization.
答:系统软件控制确保操作系统、数据库和数据通信软件保持良好的运行状态，并确保为本组织业务目的服务的信通技术基础设施和系统的安全和成功运行。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

3. Question: Which are the main types of systems software controls?
图 3。问题:系统软件控制的主要类型是什么？

3. Answer: he main types of systems software controls are: Systems Software Controls, Data Base Controls, Data Communications Controls, Audit Trail Controls, and Change Management Controls.

答:系统软件控制的主要类型有:系统软件控制、数据库控制、数据通信控制、审计跟踪控制和变更管理控制。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

4. Question: Which is the main purpose of systems software controls?
图 4。问题:系统软件控制的主要目的是什么？

4. Answer: he main purpose of systems software controls is to ensure that the operating system, the data communications software, the data base management system software, the utilities of the operating system, the libraries containing system, database, application and network software, the security iles, the various control iles, and whatever other components are needed for the safe and secure operation of the data centre and the computerized applications running in it are in full productive status.

答:系统软件控制的主要目的是确保操作系统、数据通信软件、数据库管理系统软件、操作系统的实用程序、包含系统、数据库、应用程序和网络软件的图书馆、安全文件、各种控制文件以及任何其他组件都处于充分生产状态，以保证数据中心的安全和可靠运行。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

5. Question: What actions are required to manage the changes to system software supplied by system software suppliers?
问题:需要采取什么行动来管理系统软件供应商提供的系统软件的更改？

5. Answer: he actions required to manage system software suppliers are: Authorizing all systems software changes, documenting all changes, testing all changes before they are moved to production, keeping a log of all changes, backing up the complete system software and ICTs environment before the changes are implemented, and having a recovery plan prepared in case the implemented changes create errors and problems when they are moved to the production environment.

答:管理系统软件供应商所需采取的行动是:批准所有系统软件更改，记录所有更改，在转移到生产环境之前测试所有更改，保存所有更改的日志，在更改实施之前备份完整的系统软件和 ict 环境，并准备一份恢复计划，以防所实施的更改在转移到生产环境时产生错误和问题。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

6. Question: Which forms are used for documenting systems software changes by systems programming person?

问题:系统编程人员使用哪些表格来记录系统软件更改？

6. Answer: The forms are used for documenting systems software changes by systems

答案:他的表格是用来记录系统软件的变化

programming personnel are: Systems software change installation control form, systems software installation authorization form, systems software review procedure control form, and systems software emergency update form.

编程人员有:系统软件变更安装控制表、系统软件安装授权表、系统软件评审程序控制表、系统软件应急更新表。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

7. Question: What is the objective of controls in the Data Base area?

图 7。问题:数据库区域中控件的目标是什么？

7. Answer: The objective of controls in the area of Data Base is to protect all resources of the data base system (application software, data base management system software, data dictionary, data bases and users) from potential harm or damage, and to keep them in excellent operational mode and of the highest quality and integrity.

答:数据库领域的控制目标是保护数据库系统的所有资源(应用软件、数据库管理系统软件、数据字典、数据库和用户)不受潜在的危害或损害，并保持其优良的运行模式和最高的质量和完整性。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

8. Question: Which are the main data base controls?

图 8。问题:哪些是主要的数据库控件？

8. Answer: The main data base controls are: Data custodian, data owner, data privacy officer, data base administration, data dictionary controls, data base integrity checking, Audit trail, data base testing controls, and data base purging.

答:主要的数据库控制有:数据监管、数据所有者、数据隐私保护者、数据库管理、数据字典控制、数据库完整性检查、审计跟踪、数据库测试控制和数据库清理。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

9. Question: What is the responsibility of an appointed Data base Administrator?
图 9。问题:指定的数据库管理员的职责是什么？

9. Answer: he responsibility of an appointed Data base Administrator (DBA) will
答:由指定的数据库管理员(DBA)负责

include: Controlling the subschema of the data base, implementing access controls to individual programs updating the organizational data bases, maintaining the integrity of the data base environment, implementing the data ownership and data deletion procedures, especially on common data laying down and monitoring data documentation standards, setting up and maintaining the data dictionary, and setting standards of data backup and recovery.
包括:控制数据库的子模式，对个别程序实施访问控制，更新组织数据库，保持数据库环境的完整性，实施数据所有权和数据删除程序，特别是在通用数据编制和监控数据文档标准方面，建立和维护数据字典，以及制定数据备份和恢复标准。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

10. Question: Which are the main actions of a data base purging operation?
图 10。问题:数据库清除操作的主要作用是什么？

10. Answer: All purging operations should be authorized by the data owners, reported to the board, logged in a formal register, and the pertinent iles copied before the purging operation is carried out.
答:所有的清洗操作都应该由数据拥有者授权，向董事会报告，在正式的登记簿中登记，并在清洗操作执行之前复制相关的文件。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

11. Question: Which is the objective of data communications controls?
图 11。问题:数据通信控制的目标是什么？

11. Answer: he objective of data communications controls is to protect all resources of online system (network servers and software, application software, data communications software, transmitted data and network users) from potential harm or damage, and to keep them in excellent operational mode and of the highest quality.
答:数据通信控制的目的是保护在线系统的所有资源(网络服务器和软件、应用软件、数据通信软件、传输数据和网络用户)不受潜在的危害或损害，并使它们处于优良的运行模式和最高的质量。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

12. Question: Which are the main data communications controls?
图 12。问题:哪些是主要的数据通信控制？

12. Answer: he main data communications are: Data Communications Management Plan, Network Cryptographic controls, Communications security controls, Firewalls, Wireless Networks Controls, Eavesdropping Controls, Signal Controls, Masquerading Controls, Web Administrator Segregation of Duties, Login Controls, Penetration Tests, Network Segregation, Intrusion Detection System, and Specialized Security Application.
答:他的主要数据通信是:数据通信管理计划，网络加密控制，通信安全控制，防火墙，无线网络控制，窃听控制，信号控制，伪装控制，网络管理员职责分离，登录控制，渗透测试，网络分离，入侵预防系统，和专门的安全应用。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

13. Question: Which are the main network cryptographic controls?
图 13。问题:哪些是主要的网络加密控制？

13. Answer: he main network cryptographic controls are: Encryption, hashing, digital signatures and digital certiicates.
答:主要的网络加密控制有:加密、散列、数字签名和数字认证。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

14. Question: What is a irewall?

14. Answer: A irewall can consist of an application that you install on your PC or server, or it can be a dedicated hardware appliance that protects an entire enterprise network, or it can be both a hardware and a software system that protects from intrusions.
答:irewall 可以是你安装在 PC 或服务器上的应用程序，也可以是保护整个企业网络的专用硬件设备，也可以是保护免受入侵的硬件和软件系统。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

15. Question: How are networks segregated?
图 15。问题:网络是如何隔离的？

15. Answer: Networks are segregated by adding additional layers of irewalls, honeypot diversion devices and other trapping mechanisms.

答:通过增加防火墙、蜜罐转移装置和其他诱捕机制的附加层来隔离网络。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

16. Question: What do Audit trails do?
图 16。问题:审计跟踪是做什么的？

16. Answer: Audit trails maintain a record of system (operating system, data base management system, data communications system, firewall, IDS, WEB, etc.) activity by system or application process and by user activity.
答:审计跟踪按系统或应用程序和用户活动维护系统(操作系统、数据库管理系统、数据通信系统、firewall、IDS、WEB 等)活动的记录。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

17. Question: Which are the minimum contents of Audit trail records?
图 17。问题:审计跟踪记录的最小内容是什么？

17. Answer: The minimum contents of Audit trail records are: Type of event, When the event or transaction occurred (time and day), User ID associated with the event or transaction, Program or command used to initiate the event or transaction, Copy of the transaction, and Copy of the database record before and after the update process.
答:审计跟踪记录的最小内容是:事件类型、事件或事务发生时间(时间和日期)、与事件或事务相关的用户 ID、用于启动事件或事务的程序或命令、事务的副本以及更新过程前后的数据库记录的副本。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

18. Question: What is the purpose of systems software change management controls?
图 18。问题:系统软件变更管理控制的目的是什么？

18. Answer: The purpose of systems software change management controls is to describe the procedures that must be followed for the request, approval, initiation, implementation and testing of changes in existing system software, data base management systems and data communications software systems.
答:系统软件变更管理控制的目的是说明要求、批准、启动、实施和测试现有系统软件、数据库管理系统和数据通信软件系统的变更时必须遵循的程序。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

19. Question: How do Systems Software controls affect the critical issues of the EU Data

问题:系统软件控制如何影响欧盟数据的关键问题

Protection Regulation, such as: Purpose specification; Data limitation; Information and access rights; Legal basis for personal data processing and transfer; Personal data rectification and deletion; Personal data quality and accuracy; Personal data security; Personal data sharing; Personal data retention; and Personal data accountability?

