2018国际研究机构数据安全治理框架解读

演讲人：谷安天下CTO 陈伟

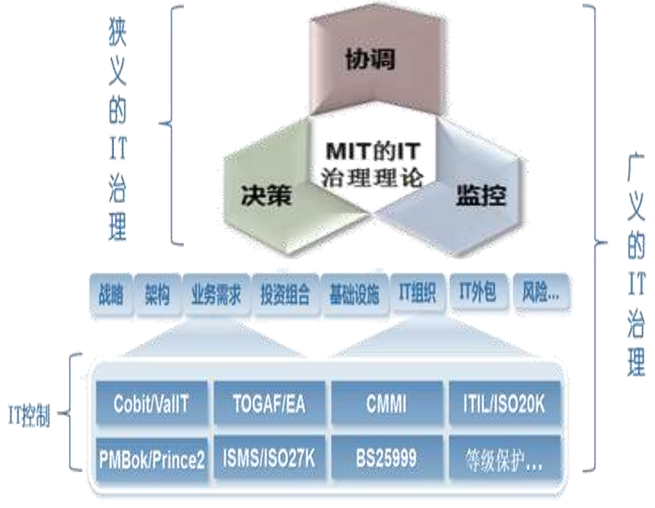
目 录

一、从IT治理到数据安全治理

- **新技术环境下IT治理的变革趋势**

✓传统的IT治理是指组织在信息化过程中需要建立的一种宏观的决策、协调及控制机制，其作用是明确IT决策责任、建立协调沟通机制，有效利用各种资源，控制信息化风险，促进IT与业务的融合，使IT为企业创造价值；新技术环境下对IT治理提出了如下图所示的新的要求和目标。

传统IT治理内容



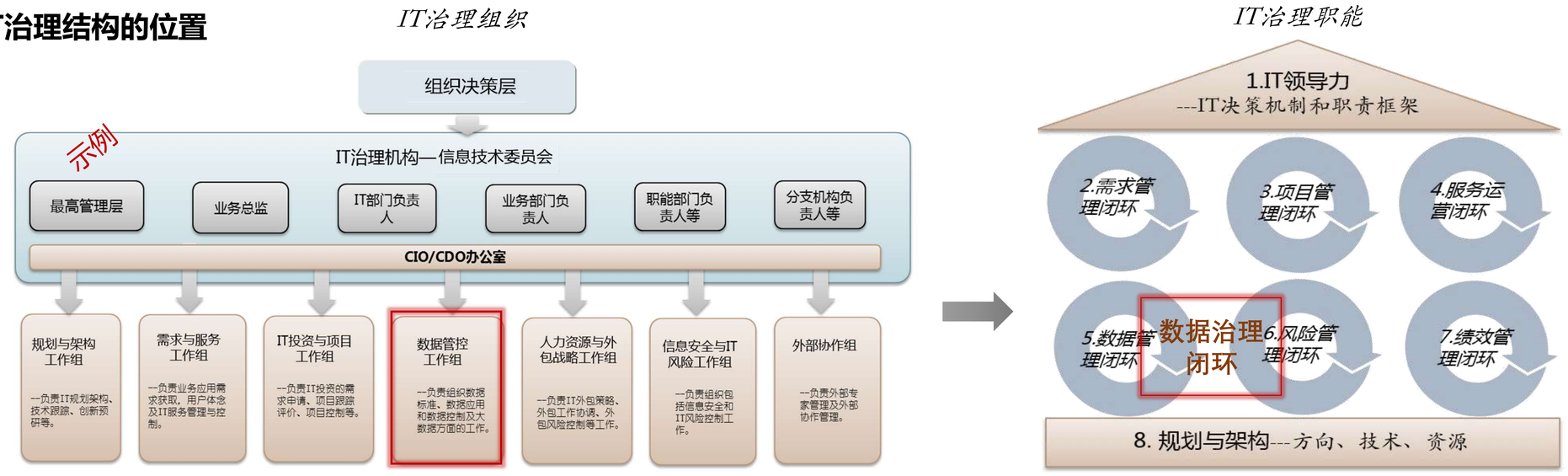
新型IT治理机制

- 推进IT科学决策
- 协助跨部门沟通
- 高效的需求管理
- 优化IT投资管理
- IT支持业务创新
- **新时期信息安全**
- 新技术跟踪预研
- IT绩效机制建立
- IT人才引进政策

