



# 数据隐私保护业务--GDPR 合规评估

IoT服务隐私保护-更着重运营层面的合规，管理行为的保障

# 通用数据保护法案核心要求

个人数据的非必要使用  
产品或服务尽可能少的  
处理个人数据，并且不  
能使用与声明功能无关  
的个人数据



个人对数据使用的知情  
同意



（informed consent）个  
人需要对数据处理知情，  
并给出个人同意



个人对数据的修改和移  
动的权利  
个人能够修改和移动个  
人数据



个人对数据的删除权  
个人有权删除、清除自  
己所有的数据

# 通用数据保护法案核心要求

## 数据保护

厂商需要对个人数据提供技术上和流程上的保护



## 加密

法案建议厂商对个人数据进行匿名化和加密



**非必要设计和功能**  
厂商的产品和服务不应当有非必要的设计和功



**隐私设计和设置**  
法案建议厂商在产品或服务当中，出厂设计与设置需要保护用户的个人隐私

# 欧盟一般数据保护条例(GDPR)的要点概述

## 欧盟企业：

- 设于欧盟成员国的企业均受GDPR管辖。
- 设于欧盟以外的企业：

非欧盟成员国的公司只要满足下列两个条件之一，该公司就受到GDPR的管辖：

- 1) 为了向欧盟境内可识别的自然人提供商品和服务而收集、处理（注）他们的信息；
- 2) 为了监控欧盟境内可识别的自然人的活动而收集、处理（注）他们的信息。

注：个人信息的“处理”包括：收集、存储、组织、修改、恢复、使用、转移、传播、保护以及销毁等。

GDPR的监管机构“Supervisory authority”接受关于违法的投诉后，**有权调查可能的违法情形**，并进行相应的处罚。其主要权力如下：

## 调查权

监管机构有权要求个人信息的“控制者”以及“处理者”提供任何所需资料；

监管机构有权通过信息保护审计的形式对“控制者”以及“处理者”展开调查；

监管机构有权进入“控制者”以及“处理者”的任何营业场所，调查其内的任何数据处理设备。

## 处罚权

监管机构有权强制性执行暂时或永久性的限制性措施，例如：禁止个人信息的处理；

监管机构有权强制性执行行政罚款（最大处罚金额详情请参考后续章节）.....

## 其他权力（授权、咨询等）.....

# 欧盟一般数据保护条例(GDPR)的要点概述 (续)

若干GDPR技术规定，在**企业合规过程中必须进行重点考虑**但在合规落地过程中影响广泛的要点：

- **“被遗忘权 ( The right to be forgotten ) ”**
  - 即个人数据删除权。个人可以随时要求掌握数据的企业删除数据，如果数据被传递给了任何第三方（或第三方网站），该第三方也应立即删除数据。
- **“可转移数据权 ( Right to data portability ) ”**
  - 个人拥有向处理其个人信息的企业获取其个人信息，并将个人信息直接从该企业转移到其他企业的权利。
- **“产品设计环节的数据保护 ( Privacy by design and default ) ”**
  - 企业在采用一个新的科技手段、新的服务或产品时，应该考虑到个人信息保护的问题，并落实相关的信息保护机制，以确保新的服务和产品不会构成对个人信息的侵犯。
- **“记录数据的处理 ( Record of processing activities ) ”**
  - 企业需对其个人信息的收集、处理、使用等过程保存完整的记录，以备查询。

# 欧盟一般数据保护条例(GDPR)的要点概述 (续)

- **赔偿责任**

- 每个个人均拥有向GDPR监管机构提出投诉、并获得有效的法律补偿方法的权利。
- 由于违反GDPR相关规定而导致个人受到严重的或其他不同程度的损失，该个人有权向企业获取相关赔偿。**如果个人信息处理涉及多家企业或组织。每家企业均有责任赔偿该个人的相关损失。**
- 欧盟成员各国需制定其他处罚细则，惩处违反GDPR相关规定的行为。

- **最大处罚金额**

- 根据所触犯条款的不同，GDPR设置了两个阶段的最大处罚金额。
- 分别为：最大处罚金额1000万欧元或是企业全球年度收入的2%（选其中较高的数字）；以及**最大处罚金额2000万欧元或是企业全球年度收入的4%（选其中较高的数字）**
- |                      |                 |
|----------------------|-----------------|
| ○ 违规的性质、严重程度和违规的持续时间 | ○ 受到影响的个人资料的种类  |
| ○ 违规是故意的还是因疏忽而造成的    | ○ 个人遭遇损害的程度     |
| ○ 对个人身份信息的责任和控制程度    | ○ 为了减轻损害而采取的行动  |
| ○ 违规是单个事件还是重复事件      | ○ 由违规产生的财务预期或收益 |

- **对企业品牌的影响**

- 除上述经济面的影响外，**诉讼以及一系列媒体对事件的报道，有可能造成潜在的重大品牌受损。**

# 欧盟依据GDPR的罚款案例



- 葡萄牙一家医院因为病人数据泄露被罚款400,000€



- 澳洲酒吧因为违法监控被罚款40,000€



- 德国一家社交APP因为使用明文传输被罚款40,000€



- 法国一家电商因为泄漏用户购买记录被罚款400,000€



# GDPR的合规不是单纯的配置硬件，或者是法律条文的匹配等技术问题

## 客户常见问题：

- 安防设备的性能不足
- 软件缺乏更新，漏洞或过时的系统平台
- GDPR合规设计功能缺失，不完善的代码使用
- 不同安全要求的网段划分不完善
- 管理制度不完善