保障规例，例如:目的介绍;资料限制;资料及查阅权利;处理及传送个人资料的法律基础;个人资料的整理及删除;个人资料的质素及准确性;个人资料保安;个人资料共用;个人资料保留;及个人资料问责？

19. Answer: Systems Software controls form the ninth crucial component that enables the ICT function to operate application systems and networks effectively and efficiently so that all risks related to these data protection issues are resolved as best as possible for the personal data collected and used by the specific company or organization.

答:系统软件控制构成第九个关键组成部分，使信通技术职能能够有效和安全地操作应用系统和网络，以便尽可能最好地解决与这些数据保护问题有关的所有风险，使专业公司或组织能够收集和使用个人数据。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ______________

3.10 COMPUTERIZED APPLICATION CONTROLS

3.10 电脑化应用程式控制

1. Question: Which is the main purpose of computerized application controls?

问题:计算机应用程序控制的主要目的是什么？

2. Answer: The main purpose of computerized application controls is to ensure that the computer programs of a particular computerized application process the business transactions according to a set of predefined rules and store the processed data in computerized files, and data bases, in a safe and secure way.

答:计算机应用控制的主要目的是确保特定计算机应用程序的计算机程序按照一套预先制定的规则处理业务交易，并以安全可靠的方式将处理后的数据存储在计算机文件夹和数据库中。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

3. Question: Which are the main types of computerized application controls?

图 3。问题:计算机化应用程序控制的主要类型有哪些？

2. Answer: The main types of computerized application controls typically include: Input controls, processing controls, output controls, database controls, change controls, and testing controls.

答:计算机化应用程序控制的主要类型通常包括:输入控制、处理控制、输出控制、数据库控制、变更控制和测试控制。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

3. Question: Why are computerized application controls built into the computer software of the specific application?

问题:为什么计算机化的应用控制内置到计算机软件的专业应用？

3. Answer: Computerized application controls are mainly built into the computer software of the specific application to prevent and deter crime and potential fraud and to minimize if not eliminate errors. Also they are instituted outside the given application at the entry and exit points of the system.

答:计算机应用程序控制主要内置在计算机软件的特殊应用程序，以防止和阻止犯罪和潜在的欺诈，并尽量减少甚至消除错误。此外，在特定申请之外，在系统的出入境点实行这些制度。

Is reply satisfactory? or NO

YES ______ ______
Reviewer's
comments: ______________

4. Question: What do input controls of computerized application controls ensure?
图 4。问题:计算机应用程序控制的输入控制保证了什么？

4. Answer: Input controls ensure accuracy of data, completeness of input and validation of input.
答:输入控件确保数据的准确性、输入的完整性和输入的有效性。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ______________

5. Question: Which are some checks written into the software code to ensure validation of input?
问题:在软件代码中写入了哪些检查以确保输入的有效性？

5. Answer: In order to ensure validation of input, information systems developers usually write software code in the system developed to perform a variety of checks, such as: Format checks, reasonableness checks, and code checks.
答:为了确保输入的有效性，信息系统开发人员通常在开发的系统中编写软件代码来执行各种检查，例如:格式检查、合理性检查和代码检查。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s
comments: ____________

6. Question: Which are some of the checks and tests included in processing controls?
图 6。问题:处理控件中包含哪些检查和测试？

6. Answer: Some of the checks and tests included in processing controls are: Crossfooting tests, reasonableness checks, functional checks, rounding of checks, parity checks, and sequence checks.
答:处理控制中包含的一些检查和测试有:错位检查、合理性检查、功能检查、舍入检查、奇偶检查和序列检查。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s
comments: ____________

7. Question: What do ‘reasonableness checks’ do?
图 7。问题:合理性检查是做什么的？

7. Answer: Reasonableness checks compare processed data to a set of pre-deined values or against an upper or lower limit before updating the corporate data base. For example, computer salary deductions should not be greater than 50% of gross salary.
答:在更新公司数据库之前，合理性检查将处理过的数据与一组预先设定的值或与上限或下限进行比较。例如，计算机工资扣除不应大于工资总额的 50%。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s
comments: ____________

8. Question: What is the main objective of output controls?
图 8。问题:输出控制的主要目标是什么？

8. Answer: he main objective of output controls is to authenticate all the other controls, i.e., to ensure that only authorized transactions are processed correctly and that reports, screens and other output (e.g. magnetic media) are of the highest quality, complete and available only to authorized personnel.

答:输出控制的主要目的是核实所有其他控制措施，即确保只有获授权的交易得到正确处理，并确保报告、屏幕和其他输出(例如磁性媒体)的质量最高，完整无缺，只供获授权人员使用。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s
comments: ______________

9. Question: What do output controls include?
图 9。问题:输出控制包括什么？

9. Answer: Output controls include: Schedule checks, distribution checks, balancing checks, report quality checks, and output log.
答:输出控制包括:计划检查、分配检查、平衡检查、报告质量检查和输出日志。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ______________

10. Question: What do report quality checks ensure and in what terms?
图 10。问题:报告质量检查确保什么?以什么条件确保？

10. Answer: Report quality checks ensure that all printed output is of the highest
回答:报告质量检查确保所有打印输出是最高的

quality, in terms of: timely (available when needed), complete (includes the stated user needs), concise (does not include elements not required by the users), relevant (is directly relevant to the situation), accurate (has no errors), precise (ofers exact and quantitative information), and appropriate in form (with the correct level of detail, tabular versus graphics, etc., and as pre-deined report quality guidelines).
质量，在以下方面:及时(有需要时提供)、完整(包括说明的用户需求)、简洁(不包括用户不要求的元素)、相关(与情况直接相关)、准确(没有错误)、精确(准确和定量信息)、形式适当(具有正确的细节水平、表格与图形等，以及作为预先制定的报告质量指南)。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ______________

11. Question: What do database controls include?
图 11。问题:数据库控件包括什么？

11. Answer: Database controls include: File updated report, critical transactions report, application-speciic access authorization, application-speciic backup and recovery, application Audit trails, and data base health checks.
答:数据库控制包括:文件更新报告、关键事务报告、应用程序专用访问授权、应用程序专用备份和恢复、应用程序审计跟踪和数据库健康检查。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ______________

12. Question: What do database health checks involve?
图 12。问题:数据库健康检查包括哪些内容？

12. Answer: Data base health checks involve writing and executing software code to read all records in application classical files and data bases and navigate all the paths of the tree or other structure of the databases, and printing a summary report with details of what records, data and figures exist in the files and the databases.

答:数据库健康检查包括编写和执行软件代码，读取应用程序中的所有经典文档和数据库中的所有记录，浏览树的所有路径或数据库的其他结构，以及打印一份摘要报告，详细说明文档和数据库中存在哪些记录、数据和语言。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

13. Question: What is the main objective of change controls?
图 13。问题:变更控制的主要目标是什么？

13. Answer: The main objective of change controls is to safeguard the integrity of the computerized application system by establishing standard procedures for making modification to the system.
答:变更控制的主要目的是通过建立对系统进行修改的标准程序来保证计算机应用系统的完整性。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

14. Question: Which are the main testing controls?
图 14。问题:哪些是主要的测试控件？

14. Answer: The main testing controls are: Test methodology, test plan, and organizational structure for application software testing.
答:主要的测试控制有:测试方法、测试计划、应用软件测试组织结构。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

15. Question: Which should the contents of a test plan be?
图 15。问题:测试计划的内容应该是什么？

15. Answer: The contents of a test plan should be: Objectives and scope, roles and responsibilities, test scenaria and cases, acceptance criteria, test results, and test approvals.
答:测试计划的内容应该是:目标和范围，角色和职责，测试场景和案例，验收标准，测试结果和测试批准。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

16. Question: What is the responsibility of a test project manager?
图 16。问题:测试项目经理的职责是什么？

16. Answer: The test project manager is the person with overall responsibility for managing, and organizing testing, obtaining, coordinating and allocating the required

resources, providing technical guidance, performing quality reviews and inspections, undertaking and managing risks, and maintaining the test library.

答:测试项目经理是全面负责管理、组织测试、获取、协调和分配所需资源、提供技术指导、进行质量检查、承担和管理风险、维护测试库的人员。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ____________

17. Question: Which are some of the usual computerized application performance measures?
图 17。问题:哪些是通常的计算机化应用性能测量？

17. Answer: Some of the usual computerized application performance measures are: Mean time between application failures, application change controls not followed, application software not kept current, application input controls not used, etc.