新型IT治理目标

- 提升战略迅速决策能力
- 完善需求有效把握能力
- 促进项目快速实施能力
- 优化系统部署服务能力
- **建立自适应信息安全能力**
- 培育IT投资管理能力

- **数据治理在IT治理结构的位置**



- **数据安全治理是数据治理的重要内容**

IT治理机构/CIO

首席数据官CDO

数据治理体系

数据生产者
数据生产
数据质量初审
数据质量绩效执行

生产

数据使用者
数据使用
数据统计分析
数据质量绩效执行

使用

数据应用支撑平台

数据拥有者
数据owner
数据挖掘
数据质量绩效评估

挖掘

数据管理者
数据管理
数据安全保护
数据质量绩效执行

管理

数据安全治理体系

数据生命周期安全

数据通用安全

数据安全治理机制

二、Gartner的数据安全治理

- **Gartner的数据安全治理(DSG)的概念**

✓国际知名的IT咨询与研究机构Gartner认为，当前数字业务正在为企业创造价值，但不能忽视不断增长的业务风险和责任。安全和风险管理领导者应该制定适当的数据安全治理框架，以减轻安全威胁、数据驻留和隐私问题带来的风险。

数据安全面临的挑战

- 新的数据和隐私保护的合规要求
- 网络攻击造成的数据泄露破坏了组织声誉和客户信任
- 混和IT架构环境下缺乏通用的数据安全策略
- 数据安全和身份管理产品不会整合甚至不共享通用策略

DSG的定位

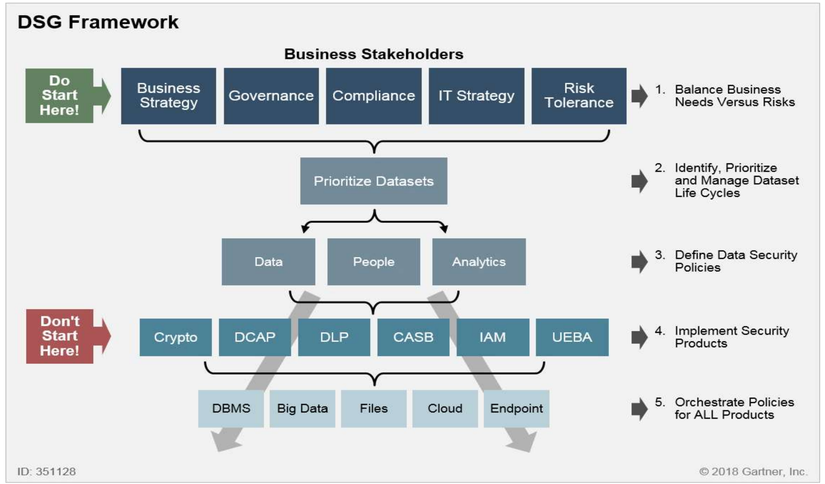
DSG的主要目标

- 协调信息治理和信息安全治理
- 使数据分类、数据生命周期管理与数据安全管理的方法保持一致
- 以数据财务分析作为数据资产使用和管理责任的基础

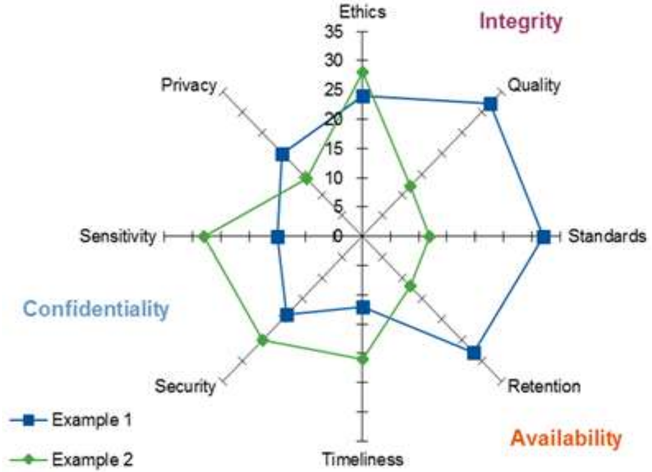
- **Gartner数据安全治理DSG框架**

✓Gartner于2018年4月提出了数字安全治理DSG框架，目的是为了对业务风险进行优先级排列，然后采取适当的安全措施对业务风险进行控制。DSG要先从组织的高层业务风险分析出发，对组织业务中的各个数据集进行识别、分类和管理；针对数据集的数据流和数据分析库的机密性、完整性、可用性创建8种安全策略；根据策略落实管理措施和部署安全技术产品加以控