而是一个综合持续的管理改善问题。



# 如何应对挑战？

—— 选择TUV莱茵的隐私保护咨询服务。我们与众不同之处: 丰富的数据隐私保护经验，最先接触GDPR修订的认证机构

TUV莱茵是德国专业的技术认证组织机构提供IOT物联网隐私保护认证的专业服务的组织，具有欧盟工业4.0下的IOT物联网安全认证资质，是最先接触GDPR修订的技术认证机构



## LEGAL DISCLAIMER

This document remains the property of TÜV Rheinland. It is supplied in confidence solely for information purposes for the recipient. Neither this document nor any information or data contained therein may be used for any other purposes, or duplicated or disclosed in whole or in part, to any third party, without the prior written authorization by TÜV Rheinland. This document is not complete without a verbal explanation (presentation) of the content.

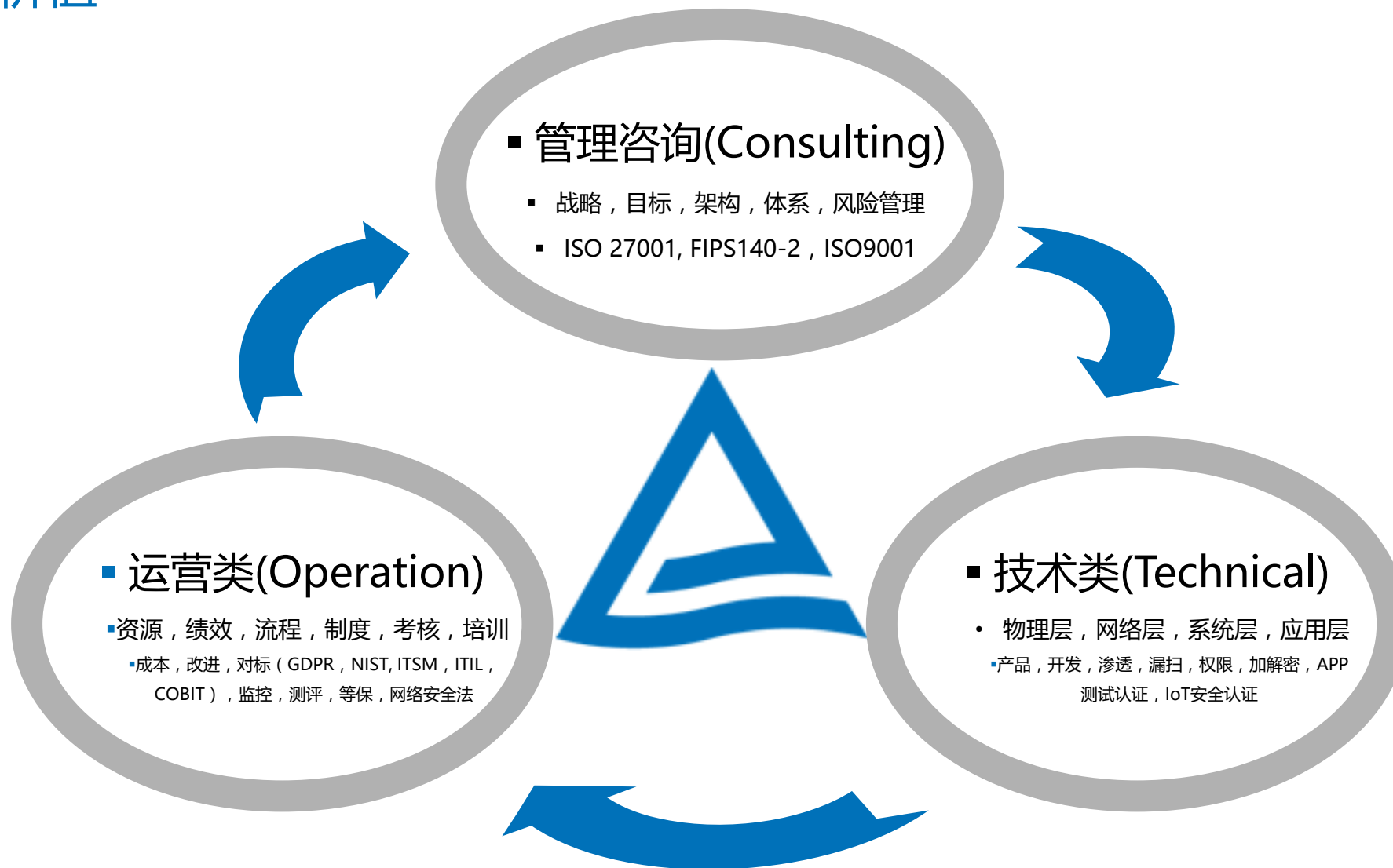
TÜV Rheinland AG

# 我们应对挑战的思路

我们会从管理，技术，运行三个方面对整体的GDPR合规水平进行合规评估。

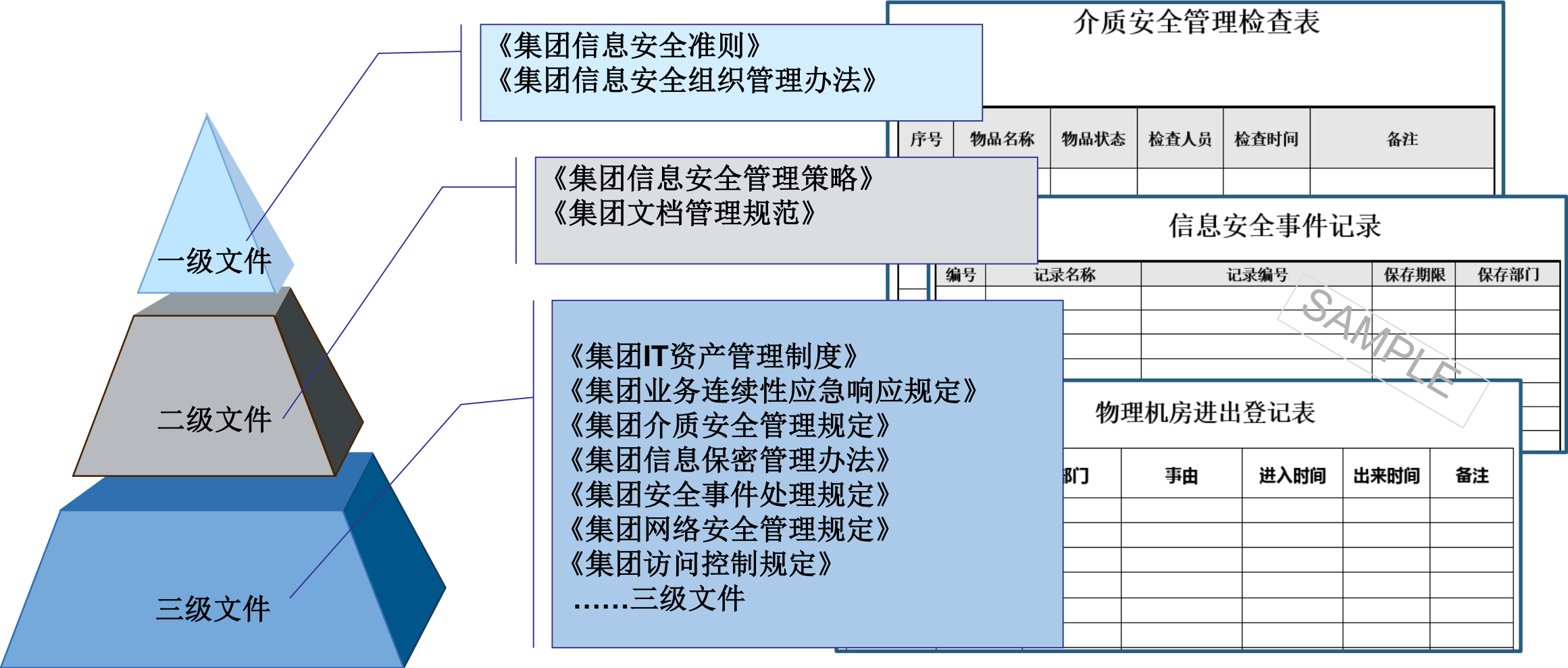


# 综合价值

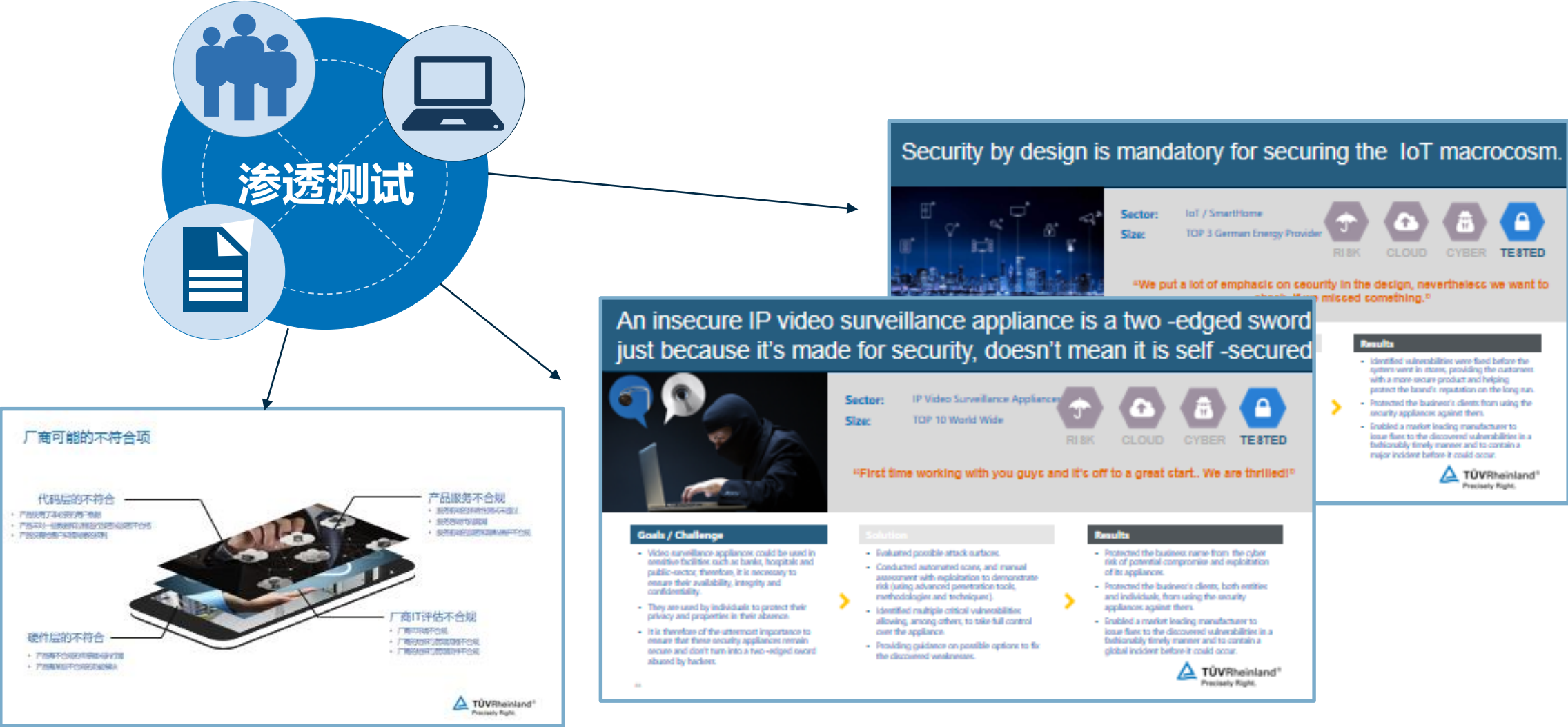


# 管理体系重点—制度体系（管理主线）

为了使信息安全管理系统的完备性、安全性、可控性，可维护性能统一规范管理，制定三级文档管理体系。



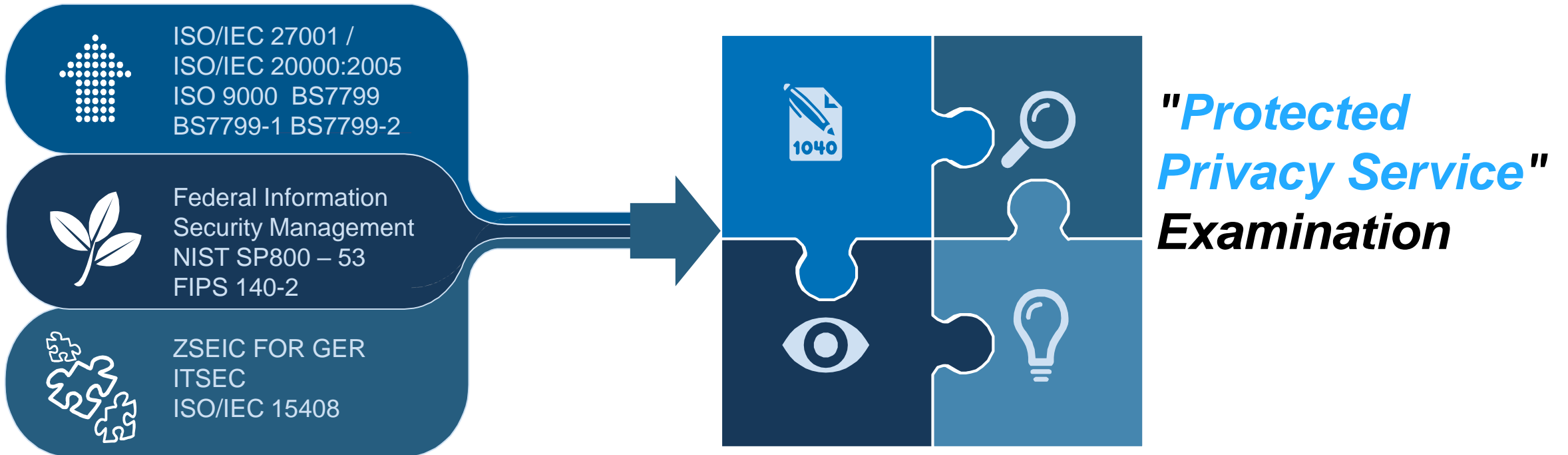