答:一些常用的计算机化应用程序性能测量方法有:应用程序失效之间的平均时间、没有遵循应用程序更改控制、应用程序软件没有保持最新状态、应用程序输入控制没有使用等。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s comments: ________________

18. Question: What should be done to review source document design?
图 18。问题:在审查源文档设计时应该做什么？

18. Answer: The action that should be carried out during source documents design are: Determine if source documents are pre-numbered, determine if, for each type of transaction, the source document used provides a unique code or identifier, determine if source documents are specially designed to guide the initial recording of data in a uniform format, and determine if source documents have a cross-reference to the transactions used by the given IT system.

答:在源文件设计过程中应采取的行动是:确定源文件是否预编号，确定对于每一类交易，所使用的源文件是否提供了独特的代码或标识，确定源文件是否专门设计来指导以统一格式初始记录数据，并确定源文件是否与特定信息技术系统使用的交易相互参照。

Is reply satisfactory?
YES ______ or NO ______
Reviewer’s comments: ________________

19. Question: What should be done to review source code?
图 19。问题:应该做什么来审查源代码？

19. Answer: Source code documentation (per application program) should be reviewed
答:应该审查源代码文档(每个应用程序)

to determine whether: the source code is well documented, the source code is readable, if any logic bombs exist within the source code, if comments exist within the source code, and if there are logic loops for the source code reviewed.

判断:源代码是否有很好的文档记录，源代码是否可读，源代码中是否存在逻辑炸弹，源代码中是否存在注释，以及源代码中是否存在逻辑循环。

Is reply satisfactory? or NO

YES ______ ______
Reviewer's
comments: ____________

20. Question: How is application stability determined?
图 20。问题:如何确定应用稳定性？

20. Answer: Application stability is determined by examining: he robustness of the application, that the application downtime has been minimal, that the users have expressed concern over the system (speed, durability, poor outcomes, etc., whether there are any substantial outstanding issues with the vendors, whether there are major ongoing problems with the maintenance of the system (software/hardware/peripherals), and whether upgrades have been provided in accordance with contractual obligations.
答:应用程序的稳定性是由以下因素决定的:应用程序的健壮性、应用程序停机时间最小、用户对系统表示关注(速度、耐久性、糟糕的结果等等)、供应商是否存在任何实质性的未决问题、系统(软件/硬件/外围设备)的维护是否存在重大的持续性问题，以及是否根据合同义务提供了升级。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ____________

21. Question: How do Computerized Application controls afect the critical issues of the EU
问题:计算机应用控制如何影响欧盟的关键问题
Data Protection Regulation, such as: Purpose speciication; Data limitation; Information and access rights; Legal basis for personal data processing and transfer; Personal data rectiication and deletion; Personal data quality and accuracy; Personal data security; Personal data sharing; Personal data retention; and Personal data accountability?
保障资料规例，例如:目的说明;资料限制;资料及查阅权利;处理及传送个人资料的法律基础;个人资料的整理及删除;个人资料的质素及准确性;个人资料保安;个人资料共用;个人资料保留;及个人资料问责？

21. Answer: Computerized Application controls form the tenth crucial component that enables the ICT function to operate efectively and eiciently so that all risks related to these data protection issues are resolved as best as possible for the personal data collected and used by the speciic company or organization.
答:计算机化应用程序控制是第十个关键组成部分，它使信息和通信技术职能能够有效和安全地运作，以便尽可能最好地解决与这些数据保护问题有关的所有风险，使专业公司或组织能够收集和使用个人数据。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ______________

3.11 BUSINESS DATA MANAGEMENT CONTROLS

3.11 业务数据管理控制

1. Question: Which is the distinction between data, information and knowledge?
问题:数据、信息和知识的区别是什么？

1. Answer: Data are about facts. Information and knowledge are about meaning.
答:数据是关于事实的。信息和知识是关于意义的。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ______________

2. Question: What are business data?
图 2。问题:什么是业务数据？

2. Answer: Business data form your business records (paper or digital) and are expressed in paper or digital documents, and are processed and maintained by recordkeeping systems.
答:业务数据来自你的业务记录(纸质或数字)，以纸质或数字文件的形式表示，并由记录保存系统处理和维护。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

3. Question: What are business records?
图 3。问题:什么是业务记录？

3. Answer: A record, in business terms, is an item or collection of data, which may
答:在商业术语中，记录是一个数据项或数据集合，它可以

contain: a set of ields in a database related to one entity, data about business transactions, medical history and treatments of persons, personal data of people, minutes of meetings, music, video, pictures, other forms of digital information (like e-mail messages), etc.

包含:与一个实体相关的数据库中的一组挥发区、有关业务交易的数据、人员的病史和治疗、人员的个人数据、会议记录、音乐、视频、图片、其他形式的数字信息(如电子邮件信息)等。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

4. Question: What do business documents contain?
图 4。问题:商业文件包含什么？

4. Answer: Documents in business environments may contain: invoices, purchase order data, contracts, packing slips, reports, spreadsheets, bills of lading, vendor quotations, customs manifests, licenses, certiicates, transaction forms, computerized text iles, etc.
答:业务环境中的文件可能包括:发票、采购订单数据、合同、包装单、报告、电子表格、提单、供应商报价、海关清单、许可证、证明、交易表格、计算机文本等。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ______________

5. Question: What are the contents of a Corporate Policies and Procedures Manual?
5.问题:公司政策和程序手册的内容是什么？

5. Answer: A Corporate Policies and Procedures Manual would usually contain your general corporate policies and procedures for the following issues of your company: Board Operation, Management Procedures, Personnel Administration, Business Strategy, Financial accounting, Expense management, Revenue control, Regulatory compliance, Risk management, Purchasing, Payroll, etc.
回答:公司政策和程序手册通常包含你公司下列问题的一般公司政策和程序:董事会运作，管理程序，人事管理，业务战略，财务会计，费用管理，收入控制，守规，风险管理，采购，工资，等等。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ______________

6. Question: What do Business Operational Manuals contain?
图 6。问题:业务操作手册包含什么？

6. Business Operational Manuals contain detail procedures instructing operational staf, in all business functional departments (Finance, IT, Sales, Production, Quality, Customer service, etc.), how to carry out their detailed work tasks in their speciic function.
业务操作手册包含详细的程序，指示所有业务职能部门(财务、IT、销售、生产、质量、客户服务等)如何在其专业职能中执行其详细的工作任务。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ______________

7. Question: What does a Business Forms Manuals contain?
图 7。问题:商业表格手册包含什么？

7. Answer: A Business Forms Manual contains examples of forms and instructions on
答:《商业表格手册》载有商业表格的例子及说明

the use of the following forms: Purchase Order, Invoice, Journal Entry, Expense Approval, Vacation Approval, Overtime Approval, Master File Inventory Log, Records Inventory Log, Reports Inventory Log, Documents Inventory Log, Files, Documents and Records transfer form, Files, Documents and Records Deletion Form, Document Distribution Form, Document Revision Form, etc.

使用下列表格:采购订单、发票、日记账、费用批准、休假批准、加班批准、主档案库存日志、记录库存日志、报告库存日志、文件库存日志、档案、文件和记录转移表、档案、文件和记录删除表、文件分发表、文件修改表等。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

8. Question: What does a Business Records System contain?
问题:业务记录系统包含什么？

8. Answer: A Business Records System usually contains:
答:业务记录系统通常包括:

a) Employee personnel records including all employee accidents and illnesses, copies of monthly safety meetings, with the date and signatures of all employees in attendance, employee training records, including health, safety, payroll, and payments to pensioners (permanent retention);
员工人事记录，包括所有员工的事故和疾病，每月安全会议的副本，所有员工出席的日期和签名，员工培训记录，包括健康，安全，工资，和养老金领取者(永久保留);

b) Employment applications with completed data (5 years retention);
有完整数据的雇佣申请(保留 5 年);

c) Expense reports (to be retained as many years as specified in the tax system of each country);
费用报告(根据各国税收制度的具体情况保留年限);

d) Insurance policies and claims;
保险单及索偿;

e) Accounting and posting journal entries, financial statements and general ledgers (permanent retention);
会计和过帐分录，财务报表和总账(永久保留);

f) Payments, checks, bank statement, cash slips, invoices from vendors and to customers (to be retained as many years as specified in the tax system of each country);
付款、支票、银行对账单、现金单、供应商和客户的发票(根据各国税收制度的具体要求保留多少年);

g) Purchase orders, sales records, inventory records, asset disposition, records, etc. (as speciied in the tax system of each country); and

采购订单、销售记录、存货记录、资产处置、记录等(每个国家的税务系统都有专门的记录);

h) Correspondence, electronic mail and FAX messages, security logs and incidents, visitors' logs, audit reports, tax returns, contracts, and minutes of Board of Directors, including bylaws and articles of incorporation (permanent retention).

