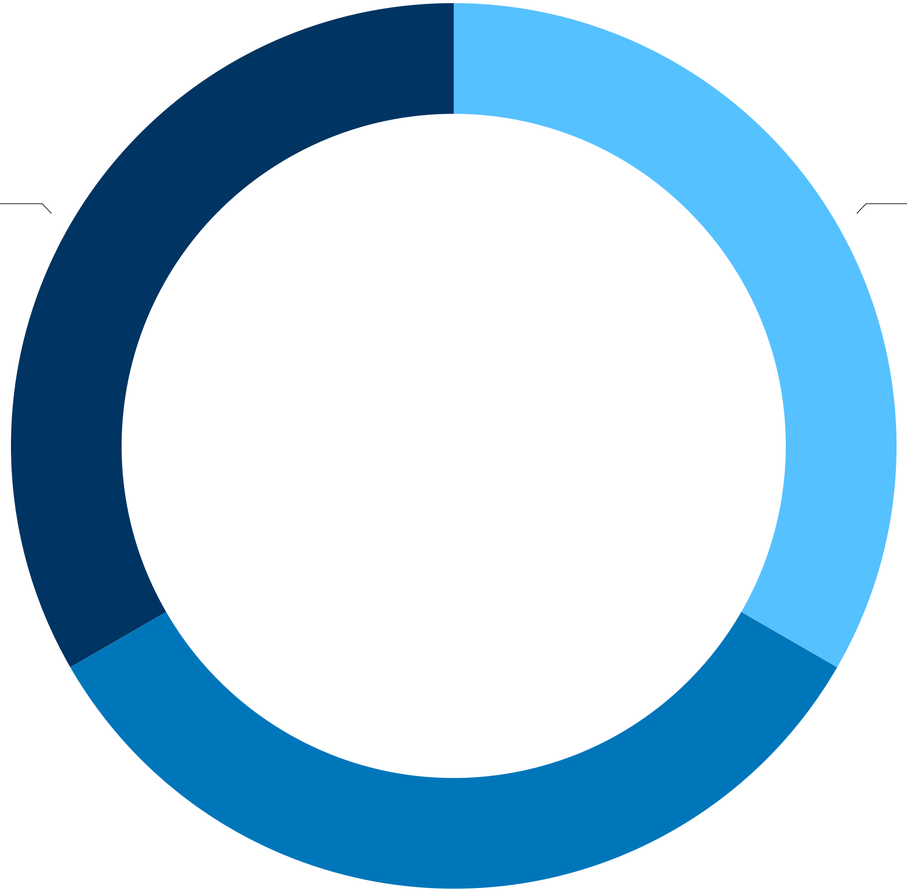
Framework for Improving Critical Infrastructure Cybersecurity
提升关键性网络安全基础设施的框架

网络安全框架的三大组成部分



框架核心
framework core

- 围绕特定结果而组织的网络安全活动和参考资料
- 使得关于网络风险的沟通在一个机构内成为可能

框架配置文件
framework profile

- 使行业标准和最佳实践情况与特定实施方案中的框架核心保持一致
- 把商业需求作为考虑因素的条件下，支持优先考虑与测量

框架实施层
framework implementation tier

- 描述了网络风险是如何被一个机构管理的，以及以及风险管理实践所展示出的关键特征的程度

框架核心

- 围绕特定结果而组织的网络安全活动和参考资料
- 使得关于网络风险的沟通在一个机构内成为可能

函数　　类

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
Protect	Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	COBIT 5 APO01.02, DSS06.03 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.3, A. 15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	COBIT 5 APO02.06, APO03.01 NIST SP 800-53 Rev. 4 PM-8
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	COBIT 5 APO02.01, APO02.06, APO03.01 ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 NIST SP 800-53 Rev. 4 PM-11, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established	ISO/IEC 27001:2013 A.11.2.2, A. 11.2.3, A.12.1.3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14

识别

保护

检测

响应

恢复

例如：

IDENTIFY识别	asset management资产管理	ID.AM
	business environment商业环境*	ID.BE*
	governance治理	ID.GV
	risk assessment风险评估	ID.RA
	risk management strategy风险管理策略	ID.RM
PROTECT保护	access control访问管理	PR.AC
	awareness and training意识与演习	PR.AT
	data security数据安全	PR.DS
	……	
	……	
DETECT检测	……	
	……	
	……	
	……	