DSG框架



安全策略的8个方面

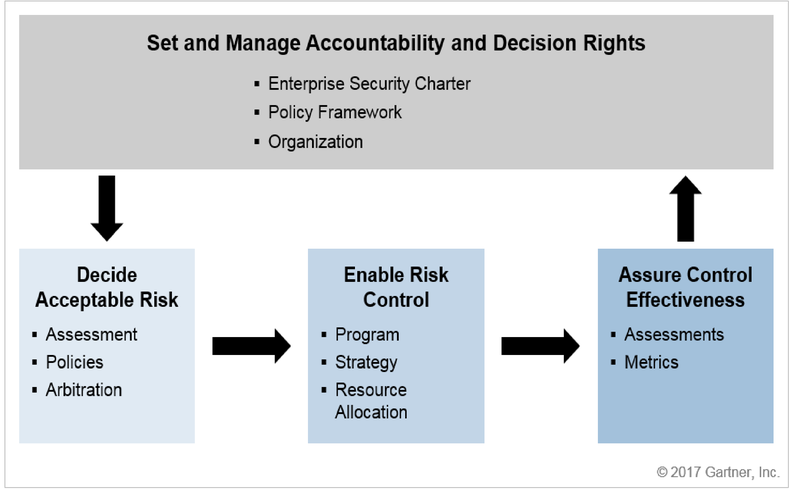


•Gartner预测，到2021年，超过30%的企业将实施数据安全治理框架，这一比例目前的不足5%。

- **DSG的数据安全决策机制与职责分配框架**

✓DSG最重要的就是要形成组织高级管理层及各类部门参与的安全决策机制，落实决策权的归属和职责担当的框架，使得数据安全是全范围组织内的重要事项，数据安全参与重大决策并纳入到组织总体战略规划与资源计划中。

数据安全决策机制



数据安全职责分配机制

Role	Assess Risk	Manage Risk	Fund Resources	Implement	Assure
Data Owner	I	R, A	R, A	A	A
IT	I	C	I	R	I
Operational Risk	R, A	I	I	I	C
Security	C	C	I	I	R

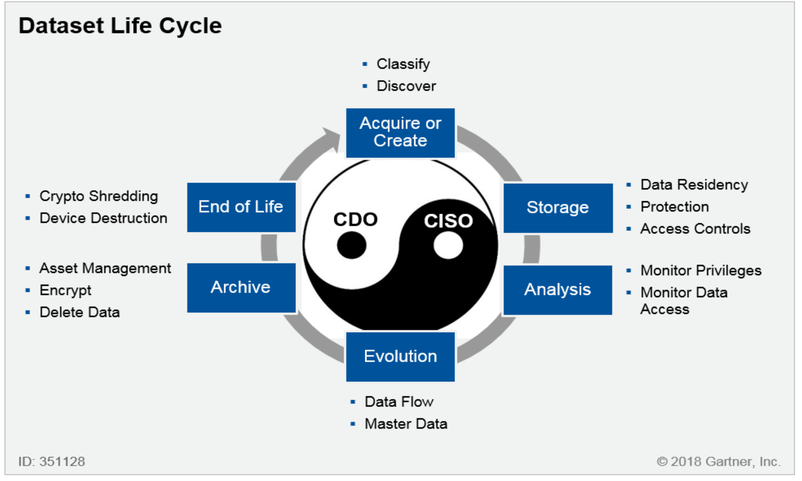
Responsible: Person or function responsible for executing the activity
Accountable: Person or function that owns the activity, approves work and is held accountable for it
Consulted: Person or function with information relevant to the activity
Informed: Person or function to be informed of progress and results

Data Owner

- **DSG推荐用数据生命周期法来识别与管理数据**

✓DSG框架建议数据管理与信息安全管理两组团队针对整合的业务数据生命周期过程进行业务影响分析(BIA), 发现的各种数据隐私和数据保护风险,以降低整体的业务风险。