# 技术体系的建设基础渗透测试--（技术主线）




# 运行体系主线建设方法（运行主线）



以ISMS为基础，结合多个世界公认的管理标准要求，结合隐私保护要求，在组织的质量管理方法和标准内结合质量管理思想，配合客户提供的流程和测评的最佳实践经验结合形成隐私保护矩阵。



# GAP Analysis Requirements

|   |   |  |
|---|---|--|
| TÜV Rheinland i-sec GmbH  | Protected Privacy IoT Service   |  TÜVRheinland®<br>Genau. Richtig. |
| Table of Contents   |   |  |
| 1   | Motivation for the "Protected Privacy IoT Service" Examination .....          | 4  |
| 2   | Prerequisites for the examination .....                                       | 5  |
| 3   | Test information .....  | 6  |
| 4   | Scope of the service examination .....  | 7  |
| 5   | Requirements.....   | 8  |
| 5.1   | Cryptography Requirements .....   | 8  |
| 5.2   | Requirements of the Service Provider's Network Architecture .....             | 9  |
| 5.3   | Requirements relating to the Service Provider's Use of IaaS services .....    | 9  |
| 5.4   | Data Storage and Data Communication Requirements.....                         | 10   |
| 5.5   | Requirements on the Conformity Certificate of IoT Devices .....               | 10   |
| 5.6   | Requirements of the Service Provider's Databases .....                        | 11   |
| 5.7   | Configuration Requirements of the Service Provider's Network Components ..... | 12   |
| 5.8   | Configuration Requirements of the Service Provider's Systems.....             | 12   |
| 5.9   | Requirements on the Conformity Certificate of the IoT Configuration.....      | 13   |
| 5.10  | Identity and Authorization Management Requirements.....                       | 13   |
| 5.11  | Web Application Requirements.....   | 14   |
| 5.12  | Mobile Applications (Android, iOS) Requirements.....                          | 15   |
| 5.13  | Requirements of the Service Provider's Physical Security .....                | 15   |
| 5.14  | Data Center Availability Requirements.....                                    | 16   |
| 5.15  | Service Provider Back-up Requirements .....                                   | 16   |
| Version 0.97 (Entwurf)      No part of this document may be reproduced.      Page 2 of 24 |   |  |