通信、电子邮件和传真信息、安全日志和事件、来访者日志、审计报告、纳税申报表、合同和董事会会议记录，包括公司章程和公司章程(永久保留)。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ______________

9. Question: What are some of the risks afecting your business records and recordkeeping systems?

问题:建立你们的商业记录和记录保存系统有哪些风险？

9. Answer: Some of the risks afecting business records and recordkeeping systems

答:建立商业记录和记录保管系统的一些风险

are: human errors; lack of related corporate security policy and procedures; minor and major building problems; broken pipes; ire; lood; earthquake; terrorism; poor security or environmental or safety and health conditions; and technological obsolescence issues, etc.

这些问题包括:人为错误;缺乏相关的企业保安政策和程序;较小和较大的建筑问题;破裂的管道;愤怒;卢德;地震;恐怖主义;保安或环境或安全和健康条件差;以及技术过时问题等。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ______________

10. Question: What is the purpose of a Business Raw Data Retention Procedure?

图 10。问题:业务原始数据保留程序的目的是什么？

10. Answer: he purpose of a Business Raw Data Retention Procedure is to keep all incoming, processed and outgoing data and transactions of your company in the original ('raw') format, in a well-protected, safe (from ire, etc.) and secure (access restriction rules) location for as long as required by government regulations (tax, health, safety, etc.) and in accordance with industrial and other practices (stock exchange, banks, etc.) applicable to your business operation.

答:业务原始数据保留程序的目的是，按照政府法规(税务、健康、安全等)的要求，并根据适用于你业务运作的行业和其他惯例(证券交易所、银行等)，以原始("原始")格式、受到良好保护的、安全的(防火等)和安全的(访问限制规则)存放你公司的所有进入、处理和发出的数据和交易。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ______________

11. Question: What is the purpose of a Business Data Register?
图 11。问题:商业资料登记册的目的是什么？

11. Answer: he purpose of a Business Data Register is to record the attributes (data element description, type, format, validating and editing instructions, business processing rules, etc.) of the business data of all your business documents, records and iles used and maintained by the Recordkeeping systems, iles and data bases of your company.
答:商业资料登记册的目的是记录贵公司的记录保管系统、文件夹和数据库使用和维护的贵公司所有商业文件、记录和文件的商业资料的属性(数据元素描述、类型、格式、验证和编辑指令、业务处理规则等)。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

12. Question: What can you achieve with a Data Quality Monitoring Procedure?
图 12。问题:使用数据质量监控程序可以实现什么？

12. Answer: A Data Quality Monitoring Procedure can support you to recognize data problems, inspect data sources and data processes, and implement the data corrections to get the problems ixed.
答:数据质量监测程序可以帮助您识别数据问题，检查数据源和数据处理，并实施数据修正以解决问题。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

13. Question: What are the steps of a Data Quality Improvement procedure?
图 13。问题:数据质量改进程序的步骤是什么？

13. Answer: he steps of a Data Quality Improvement procedure are:
答:数据质量改进过程的步骤是:

Step 1: Discover problem causes
第一步:发现问题的原因

Step 2: Measure data quality aspects
步骤 2:测量数据质量方面

Step 3: Measure business rule integrity
步骤 3:测量业务规则的完整性

Step 4: Complete problem analysis
第四步:完成问题分析

Step 5: Plan the data improvement process

步骤 5:计划数据改进过程

Step 6: Execute the data improvement process
步骤 6:执行数据改进过程

Step 7: Improve the data quality improvement process
步骤 7:改进数据质量改进过程

Is reply satisfactory?
YES ______ or NO ______
Reviewer's
comments: ________________

14. Question: What is a Data Cleansing or Cleaning procedure?
图 14。问题:什么是数据清理或清理过程？

14. Answer: A Data Cleansing or Cleaning procedure is the process of detecting, removing, correcting and deleting (in certain cases) incorrect, incomplete, irrelevant, corrupt, out-of-date, formatted incorrectly, duplicated, etc., data or records from a computerized ile, data base table, database, or record set, etc.

答:数据清理或清理程序是检测、删除、纠正和删除(在某些情况下)不正确、不完整、不相关、损坏、过时、格式不正确、重复等数据或记录的过程，这些数据或记录来自计算机文件、数据库表、数据库或记录集等。

Is reply satisfactory?
YES ______ or NO ______
Reviewer's comments: ________________

15. Question: How do Business Data Management Controls afect the critical issues
问题:业务数据管理控制如何处理关键问题

of the EU Data Protection Regulation, such as: Purpose speciication; Data limitation; Information and access rights; Legal basis for personal data processing and transfer; Personal data rectiication and deletion; Personal data quality and accuracy; Personal data security; Personal data sharing; Personal data retention; and Personal data accountability?
个人资料的质素及准确性;个人资料保安;个人资料共用;个人资料保留;及个人资料问责？

15. Answer: Business Data Management Controls form the most critical and crucial component that enables the speciic company to operate all aspects of data governance efectively and eiciently so that all risks related to these data protection issues are resolved as best as possible for the personal data collected and used by the speciic company or organization.

答:业务数据管理控制构成了最关键和最关键的组成部分，使专业公司能够有效地运作数据治理的所有方面，以便尽可能最好地解决与这些数据保护问题有关的所有风险，使专业公司或组织能够收集和使用个人数据。

4 SUMMARY OF THE NEW EU GENERAL DATA PROTECTION REGULATION

新的欧盟一般数据保护条例摘要

Overview (link to the Data Protection and Privacy Management System)
概览(连结至资料保护及私隐管理系统)

This chapter provides further details of the actions defined in 'Step AP# 2: Collect Privacy Laws' of 'Phase 1-DP Preparation' of the Data Protection and Privacy Management System (as described in 'Chapter 2: Data Protection and Privacy Management System').
本章提供「资料保护及私隐管理系统第一阶段-资料保护及私隐管理系统」的「第一阶段-资料保护及私隐管理系统」的「第二步:收集私隐法例」所采取行动的进一步详情(见「第二章:资料保护及私隐管理系统」)。

Summary
摘要

This chapter describes, in summary, the six key components of the GDPR that European corporate executives need to understand and take specific actions and implement relevant controls to protect the data of their enterprise.
本章概括介绍了欧洲企业管理人员需要了解和采取具体行动并实施相关控制以保护企业数据的 GDPR 的六个关键组成部分。

1. **Description of the GDPR**
关于 GDPR 的描述

The EU General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Commission intends to strengthen and unify data protection for individuals within the European Union (EU).
《欧盟一般资料保护规例》(《规例》(欧盟)2016/679)旨在加强和统一对欧洲联盟(欧盟)内个人资料的保护。

It also addresses export of personal data outside the EU. The Commission's primary objectives of the GDPR are to give citizens back the control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.
该法案还涉及个人数据在欧盟以外的出口。欧盟委员会的首要目标是让公民重新控制自己的个人数据，并通过统一欧盟内部的规定，简化国际商业的监管环境。

When the GDPR takes effect it will replace the official Directive 95/46/EC from 1995. The regulation was adopted on 27 April 2016. It enters into force 25 May 2018 after a

two-year transition period and, unlike a directive it does not require any enabling legislation to be passed by governments.
1995 年颁布的《第 95/46/ec 号公约》将取代《第 95/46/ec 号公约》。该规例于 2016 年 4 月 27 日获得通过。经过两年的过渡期后，该法于 2018 年 5 月 25 日生效，与指令不同，该法不要求政府通过任何授权立法。

The new law will replace a patchwork of 28 different sets of national privacy laws by creating a single set of rules for the protection of data within the EU.
新法律将通过创建一套单一的欧盟内部数据保护规则，取代拼凑而成的 28 套不同的国家隐私法。

This consolidation to one national privacy regulator should lighten the administrative burden on companies as they'll be able to conduct business across the entire EU without having to monitor compliance with multiple autonomous privacy laws.
他与一个国家隐私监管机构的合并应该减轻公司的行政负担，因为他们将能够在整个欧盟范围内开展业务，而不必监督多个自治隐私法的遵守情况。