数据生命周期中的六个环节



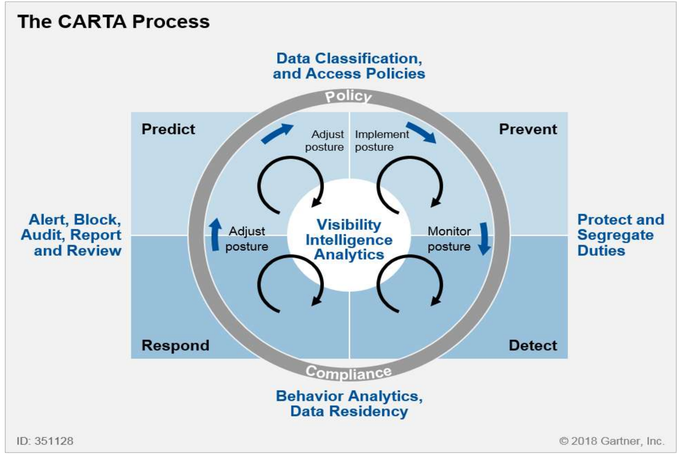
数据生命周期中管理要点

- 利用应用数据发现技术为每个数据集的容量、变化和准确性确定范围。
- 识别每个数据集产生的业务风险和财务影响并确定优先顺序。
- 检查影响每个数据集的数据存储涉及法律合规问题。
- 应用数据分类和主数据策略来优先确定哪些数据集需要安全性。
- 为每个数据集创建访问和使用策略，并确保这些策略在所有可用数字业务环境保持一致。

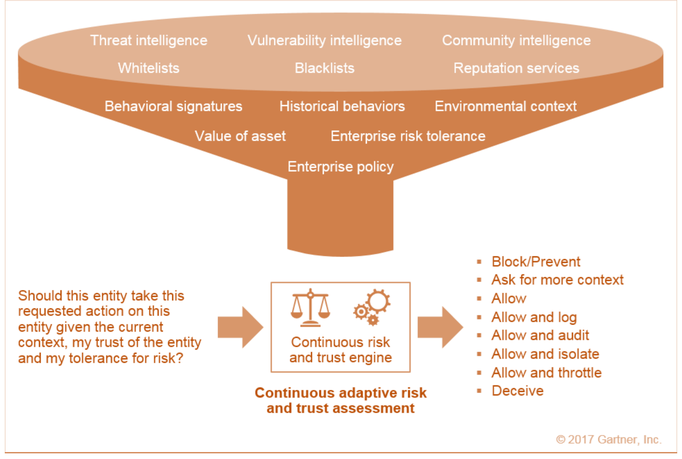
- **DSG推荐用CARTA模型来保护数据安全**

✓2017年Gartner提出了持续自适应的安全风险和信任评估模型（CARTA），旨在使安全与风险管理的领导者在持续的和自适应的风险与信任评估的基础上，对于实时出现的各类事件做出及时和合理的反应，在风险可接受的程度上保障数字业务的健康运行。CARTA的方法同样适用于数据安全评估与控制.