## 5 Requirements

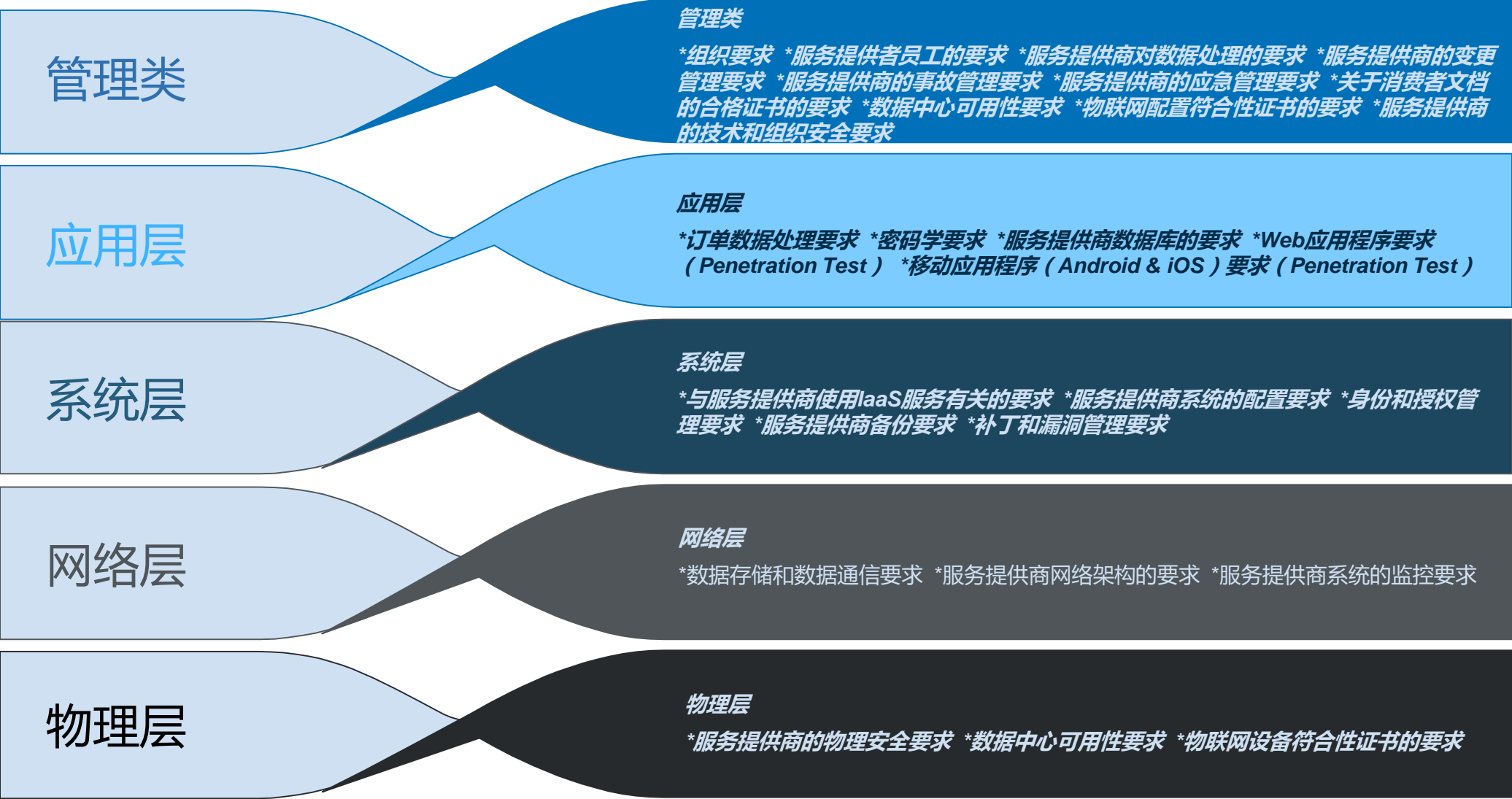
This section outlines the main requirements of the service, the underpinning processes and necessary hardware. The data protection requirements are also enumerated. The description focuses solely on the key aspects. The aspects for examination are detailed in the Inspection Catalogue.

***For this purpose, the requirements from this Inspection Catalogue are oriented to the following standards:***

- *the European General Data Protection Regulation (GDPR)*
- *Cloud Computing Compliance Controls Catalogue (C5), German Federal Office for Information Security (BSI)*
- *Technical Guideline TR-02102 Cryptographic Mechanisms: Recommendations and Key Lengths, German Federal Office for Information Security (BSI)*