At the same time, the GDPR sets the privacy bar quite high, placing extensive limits around how businesses must treat personal data and requiring consistent privacy monitoring controls.
与此同时，GDPR 设置了相当高的隐私标准，在企业必须如何处理个人数据方面设置了广泛的限制，并要求一致的隐私监控控制。

2. **Main components of the GDPR**
Gdpr 的主要成分

There are six key components of the GDPR that European corporate executives need to understand:
以下是欧洲企业管理人员需要理解的 GDPR 的六个关键组成部分:

Component 1: Broader concept of ‘personal data’
组成部分 1:更广泛的"个人数据"概念

The definition of “personal data” has been widely expanded to include information related to a data subject’s physical, physiological, genetic, mental, economic, cultural or social identity. This is going to require a rethink of most organizations’ previous data privacy policies.
"个人数据"的定义已被广泛扩展，包括与数据主体的身体、生理、遗传、心理、经济、文化或社会身份有关的信息。他将要求重新考虑大多数组织以前的数据隐私政策。

Component 2: Notifications for data breaches
组成部分 2:数据泄露通知

The GDPR establishes a uniform data breach notification requirement: in the event of a data breach leading to the loss, access or disclosure of personal data, organizations must notify regulators “without undue delay” and – unless the data is encrypted or the individuals involved will be harmed – they must do so within 72 hours.
他建立了一个统一的数据泄露通知要求:在发生数据泄露导致个人数据丢失、访问或披露的情况下，各组织必须"毫不拖延地"通知监管机构，除非数据被加密或相关个人将受到伤害，否则必须在 72 小时内通知监管机构。

Component 3: Data transfer rules
组件 3:数据传输规则

Data transfer out of the EU will only be allowed if the European Commission has evaluated the level of data protection in the country where the data is being transferred and has affirmed that it is acceptable.
只有欧盟委员会评估了数据传输所在国的数据保护水平，并确认数据传输是可接受的，才允许数据传输出欧盟。

Component 4: Consent rules
组成部分 4:同意规则

Under the GDPR, consent must be freely given, specific and informed. Any organization collecting personal data must be clear that the individual providing that

information is making a clear and unambiguous decision that they're entering into an agreement for the organization to collect and process that data.
根据 GDPR，同意必须是自由的、具体的和知情的。任何收集个人数据的组织都必须清楚，提供这些信息的个人正在做出一个明确和毫不含糊的决定，即他们正在为组织收集和处理这些数据达成协议。

Component 5: Data Protection Oicer
组件 5:数据保护器

If a company consistently monitors or processes sensitive personal data – regardless of where that data is processed in the world – they will have to appoint a Data Protection Oicer who has appropriate data protection law expertise.
如果一家公司持续监测或处理敏感的个人数据——不管这些数据在世界上哪里处理——它们就必须指定一名拥有适当数据保护法律专业知识的数据保护专家。

The data protection officer may be employed by the company or be engaged with a service contract, but either way that professional’s tasks must include advising the company on data protection issues, monitoring compliance with the GDPR and acting as the point of contact for regulators.
数据保护员可能受雇于公司，也可能从事服务合同，但无论哪种方式，专业人员的任务必须包括就数据保护问题向公司提供咨询意见，监测遵守 GDPR 的情况，并充当监管机构的联络点。

Component 6: Enforcement
组成部分 6:执法

The GDPR gives individual consumers a private right of action in EU courts, which means they have a right to seek financial damages for any harm caused by the processing of personal data. Meanwhile, regulators have been empowered to issue opinions, adopt binding decisions and otherwise oversee data protection processes to ensure compliance by organizations.
欧盟委员会赋予个人消费者在欧盟法院提起诉讼的私人权利，这意味着他们有权要求因处理个人数据而造成的任何伤害的金融损害赔偿。与此同时，监管机构被授权发表意见，通过具有约束力的决定，并以其他方式监督数据保护过程，以确保组织的遵守。

The power to assess fines is alarming – up to 4% of worldwide corporate revenues is astounding – although the GDPR makes it clear that the amount of the fine will depend on several factors such as the nature, gravity and duration of the infringement.
评估信用卡的权力令人震惊——高达全球企业收入的 4%令人震惊——尽管 gpr 明确表示，信用卡的金额将取决于几个因素，如侵权的性质、严重程度和持续时间。

5 PERSONAL DATA CHECKLIST

5 个人资料清单

Overview (link to the Data Protection and Privacy Management System)
概览(连结至资料保护及私隐管理系统)

his chapter provides further details of the actions deined in 'Step AP# 1: Conduct Privacy Analysis' of 'Phase 1-DP Preparation' of the Data Protection and Privacy Management System (as described in 'Chapter 2: Data Protection and Privacy Management System').
本章提供资料保护及私隐管理系统「第一阶段-资料保护及私隐管理系统」的「第一步:进行私隐分析」所采取行动的进一步详情(见「第二章:资料保护及私隐管理系统」)。

Summary
摘要

his chapter identiies some common types of personal data that are linked to individuals and which (data) may be collected, processed, maintained, shared or used by enterprises in the current socio-economic, business and digital environment.
他的章节列出一些与个人有关连的常见个人资料，这些资料可供企业在现时的社会经济、商业及数码环境中收集、处理、保存、分享或使用。

Enterprises may use this list as a baseline to ensure they have identiied all personal data that may be subject to applicable laws, regulations, and policies.
企业可以使用这个列表作为基准，以确保他们已经识别了可能受到适用的法律、法规和政策约束的所有个人数据。

1. **Data Type 1: Basic Personal Identiication Numbers (BP)**
资料类别 1:基本个人身分识别号码

Field name #BP01: <Last Name>
域名#bp01:姓氏

Field name #BP02: <Middle Name>
域名#bp02:中间名

Field name #BP03: <First Name>
字段名#bp03:名

Field name #BP04: <Birth date>
字段名#bp04:出生日期

Field name #BP05: <Sex>
域名#bp05:性

Field name #BP06: <Age>
字段名#bp06:年龄

Field name #BP07: <Mother's maiden name>
字段名#bp07:母亲的娘家姓

Field name #BP08: <Birth Certiicate number>
字段名#bp08:出生证明号码

Field name #BP09: <Social Security number>
域名#bp09:社会保障号码

Field name #BP10: <Drivers’ license number>
字段名#bp10:驾驶执照号

Field name #BP11: Citizenship 1
域名#bp11:公民身份 1

Field name #BP12: Citizenship 2
域名#bp12:公民身份 2

Field name #BP13: <Credit card number 1>
字段名#bp13:信用卡号 1

Field name #BP14: <Credit card number 2>
字段名#bp14:信用卡号 2

Field name #BP15: <Credit card number 3>
字段名#bp15:信用卡号 3

Field name #BP16: <Bank account number (bank 1)>
字段名#bp16:银行账户号码(银行 1)

Field name #BP17: <Bank account number (bank 2)>
字段名#bp17:银行帐号(银行 2)

Field name #BP18: <Bank account number (bank 3)>
字段名#bp18:银行账号(银行 3)

Field name #BP19: <Passport number>
字段名#bp19:护照号码

Field name #BP20: <Other Government ID # or unique identiier 1 (tax)>
域名#bp20:其他政府 ID#或唯一标识 1(tax)

Field name #BP21: <Other Government ID # or unique identiier 2 (customs)>
域名#bp21:其他政府 ID#或唯一标识符 2(海关)

Field name #BP22: <Other Government ID # or unique identiier 3 (criminal register)>
域名#bp22:其他政府 ID#或唯一标识符 3(刑事登记)

2. **Data Type 2: Electronic Personal Data (ED)**
资料类别二:电子个人资料

Field name #ED01: <E-mail address 1>
域名#ed01:E-mail 地址 1

Field name #ED02: <E-mail address 2>
域名#ed02:电子邮件地址 2

Field name #ED03: <E-mail address 3>
域名#ed03:电子邮件地址 3

Field name #ED04: <Social media address 1>
域名#ed04:社交媒体地址 1

Field name #ED05: <Social media address 2>
域名#ed05:社交媒体地址 2

Field name #ED06: <Social media address 3>
域名#ed06:社交媒体地址 3

Field name #ED07: <Web site 1>
域名#ed07:Website1

Field name #ED08: <Web site 2>
域名#ed08:Website2

Field name #ED09: <Blog address>
字段名#ed09:博客地址

Field name #ED10: <User name 1>
字段名#ed10:用户名 1

Field name #ED11: <Password 1>
字段名#ed11:Password1

Field name #ED12: <User name 2>
域名#ed12:用户名 2

Field name #ED13: <Password 2>
字段名#ed13:Password2

Field name #ED14: <Avatar>
字段名#ed14:avatar

Field name #ED15: <IP address>
字段名#ed15:ip 地址

Field name #ED16: <Log data (time, date, referrer site, browser type)>
字段名#ed16:日志数据(时间、日期、引用站点、浏览器类型)