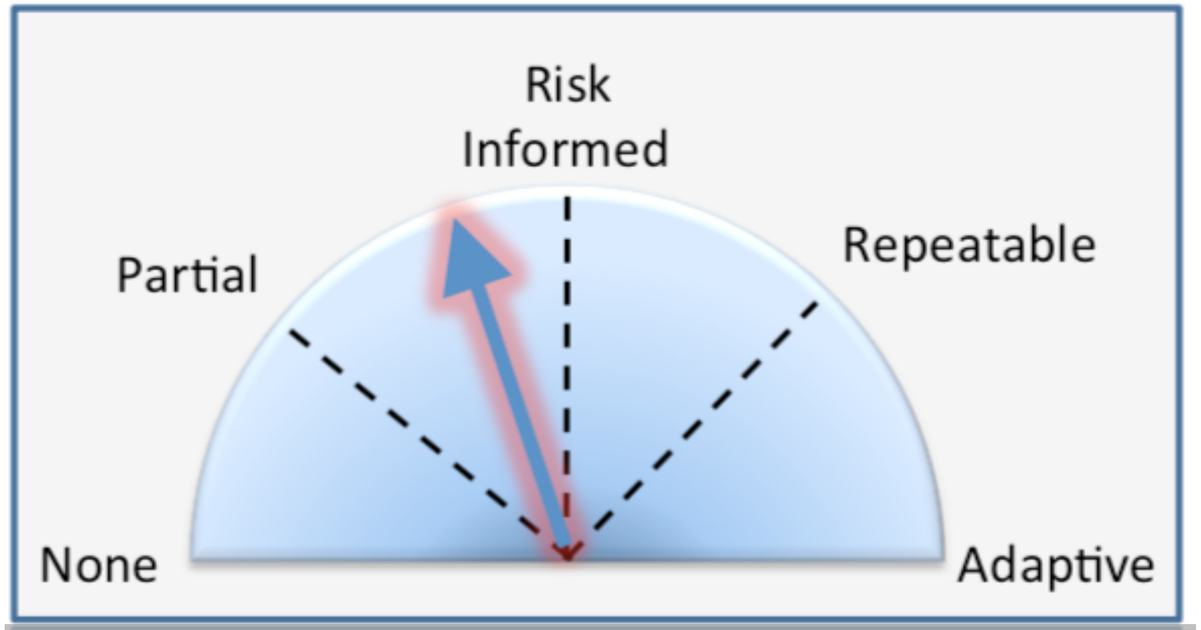
*在ID.BE下的五个亚类:

ID.BE-1：
在供需链中该组织的角色是已被辨识的且相连的(可沟通的)
informative references消息性参考:
COBIT 5 APO01.02, DSS06.03
ISA 62443-2-1:2009 4.3.2.3.3
ISO/IEC 27001:2013 A.6.1.1
NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
……

框架实施层

“描述了网络风险是如何被一个机构管理的，
以及风险管理实践所展示出的关键特征的程度。”

None->Partial	->Risk Informed->Repeatable	->Adaptive
无	部分的	风险被告知的	可重复的	适应性的
0	1	2	3	4



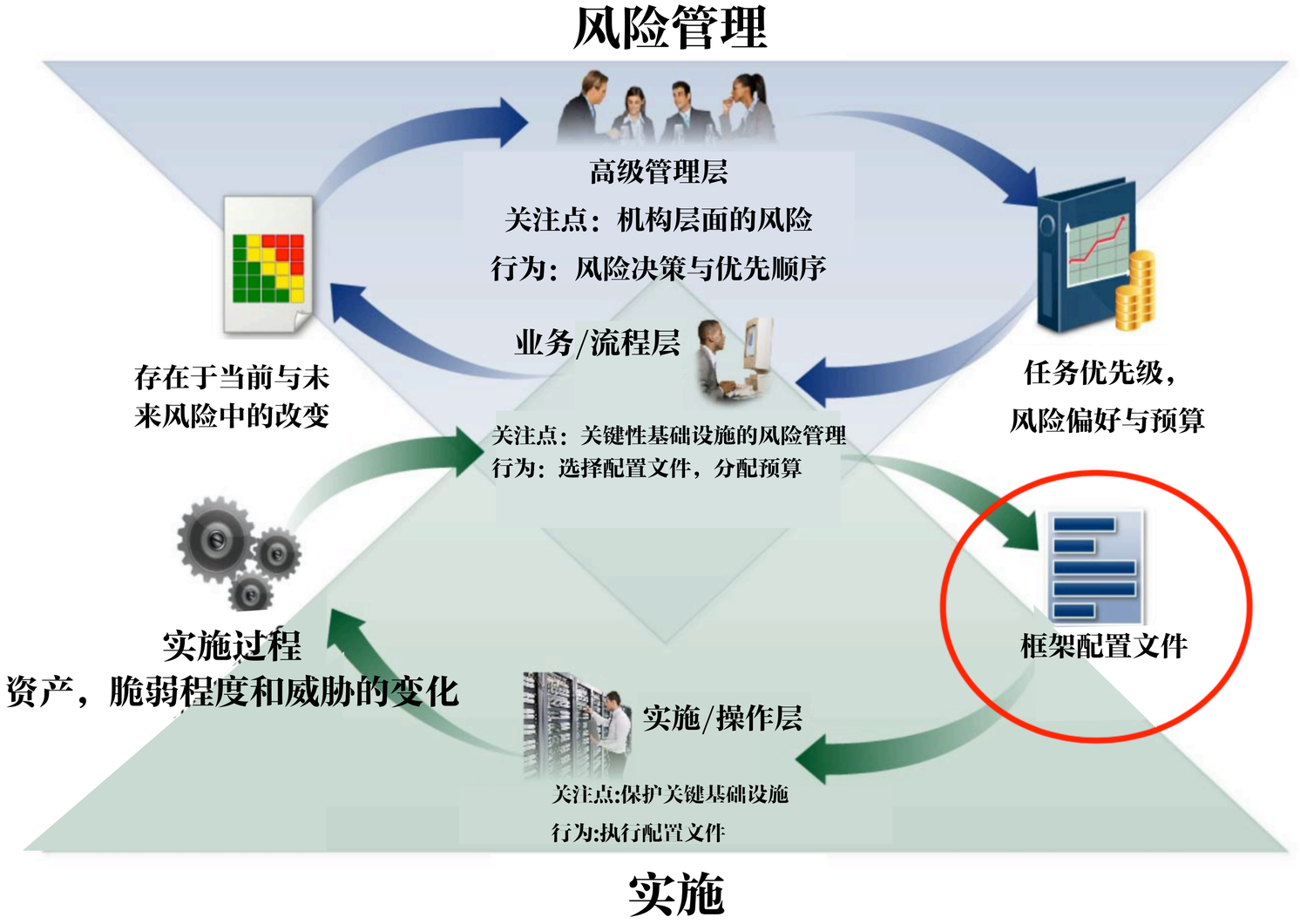
- 允许实施过程中的灵活性并且带入了成熟模型中的概念
- 反映了一个机构是如何实施框架核心方程并且管理其中风险的
- 范围逐步从部分的 (层1) 到适应性的 (层4)，其中每一个层都被建立在上一个层的基础上
- 特性在机构层级被定义，并且被运用到框架核心，以此来决定一个类 (category) 是如何被实施的