数字风险管理CARTA模型



CARTA模型的核心--基于大数据分析与评价的动态安全决策



三、Microsoft的数据安全治理

- **Microsoft的数据安全治理**

✓微软开发了一个针对隐私，保密和合规性（DGPC）的数据治理框架，以帮助组织更好进行数据安全风险控制。 DGPC框架围绕三个核心能力领域：人员、流程和技术。

Microsoft的DGPC框架

DGPC的主要目标

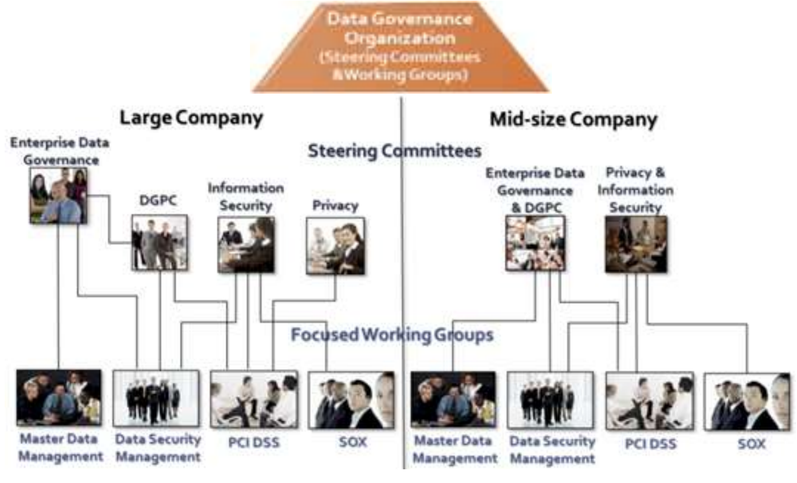
- DGPC框架重点放在数据安全的“树状结构”上，以识别和管理与特定数据流相关的安全和隐私风险需要保护的信息，包括个人信息、知识产权、商业秘密和市场数据等。
- DGPC框架创建了一个环境，可识别网络安全威胁和隐私泄露威胁，例如违反客户选择和同意原则而带来的风险，以及以及如何使用、处理和共享隐私信息等。
- 可以与组织现有的IT管控框架（如COBIT、ISO27001、PCI DSS等）协同工作。

- **DGPC在”人员”领域的控制要求**

✓有效的数据安全治理要求建立适宜的组织架构和人员设置。DGPC把数据安全相关的组织分为战略层、战术层的操作层三个层次，每一层次都要明确组织中的数据安全相关的角色职责、资源配置和操作指南。

DGPC 金字塔

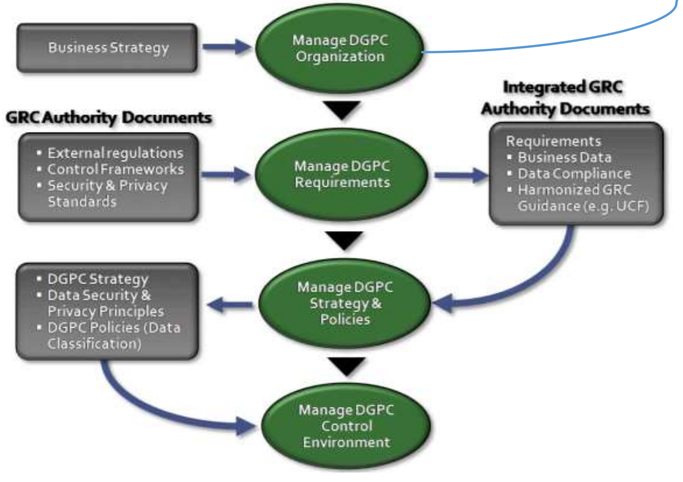
DGPC组织示例



- **DGPC在”流程”领域的控制要求**

✓有了合适的组织和人员，组织就可以专注于定义所涉及的数据安全管理流程。首先检查数据安全相关的各种法规、标准、政策和程序，明确必须满足的要求，并使其制度化与流程化，以指导数据安全实践；组织应该在特定数据流的背景下，在制度和流程指导下，识别数据安全威胁、隐私风险和合规风险，并确定适当的控制目标和控制活动。

DGPC制度与流程



“管理DGPC组织”的流程活动示例

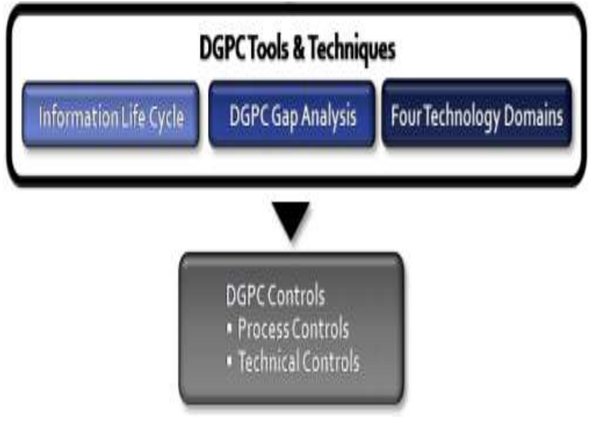
No.	Activity	Input	Output	Responsible Party
1.	Appoint executive leader to GRC council and define role and responsibilities	List of executive leader candidates	GRC council executive leader's role and responsibilities	Enterprise senior leadership team
2.	Define GRC council charter	Business strategy	GRC council charter	Enterprise senior leadership team
3.	Appoint GRC council members and define role and responsibilities	List of GRC council member candidates	GRC council members' role and	Enterprise senior leadership team
4.	Define GRC council goals and objectives			
5.	Appoint DGPC steering committee members			
6.	Define DGPC steering committee goals and objectives			
7.	Create focused working groups			
8.	Appoint focused working group members			
9.	Define focused working group goals and objectives			
10.	Report focused working group performance to DGPC steering committee			