Field name #ED17: <Tracking data (e.g., single- or multi-session cookies, beacons)>
字段名#ed17:跟踪数据(例如，单会话或多会话 cookie、信标)

Field name #ED18: <Forms data>
字段名#ed18:formsdata

3. **Data Type 3: Additional Personal Data (AD)**
资料类别 3:额外的个人资料(AD)

Field name #AD01: <Phone number 1>
域名#ad01:电话号码 1

Field name #AD02: <Phone number 2>
域名#ad02:电话号码 2

Field name #AD03: <Phone number 3>

域名#ad03:电话号码 3

Field name #AD04: <Fax>
字段名#ad04:fax

Field name #AD05: <City>
域名#ad05:城市

Field name #AD06: <Postal address>
域名#ad06:邮政地址

Field name #AD07: <Marital status>
域名#ad07:婚姻状况

Field name #AD08: <Name of wife/husband 1>
域名#ad08:妻子/丈夫姓名 1

Field name #AD09: <Name of wife/husband 2>
域名#ad09:妻子/丈夫姓名 2

Field name #AD10: <Name of wife/husband 3>
字段名#ad10:妻子/丈夫姓名 3

Field name #AD11: <Names of children>
字段名#ad11:孩子的名字

Field name #AD12: <Details of relatives>
字段名#ad12:亲属的详细信息

Field name #AD13: <Sexual orientation>
字段名#ad13:性取向

Field name #AD14: <Race>
字段名#ad14:race

Field name #AD15: <Ethnicity>
域名#ad15:种族

Field name #AD16: <Religion>
域名#ad16:宗教

Field name #AD17: <Education 1>
域名#ad17:Education1

Field name #AD18: <Education 2>
字段名#ad18:教育 2

Field name #AD19: <Education 3>
字段名#ad19:教育 3

Field name #AD20: <Profession>
域名#ad20:职业

Field name #AD21: <Employment 1>
域名#ad21:Employment1

Field name #AD22: <Employment 2>
域名#ad22:Employment2

Field name #AD23: <Employment 3>
域名#ad23:就业 3

Field name #AD24: <Health information>
域名#ad24:健康信息

Field name #AD25: <Insurance information>
域名#ad25:保险信息

Field name #AD26: <Medical treatment information>
域名#ad26:医疗信息

Field name #AD27: <Criminal history>
域名#ad27:犯罪历史

4. **Data Type 4: Physical Personal Data (PD)**
资料类别四:个人实体资料

Field name #PD01: <Physical descriptor 1 (eye color) >
字段名#pd01:物理描述符 1(眼睛颜色)

Field name #PD02: <Physical descriptor 2 (hair color) >
字段名#pd02:物理描述符 2(头发颜色)

Field name #PD03: <Physical descriptor 3 (height) >
字段名#pd03:物理描述符 3(高度)

Field name #PD04: <Physical descriptor 4 (body marks) >
字段名#pd04:物理描述符 4(主体标记)

Field name #PD05: <Signature>
字段名#pd05:签名

Field name #PD06: <Fingerprints>
域名#pd06:指纹

Field name #PD07: <Handprints>
字段名#pd07:手印

Field name #PD08: <Photo, scans (retinal, facial) >
字段名#pd08:照片，扫描(视网膜，面部)

Field name #PD10: <Voice>
字段名#pd10:voice

Field name #PD11: <Physical movements (e.g., finger swipes, keystrokes) >
字段名#pd11:身体动作(例如，手指滑动，击键)

Field name #PD12: <DNA markers>
字段名#pd12:dna 标记

5. **Data Type 5: Device-related Personal Data (DD)**
资料类别五:与装置有关的个人资料(DD)

Field name #DD01: <User names>
字段名#dd01:用户名

Field name #DD02: <Passwords>
域名#dd02:密码

Field name #DD03: <Unique device identiier>
字段名#dd03:唯一设备标识符

Field name #DD04: <Location/GPS data>
域名#dd04:位置/gps 数据

Field name #DD05: <Camera controls (photo, video, videoconference)>
字段名#dd05:相机控制(照片、视频、视频会议)

Field name #DD06: <Microphone controls>
字段名#dd06:麦克风控制

Field name #DD07: <Other hardware/software controls>
字段名#dd07:其他硬件/软件控件

Field name #DD08: <Photo data>
字段名#dd08:照片数据

Field name #DD09: <Audio/sound data>
字段名#dd09:音频/声音数据

Field name #DD10: <Other device sensor controls>
字段名#dd10:其他设备传感器控件

Field name #DD11: <On/Of status and controls>
字段名#dd11:on/ofstatusandcontrols

Field name #DD12: <Cell tower records (e.g., logs, user location, time, date) >
字段名#dd12:基站记录(例如，日志、用户位置、时间、日期)

Field name #DD13: <Data collected by apps (itemize)>
字段名#dd13:应用程序收集的数据(逐项列出)

Field name #DD14: <Contact lists and directories>
字段名#dd14:联系人列表和目录

Field name #DD15: <Network communications data>
字段名#dd15:网络通信数据

Field name #DD16: <Device settings (e.g., security, sharing, status, etc.) >
字段名#dd16:设备设置(例如，安全性、共享、状态等)

APPENDIX 1: COMPONENTS OF A DATA PROTECTION AND PRIVACY PROGRAM

附录 1:数据保护和隐私程序的组成部分

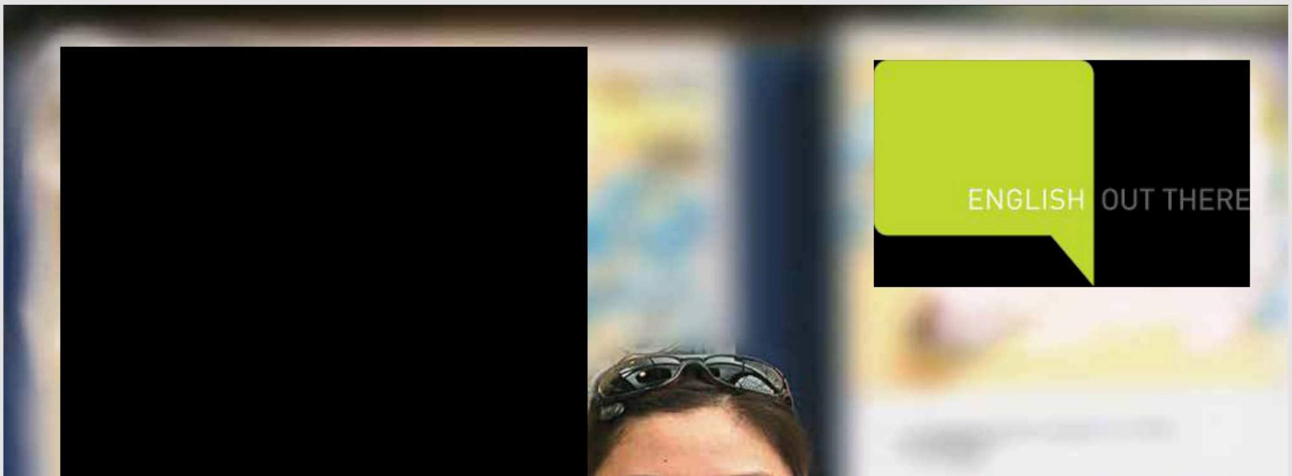
Summary

摘要

hhis appendix contains a list of the various components of an efective Data Protection and Privacy Program. hhese components are detailed in the other volumes of this book.
他的附录中列出了有效数据保护和隐私计划的各个组成部分。这些成分在这本书的其他部分有详细说明。

Contents

内容



[redacted]

DP&P Plan # 5: Integration Activities Plan
Dp&p 计划#5:整合活动计划

DP&P Plan # 6: Data Quality Improvement Plan
Dp&p 计划#6:数据质量改进计划

DP&P Policy # 1: Data Protection Policy
Dp&p 策略#1:数据保护策略

DP&P Policy # 2: Corporate Records Retention and Destruction Policy
Dp&p 政策#2:公司记录保留和销毁政策