# 运行中GDPR的差异分析（GDPR隐私保护分析重点）

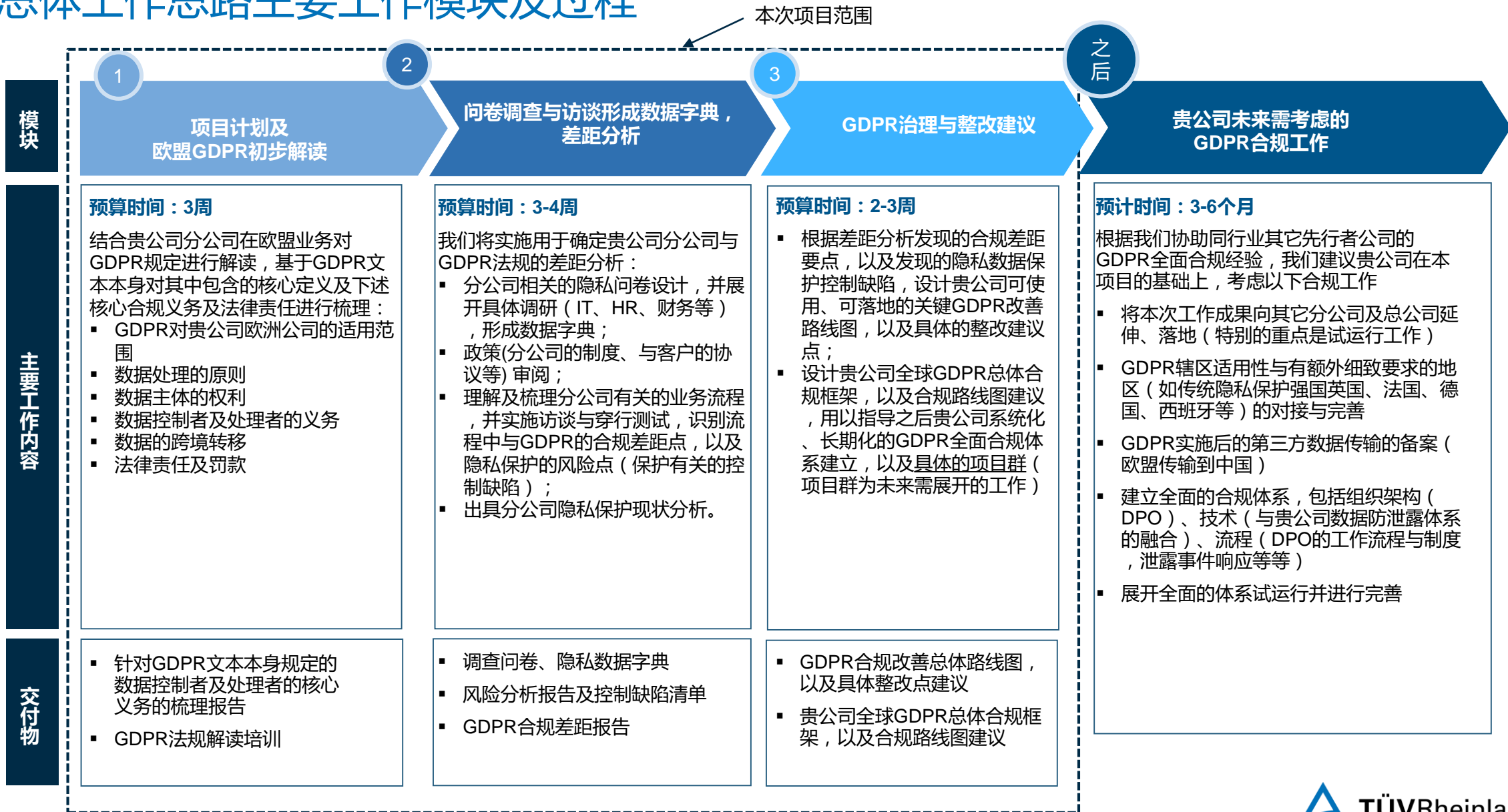


# 管理建议 – 制度和流程: 数据保护制度 ( 例 )

| Regular review & update; communication & training; testing/assurance                      |  |   |  |  |
|---|--|---|--|--|
| Registers   | Policies   | Processes & Procedures  | Governance   | Evidence   |
| Registers should be kept at all business levels and collated into a group level register. | Policies should be organisation-wide, however there may be exceptions or different policies for specific business areas/jurisdictions. | Processes and procedures should be standardised, uniformly applied and documented across the organisation. Where exceptions exist, these should be clear and readily available. | Governance documentation should be kept for each relevant level of the organisation, feeding into a set of group level governance documentation. | Evidence documentation should be kept at all levels where it is required to maintain an audit trail for each conducted action. |
| Information asset register  | Data protection policy   | Breach handling & escalation procedures   | Roles & responsibilities descriptions  | Documentation of responses to law enforcement requests   |
| Register of personal data processing activities   | Information security policy  | Privacy risk assessment procedures  | Steering committee terms of references   | Record of staff involved in fulfilling processing activity   |
| Register of third party recipients of data  | Information classification and handling policy   | Data Protection Impact Assessment procedures  | Documented control framework   | Documentation of regulatory challenge and response   |
| Corporate risk register   | Acceptable use policy  | Procedure for regulatory intervention & liaison   | Design review boards   | Documentation of works councils consultation   |
| Register of retention schedules   | BYOD policy  | Project/change management procedures  | Organisational structure & reporting lines   |  |
| Risk event logs   | Social media policy  | Procurement procedure   |  |  |
| Data flow maps  | Employee handbook  | Authorisation & sign-off procedures   |  |  |
| Business functions register   | Procurement policy (including due diligence)   | Complaints handling procedures  |  |  |
| Register of outsourced arrangements   |  | Assurance & testing procedures  |  |  |

**Please note – Some of these documents are group-level documentation, while others would be required at various levels of the business. The documents and processes recommended are indicative of best practices and are not exhaustive in nature.**