No.	Activity	Input	Output	Responsible Party
		objectives		
11.	Respond to focused working group status report	Focused working group status report	Guidance to focused working group	DGPC steering committee
12.	Report DGPC steering committee performance to GRC council	Performance status of DGPC steering committee goals and objectives	DGPC steering committee status report	DGPC steering committee
13.	Respond to DGPC steering committee status report	DGPC steering committee status report	Guidance to DGPC steering committee	GRC council
14.	Report GRC council performance to enterprise senior leadership team	Performance status of GRC council goals and objectives	GRC council status report	GRC council
15.	Respond to GRC status report	GRC council status report	Guidance to GRC council	Enterprise senior leadership team

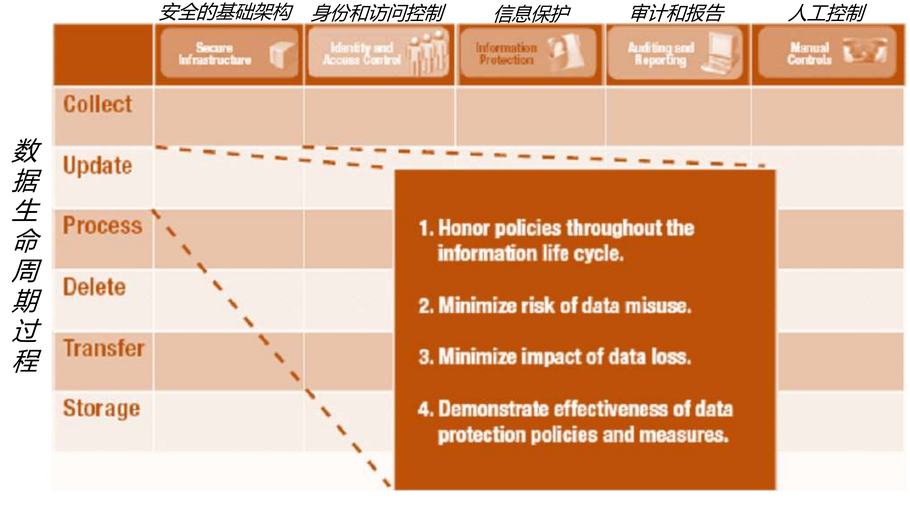
- **DGPC在”技术”领域的控制要求**

✓Microsoft开发了一种工具方法来分析与评估数据安全流程控制和技术控制存在的特定风险。这种方法需要填写一个称为安全差距分析表，该表围绕三个要素构建：信息生命周期，五种控制方法以及评估维度的数据隐私和保密原则。。