DP&P Policy # 3: Data Classiication Policy
Dp&p 策略#3:数据分类策略

DP&P Policy # 4: Data Quality Policy
Dp&p 政策#4:数据质量政策

ITSEC Policy # 1: Information Technology (IT) Policy
资讯科技及广播局政策#1:资讯科技政策

ITSEC Policy # 2: Information Technology (IT) Security Policy
资讯科技及广播局政策#2:资讯科技保安政策

ITSEC Policy # 3: Password Controls Policy
资讯科技安全政策#3:密码控制政策

ITSEC Policy # 4: Security Policy for Personal Computers
资讯科技安全政策#4:个人电脑保安政策

ITSEC Policy # 5: Security Policy for Laptops and Smart Devices
Itsec 政策#5:笔记本电脑和智能设备的安全政策

CM Policy # 1: Conidentiality Policy
配置管理策略#1:同一性策略

CM Policy # 2: Business Ethics Policy
配置管理政策#2:商业道德政策

CM Policy # 3: Clean Desk Policy
中药政策#3:清洁办公桌政策

CM Policy # 4: Workplace Wellness Policy
Cm 政策#4:工作场所健康政策

CM Policy # 5: Occupational Stress Policy
中医政策#5:职业压力政策

CM Policy # 6: Health and Safety Policy
Cm 政策#6:健康和安全政策

DP&P Job # 1: Data Protection Oicer Job Description
Dp&p 工作#1:数据保护员工作描述

DP&P Job # 2: Information Security Manager
Dp&p 工作#2:信息安全管理员

DP&P Job # 3: Data Quality Roles and Responsibilities (for Managers; ICT Personnel; Data Quality Oicers; Administrative staf; Business Data Librarian; Business Data Steward; and Data Custodian or Data Base Administrator) DP&P Register # 1: Business Data Elements Register

Dp&p 工作#3:数据质量角色和职责(适用于管理人员;信息和通信技术人员;数据质量员;行政管理人员;业务数据馆员;业务数据管理员;数据保管人或数据库管理员)dp&p 登记册#1:业务数据元登记册

DP&P Register # 2: Data Subjects Register
Dp&p 登记册#2:资料当事人登记册

DP&P Register # 3: Personal Data Elements Dictionary EU Data Protection and Privacy Controls Data Security Controls

Dp & p Register # 3: Personal Data Elements Dictionary EU Data Protection and Privacy Controls Data Security Controls

APPENDIX 2: BIBLIOGRAPHY
附录 2:参考书目

A. Books written by John Kyriazoglou
作者:JohnKyriazoglou

1. 'IT Strategic & Operational Controls' U.K.: http://www.itgovernance.co.uk/
英国:IT 战略与操作控制 http://www.itgovernance.co.uk/

2. 'Business Management Controls: A Guide' U.K.: http://www.itgovernance.co.uk/
企业管理控制:指南英国:http://www.itgovernance.co.uk/

'IT-Business Alignment' (Parts 1 & 2)': www.bookboon.com.
「资讯科技与业务联系」(第一及第二部分):www.bookboon.com。

'How to improve your company's performance': www.bookboon.com.
如何提高你的公司业绩:www.bookboon.com。

'How to Improve Your Production' (2 Parts): www.bookboon.com.
如何提高你的生产力》(2part):www.bookboon.com。

'Managing your SME more efectively' (2 Parts): www.bookboon.com.
「更有效地管理中小企业」(下篇):www.bookboon.com。

'How to Reduce Occupational Stress': www.bookboon.com'.
如何减轻职业压力:www.bookboon.com。

'Seven Milestones for a Better Life': www.bookboon.com.
7 个让生活更美好的里程碑:www.bookboon.com。

'How to Improve Your Workplace Wellness': www.bookboon.com.
如何改善你的工作场所健康:www.bookboon.com。

B. Regulatory Frameworks
规管架构

1. EU Privacy Directive (Directive 95/46/EC)
欧盟私隐指示(指示 95/46/ec)

2. FERPA (Family Educational Rights and Privacy Act)
http://www.ed.gov/oices/OM/fpco/ferpa/index.html
家庭教育权利和隐私
http://www.ed.gov/oices/om/fpco/FERPA/index.html

3. GLB (Gramm-Leach-Bliley) Act
http://www.ftc.gov/privacy/privacyinitiatives/glbact.html
《 http://www.ftc.gov/privacy/privacyinitiatives/glbact.html 》

4. HIPAA (Health Insurance Portability and Accountability Act)
http://www.hhs.gov/ocr/hipaa/
美国健康保险便利和责任法案 http://www.hhs.gov/ocr/HIPAA/协会

5. HAS (Homeland Security Act)
http://www.dhs.gov/xabout/laws/law_regulation_rule_0011.shtm
美国国土安全
http://www.dhs.gov/xabout/laws/law_regulation_rule_0011.shtm

6. NERCCIP (North America Electric Reliability Council Critical Infrastructure Protection)
北美电力可靠性委员会关键基础设施保护

7. PCI (Personal Credit Information/Industry): https://www.pcisecuritystandards.org/
个人信用信息/行业:https://www.pcisecuritystandards.org/

8. SOX (Sarbanes-Oxley Act of 2002)
Sox(2002 年萨班斯-奥克斯利法案)

C. Internet Resources
互联网资源

1. U.S. Securities and Exchange Commission: www.sec.gov
美国证券交易委员会:www.sec.gov

2. he Center for Audit Quality (CAQ): www.thecaq.org
审计质量中心(CAQ):www.thecaq.org

3. Financial Accounting Foundation: www.accountingfoundation.org
财务会计基金会:www.accountingfoundation.org

4. U.S. Federal Emergency Management Agency
美国联邦紧急事务管理局

5. Canada Emergency: www.publicsafety.gc.ca
加拿大紧急情况:www.publicsafety.gc.ca

6. Emergency Management Australia
澳洲紧急事故管理局

7. International Association of Emergency Managers: www.iaem.com
国际应急管理人员协会:www.iaem.com

8. National Emergency Management Association: www.nemaweb.org
国家应急管理协会:www.nemaweb.org

9. UK Resilience: www.cabinetoice.gov.uk/ukresilience
英国复原力:www.cabinetoice.gov.UK/ukresilience

10. International Risk Governance Council: www.irgc.org
图 10。国际风险管理委员会:www.irgc.org

11. Advanced Performance Institute (API): www.ap-institute.com
www.securitymetrics.org
图 11。高级性能研究所(API):www.ap-Institute.comwww.securitymetrics.org

www.securityfocus.com
www.securityfocus.com

www.sans.org
Www.sans.org

www.isaca.org
Www.isaca. org

www.cert.org
Www.cert. org

http://www.globalsecurity.org/security/systems/biometrics.htm
http://computer.howstufworks.com/question28.htm
http://science.howstufworks.com/environmental/energy/power.htm
http://en.wikipedia.org/wiki/Uninterruptible_power_supply
http://en.wikipedia.org/wiki/Emergency_power_system
http://faculty.nps.edu/ncrowe/eprotect_inal.htm
www.health.ny.gov/environmental/radiological/radiation_safety_guides/qalarge.htm
https://www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf
http://www.wbdg.org/resources/cybersecurity.php?r=resist_hazards
http://www.wbdg.org/design/resist_hazards.php http://www.encasement.com/about-encasement/weatherprooing http://www.nist.gov/cyberframework/index.cfm
Http://www.globalsecurity.org/security/systems/biometrics.htm
http://computer.howstufworks.com/question28.htm
http://science.howstufworks.com/environmental/energy/power.htm
http://en.wikipedia.org/wiki/uninterruptible_power_supply · http://en.wikipedia.org/wiki/emergency_power_system · http://faculty.nps.edu/ncrowe/eprotect_inal.htm · www.health.ny.gov/environmental/radiological/radiation_safety_guides/qalarge.htm

http://www.uspto.gov/
http://www.uspto.gov/

http://www.patentregister.ca/
http://www.patentregister.ca/

http://www.epo.org
http://www.epo.org

http://www.ipo.gov.uk
http://www.ipo.gov.uk

http://www.ipaustralia.gov.au/
http://www.ipaustralia.gov.au/

www.thecbi.org
Www.thecbi. org

www.drj.com

Www.drj. com

www.iwar.org.uk http://homeland.house.gov/press-release/meehan-introduces-cfats-authorization-bill http://www.americanchemistry.com/Policy/Security http://www.chemicalcybersecurity.org/

Www.iwar. org. uk http://homeland.house.gov/press-release/meehan-introduces-cfats-authorization-bill http://www.americanchemistry.com/policy/security http://www.chemicalcybersecurity.org/

www.efqm.org

Www.efqm. org

D. Security Frameworks

安全框架

http://www.opensecurityarchitecture.org/cms/index.php
http://www.sabsa.org/

http://www.opensecurityarchitecture.org/cms/index.php
http://www.sabsa.org/

https://en.wikipedia.org/wiki/Sherwood_Applied_Business_Security_Architecture
http://www.opengroup.org/subjectareas/security/architecture

https://en.wikipedia.org/wiki/sherwood_applied_business_security_architecture
http://www.opengroup.org/subjectareas/security/architecture

http://www.sans.org/reading-room/whitepapers/bestprac/department-defense-architecture-framework-develop-security-requirements-34500
http://www.arctecgroup.net/pdf/ArctecSecurityArchitectureBlueprint.pdf www.sans.org/
Http://www.sans.org/reading-room/whitepapers/bestprac/department-defense-architecture-framework-develop-security-requirements-34500
http://www.arctecgroup.net/pdf/arctecsecurityarchitectureblueprint.pdf www.sans.org /

E. International Standards

E.国际标准

1. International Organization for Standardization/International Electrotechnical Commission 27001:2005, Security techniques – Information security management systems – Requirements.