# 总体工作思路主要工作模块及过程

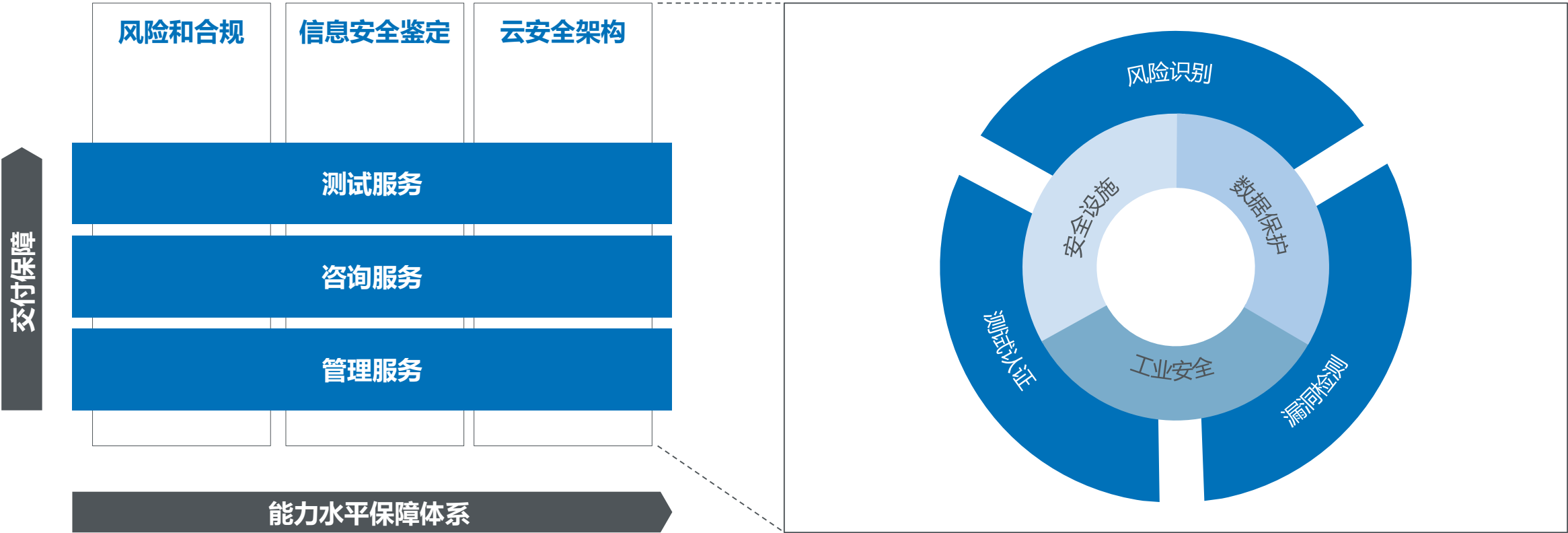


# 安全组合概述-关键功能

莱茵TUV拥有147年的系统测试和认证经验，是全球最全面的信息安全认证团队。

全球一致的信息和通信技术标准

一流的服务



通过对于数据管理成熟度的分析和各项指标的诊断，提供体系优化建议与发展路径

在完善数据保护管理体系阶段，我们会结合之前的工作，输出问题发现以及整改建议，战略规划，以及针对关注核心问题制定优化方案，提出整改意见并并协助完成数据保护管理制度文档编修。

基于成熟度模型和评估指标的评估结果

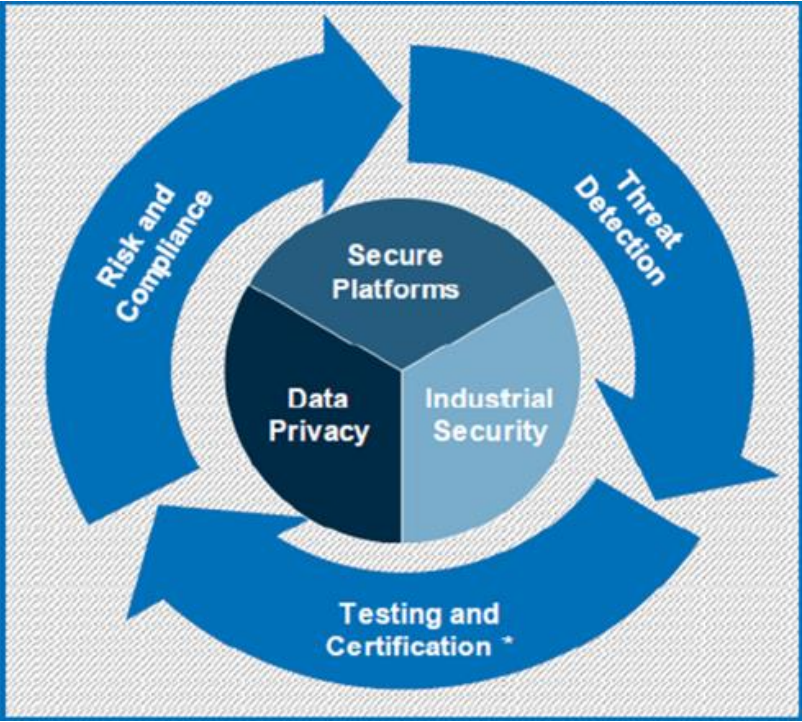
| 特征编号   | 指标特征描述                                  | 特征符合度 | 证据/说明    | 符合度调整 | 调整原因                                   | 分值  |
|--------|---|-------|----------|-------|--|-----|
| 1      | BCM体系战略与规划                              |       |          |       |  | 4.3 |
| 1.1    | BCM体系发展战略                               |       |          |       |  | 4.2 |
| 1.1.1  | BCM战略根据业务发展总体目标及经营规模制定                  | 完全满足  |          | 完全满足  |  | ●   |
| 1.1.2  | BCM战略根据风险控制的基本策略和风险偏好制定                 | 完全满足  | 领导小组会议纪要 | 完全满足  |  | ●   |
| 1.1.3  | BCM战略经过董（理）事会的审核和批准                     | 不满足   |          | 不满足   | 未提出具体审核批准要求，也未提供BCM战略经过董（理）事会的审核和批准记录。 | ●   |
| 1.1.4  | BCM战略应包括组织短期、中期和长期业务连续性目标               | 完全满足  | BCM三年规划  | 完全满足  | 《招商银行业务连续性管理工作三年规划》中已涵盖该内容。            | ●   |
| 1.1.5  | BCM战略应包括识别和利益相关方的重要性，影响业务中断事件损害程度与范围的判断 | 部分满足  | ?        | 完全满足  | 有明确分级                                  | ●   |
| 1.1.6  | BCM战略应包括将业务连续性管理纳入全行风险管理体系              | 部分满足  |          | 部分满足  | 实际未明确纳入                                | ●   |
| 1.1.7  | BCM战略应包括切实履行社会责任，保护客户合法权益，维护金融秩序的原则     | 完全满足  |          | 完全满足  |  | ●   |
| 1.1.8  | BCM战略应包括坚持预防为主，建立预防、预警机制，将              | 完全满足  |          | 完全满足  |  | ●   |
| 1.1.9  | BCM战略应                                  |       |          |       |  |     |
| 1.1.10 | BCM战略应                                  |       |          |       |  |     |
| 1.1.11 | BCM战略应                                  |       |          |       |  |     |
| 1.1.12 | BCM战略应                                  |       |          |       |  |     |