DGPC技术与工具

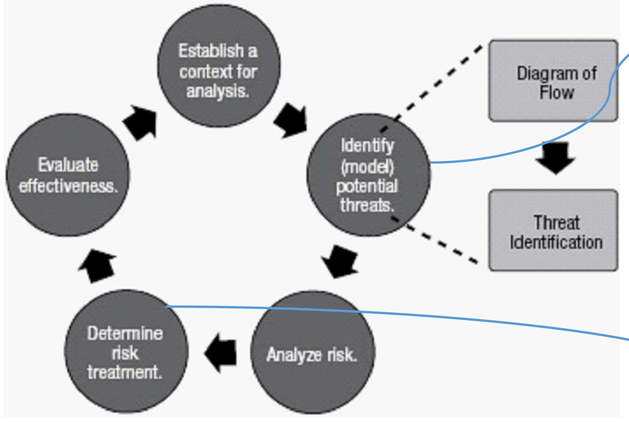


数据安全差距分析表

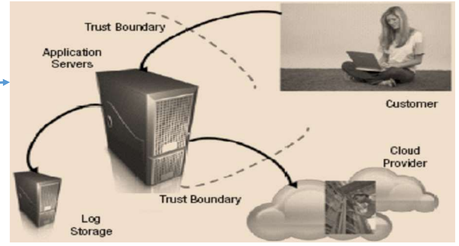


- **安全风险差距分析过程示例**

安全风险差距分析过程



识别潜在威胁



	Secure Infrastructure	Identity and Access Control	Information Protection	Auditing and Reporting	Manual Controls
Collect/ Update	*Servers are on regular OS and App. Patch cycle, and up to date in malware signatures.* *Incoming data are correctly classified and tagged as per customer choice and consent.*	**All transactions to take place on authenticated communications.**	*Choices are displayed and consent is obtained as per MPSD guide.* *Transaction log data are encrypted in transit and at rest.* **All material customer transactions arrive over encrypted communication channel.**	*All material transactions are to be logged as per logging framework.* *Communications channel and log servers are monitored. Failover process to local log servers in processor facilities is up and running.* **Alerts and alert recipients are defined and operational.** **Access and use reports, along with recipients and delivery schedules, are defined.**	**The escalation path for issues is defined.**

确定风险处置措施

四、数据安全治理的最佳实践

- **数据安全治理的通用框架**

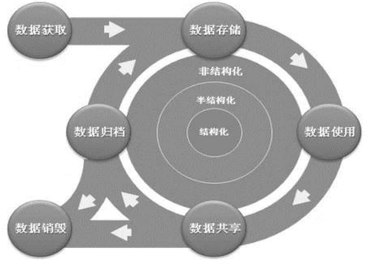
✓根据以上针对Gartner和微软数据安全治理方法的解读与分析，结合国内外其他数据安全标准及行业最佳实践，我们认为数据安全治理通用框架一般包括:数据安全治理机制、数据安全生命周期管理、数据安全技术部署等方面的内容。

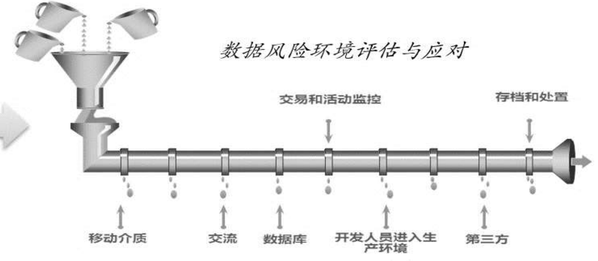
• 数据安全治理框架的应用

✓各类组织可以根据业务特征和数据安全要求，对通用数据安全治理框架进行补充或剪裁，以形成有自身特点的数据安全治理框架，以指导企业的数据安全工作。

某企业的数据安全治理框架示例

1.敏感数据分类分级	2.敏感数据控制机制	3. 全生命周期管理	4.技术手段保护机制	5. 检查审计持续改进
● 现有数据识别	● 归口管理机制	● 数据使用管理	● 网络区域隔离	● 内部合规检查
● 重要数据分类	● 申请审批机制	● 数据传输管理	● 应用访问控制	● 大数据安全评价
● 数据敏感分级	● 脱敏使用机制	● 数据存储管理	● 数据加密管理	● 实施外部IT审计
● 数据安全评估	● 隐私保护机制	● 备份销毁管理	● 操作日志审计	● 持续整改与完善





演讲人简介 - 陈伟

- 北京谷安天下科技有限公司CTO，国际注册信息系统审计师(CISA)，ISO27001主任审核员，国际信息系统审计与控制协会(ISACA)中国专家委员会副主席。
- 在企业信息化的系统集成、应用开发、信息安全与IT控制领域有超过二十年的工作经验，对国内大中型企业的IT规划架构、IT管控体系、信息安全体系与IT服务体系的设计与实施有着较丰富的经验。
- 目前工作领域集中于IT治理、IT风险管理、信息安全管理领域的方法研究与企业实践，并为多个大型组织实施过IT治理、信息安全、信息科技风险管理、IT审计等项目。
- 2006年至今担任北京大学兼职教授，为北京大学CIO高管班讲授《IT治理》、《信息安全管理》及《IT审计》课程；2007年至今担任谷安天下IT风险管理学院首席培训师，为3000多人次讲授《IT治理》、《IT审计》、《IT风险管理》、《信息系统审计师CISA认证》等课程。
- 联系方式：chenwei@gooann.com, 微信：cw1140772

THANKS