国际标准化组织/国际电工技术委员会 27001:2005，安全技术.信息安全管理系统.要求。

2. International Organization for Standardization/International Electrotechnical Commission 15408-1:2009, Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model

国际标准化组织/国际电工技术委员会 15408-1:2009，信息技术.安全技术.IT 安全的评价标准.第 1 部分:介绍和一般模型

3. International Organization for Standardization/International Electrotechnical Commission 15408-2:2008, Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements.

国际标准化组织/国际电工技术委员会 15408-2:2008，信息技术.安全技术.IT 安全的评价标准.第 2 部分:安全功能要求。

4. International Organization for Standardization/International Electrotechnical Commission 15408-3:2008, Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements.

国际标准化组织/国际电工技术委员会 15408-3:2008，信息技术.安全技术.IT 安全的评价标准.第 3 部分:安全保证要求。

5. National Institute of Standards and Technology Federal Information Processing Standards Publication 140-2, Security Requirements for Cryptographic Modules, May 2001. National Institute of Standards and Technology Federal Information Processing Standards Publication 140-3 (Draft), Security Requirements for Cryptographic Modules, December 2009.

国家标准和技术研究所联邦信息处理标准出版物 140-2，加密模块的安全要求，2001 年 5 月。美国国家标准与技术研究所联邦信息处理标准出版物 140-3(草案)，加密模块的安全要求，2009 年 12 月。

6. National Institute of Standards and Technology Federal Information Processing Standards Publication 180-4, Secure Hash Standard (SHS), March 2012.

美国国家标准与技术研究所联邦信息处理标准出版物 180-4，安全哈希标准(SHS)，2012 年 3 月。

7. National Institute of Standards and Technology Federal Information Processing Standards Publication 186-3, Digital Signature Standard (DSS), June 2009.

美国国家标准与技术研究所联邦信息处理标准出版物 186-3，数字签名标准(DSS)，2009 年 6 月。

8. National Institute of Standards and Technology Federal Information Processing Standards Publication 188, Standard Security Label for Information Transfer, September 1994.

国家标准和技术研究所联邦信息处理标准出版物 188，信息传输标准安全标签，1994 年 9 月。

9. National Institute of Standards and Technology Federal Information Processing Standards Publication 190, Guideline for the Use of Advanced Authentication

美国国家标准与技术研究所联邦信息处理标准出版物 190，高级认证使用指南

Technology Alternatives, September 1994.
技术替代品，1994 年 9 月。

10. National Institute of Standards and Technology Federal Information Processing Standards Publication 197, Advanced Encryption Standard (AES), November 2001.

美国国家标准与技术研究所联邦信息处理标准出版物 197，高级加密标准，2001 年 11 月。

11. National Institute of Standards and Technology Federal Information Processing Standards Publication 198-1, he Keyed-Hash Message Authentication Code (HMAC), July 2008.

美国国家标准与技术研究所联邦信息处理标准出版物 198-1，金钥杂凑讯息鑑别码，2008 年 7 月。

12. National Institute of Standards and Technology Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004.

国家标准和技术研究所联邦信息处理标准出版物 199，《联邦信息和信息系统安全分类标准》，2004 年 2 月。

13. National Institute of Standards and Technology Federal Information Processing Standards Publication 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006.

国家标准和技术研究所联邦信息处理标准出版物 200，《联邦信息和信息系统最低安全要求》，2006 年 3 月。

14. National Institute of Standards and Technology Federal Information Processing Standards Publication 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006.

美国国家标准和技术研究所联邦信息处理标准出版物 201-1，联邦雇员和承包商的个人身份验证(PIV)，2006 年 3 月。

Disclaimer: The material, concepts, ideas, plans, policies, procedures, forms, methods, tools, etc. presented, described and analyzed in all parts, chapters and appendices of this book, are for educational and training purposes only. These may be used only, possibly, as an indicative base set, and should be customized by each organization, after careful and considerable thought as to the needs and requirements of each organization, taking into effect the implications and aspects of the legal (e.g. European Data Protection Regulation, other national privacy laws, etc.), national, religious, philosophical, cultural and social environments, and expectations, within which each organization operates and exists. Every possible effort has been made to ensure that the information contained in this book is accurate at the time of going to press, and the publishers and the author cannot accept responsibility for any errors or omissions, however caused. No responsibility for loss or damage occasioned to any person acting, or refraining from action, as a result of the material in this publication can be accepted by the publisher or the author.

免责声明:在本书的所有部分、章节和附录中提供、描述和分析的材料、概念、想法、计划、政策、程序、形式、方法、工具等，仅用于教育和培训目的。这些词语可能仅仅用作指示性的基本词汇，每个组织都应根据自己的需要和要求进行定制，并考虑到各组织运作和存在的法律(例如欧洲数据保护条例、其他国家隐私法等)、国家、宗教、哲学、文化和社会环境以及期望的含义和方面。每一个可能的补救措施都是为了确保本书在出版时所包含的信息是准确的，出版商和作者不能为任何错误或遗漏承担责任，不管这些错误或遗漏是如何造成的。出版者或作者不能接受因本出版物中的材料而造成的任何人的行为或不行为所引起的损失或损害的责任。

ENDNOTES
尾注

1. For more on Deming, see: https://www.deming.org http://www8.gsb.columbia.edu/deming/about/history http://asq.org/learn-about-quality/quality-management-system

更多关于 Deming 的信息，请参见:https://www.Deming.orghttp://www8.gsb.columbia.edu/ Deming/about/historyhttp://asq.org/learn-about-quality/quality-management-system

2. See more details at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416 and http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000034.

更多详细信息请参阅:http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416 和 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000034。

3. For more details, see: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416 and http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000034.

更多详细信息，请参阅:http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416 和 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000034。

4. For more information on data protection laws, broken down by country, see the reports published by Privacy International, https://www.privacyinternational.org/node/44.

更多关于数据保护法律的信息，请参阅由隐私国际，https://www.privacyinternational.org/node/44 保护组织发布的报告。

5. See ‘2014 Cost of Data Breach Study: United States’.

参见 2014 年数据泄露的代价研究:美国。

6. One of the most famous cases of billions of dollars lost due to incorrect data was the JPMorgan Chase & Co. case of 2012, as per https://en.wikipedia.org/wiki/2012_JPMorgan_Chase_trading_loss and http://www.businessinsider.com/excel-partly-to-blame-for-trading-loss-2013-2

由于错误的数据导致数十亿美元损失的一个最著名的案例是 2012 年的摩根大通案例，根据 https://en.wikipedia.org/wiki/2012_jpmorgan_chase_trading_loss 和 http://www.businessinsider.com/excel-partly-to-blame-for-trading-loss-2013-2 的数据

7. For more details, see: Experian’s Data Quality Global Report for 2016, https://www.experian.com/in-novation/thought-leadership/2016-data-benchmark-report.jsp

更多详细信息，请参阅:益百利 2016 年全球数据质量报告，https://www.Experian.com/in-novation/thought-leadership/2016-Data-benchmark-Report.jsp

8. For more on EU Data Protection Directive, see: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=14623595217 58&from=EN.

更多关于欧盟数据保护指令的信息，请参见:欧洲 http://eur-lex.europa.EU/legal-content/EN/txt/pdf/?uri=celex:32016r0679&qid=14623595217 标准 58 和 EN。

To see Volume II download:
查看第二卷下载:

DP&P Strategies, Policies and Plans
Dp&p 战略、政策和计划

Data Protection and Privacy Guide – Vol II
资料保护及私隐指引-第二册