框架配置文件

1. 使行业标准和最佳实践情况与特定实施方案中的框架核心保持一致
2. 把商业需求作为考虑因素的条件下，支持优先考虑与测量

- 为已经给定的部分，分部门或者机构所定制的核心
- 商业/任务逻辑和网络安全结果的融合
- 操作性方法论与网络安全需求的结盟/一致性
- 评估和表达目标状态的根据
- 对网路安全风险管理决定的支持工具

利用配置文件联结优先顺序



通过三个步骤来构建一个框架配置文件

步骤一．任务列表 (包含：优先级+目标，…)

Mission	
Priority	Objective
1	A
2	B
3	C

Subcategory
1
2
3
…
98

步骤二.

网络安全需求：

法律法规，内外政策和最佳做法

步骤三. 操作方法论：在执行，管理和监测中的指导指引和方法

资源与预算的分配决定

Subcategory
1
2
3
…
98

ConfigServer Security&Firewall，是状态包检测（SPI）防火墙，登录/入侵检测和安全的Linux服务器的应用程序。是基于SPI的iptables防火墙，具有全面，直接，方便，灵活的配置。

- 如何运用一个CSF 配置文件?

subcategory 亚类别	priority 优先级别	gaps 间隔	year 1 activities 首年活动	year 2 activities 次年活动
1	中等	小		X
2	高等	大	X	
3	中等	中	X	
…	…	…		
98	中等	无		重新考虑

（同时也支持正在进行中的操作的决定）

通过CSF来支持RMF的几种情况

(RMF: Risk Management Framework)

案例 1. 用CSF的类(categories)支持SP800-39框架的活动

案例 2. 用CSF商业环境材料支持RMF的分类步骤(categorize step)*

案例 3. 用一个CSF配置文件来支持RMF的挑选步骤*

案例 4. 用一个CSF配置文件来支持RMF的评估与SP 800-30的评估

案例 5. 评估建立在FISMA基础上的(FISMA-Based)风险管理实践的状态

框架配置文件：一个部分，亚部分或者组织为其目标而定制的核心(core)。在组织输入中校准，识别冲突，并提高与任务目标相称的网络目标的优先级。

机构性输入：法律，命令，政策引导，政策目标和目标优先级和资源可用性，供需相关链考虑

体系结构描述：体系结构参考模型部分，解决方案体系结构模型任务和商业进程信息系统边界

类

商业环境(ID.BE)

组织的任务，目标，有利益关系者和活动应当被理解并且优先考虑；这条信息用于告知网络安全中的角色，责任和风险管理决定。

步骤一. 给信息系统分类FIPS 199/SP 800-60

步骤二. 选择安全控制FIPS 200/SP 800-53

步骤三. 执行安全控制Many SPs

步骤四. 评估安全控制SP 800-53A

步骤五. 认证信息系统SP 800-37

步骤六. 监测安全控制SP 800-137/SP 800-53A

步骤N. 如果有必要，从步骤一开始重复步骤

*制定SP 800-53 安全控制(案例3)