示例

| BCM体系评估关键领域 |           |
|-------------|-----------|
| 领域编号        | 评估领域名称    |
| 1           | 体系战略与规划   |
| 2           | 组织架构与职责   |
| 3           | 管理办法与策略   |
| 4           | 体系建设需求分析  |
| 5           | 体系资源建设与保障 |
| 6           | 业务连续性预案体系 |
| 7           | 演练验证与持续改进 |
| 8           | 监管报告与监控审计 |

示例

数据保护管理体系的发展路径



管理体系优化

架构、制度以及流程优化建议

BCM管理制度文档优化整改

| 编号     | 能力项       | 评估要素                                       | 检查点说明   |
|--------|-----------|--|---|
| 3      | IT 能力管理   | 评估IT 能力管理的需求分析工作全面性、合理性和适用性，包括：业务影响分析和风险评估 | 在管理实践中，对业务影响分析的目的、范围、工作方法、输出结果、实施规划、负责岗位有明确定义   |
| 3.1    | 制度规范      | 制度规范                                       | 近三年开展过以信息系统中断为场景的业务影响分析工作，并形成分析报告文档记录   |
| 7      | IT 能力管理流程 | 评估在IT 能力管理中对外部相关方的全面性、合理性和适用性              | 从有文件化的业务影响分析方法，使业务人员能够掌握在信息系统中面对业务影响分析，可看到以下内容：<br>- 对重要业务，明确重要业务在信息系统中<br>- 对重要业务运营流程的信息系统<br>- 对重要业务运营流程的信息系统 |
| 7.1    | 应急响应计划与流程 | 应急响应计划与流程                                  | 应急响应计划与流程   |
| 7.1.1  | 应急响应计划与流程 | 应急响应计划与流程                                  | 应急响应计划与流程   |
| 7.1.2  | 应急响应计划与流程 | 应急响应计划与流程                                  | 应急响应计划与流程   |
| 7.1.3  | 应急响应计划与流程 | 应急响应计划与流程                                  | 应急响应计划与流程   |
| 7.1.4  | 应急响应计划与流程 | 应急响应计划与流程                                  | 应急响应计划与流程   |
| 7.1.5  | 应急响应计划与流程 | 应急响应计划与流程                                  | 应急响应计划与流程   |
| 7.1.6  | 应急响应计划与流程 | 应急响应计划与流程                                  | 应急响应计划与流程   |
| 7.1.7  | 应急响应计划与流程 | 应急响应计划与流程                                  | 应急响应计划与流程   |
| 7.1.8  | 应急响应计划与流程 | 应急响应计划与流程                                  | 应急响应计划与流程   |
| 7.1.9  | 应急响应计划与流程 | 应急响应计划与流程                                  | 应急响应计划与流程   |
| 7.1.10 | 应急响应计划与流程 | 应急响应计划与流程                                  | 应急响应计划与流程   |
| 7.1.11 | 应急响应计划与流程 | 应急响应计划与流程                                  | 应急响应计划与流程   |
| 7.1.12 | 应急响应计划与流程 | 应急响应计划与流程                                  | 应急响应计划与流程   |

示例

# TÜV莱茵: 是你项目成功过程中最值得信赖的伙伴, 我们期待和客户共同成长



**经验：**数据保护项目中丰富的技术经验和实施经验



**权威：**所有的认证方法均来自GDPR的主导国德国



**独立：**独立第三方认证机构



**标准一致：**全资子公司, 全球一致的数据保护认证方法



**丰富的成果：**不同行业中丰富的GDPR项目实施经验

- 600 Security Experts
- \$2.3 Billion
- Privately Held
- 147 Years Old
- 500 Locations
- 69 Countries
- 19,320 people





# 总结

GDPR作为中国企业走向欧洲市场必须的合规要求，我们会在专业的层面上为客户解决实际的困难，并协助客户共同应对合规道路上的挑战。