《数字时代—基于行业最佳实践的安全保护框架》

数十位产业、行业安全专家智慧结晶

PCSA • 数世咨询 • 数说安全• CIO时代/安全学院

中国信息协会 信息安全专业委员会

2022年6月18日 联合出品

聚合中国关键安全能力，赋能数字智能时代

第一篇：为什么需要新一代《安全保护框架》

谭晓生，汉族，毕业于西安交通大学，清华大学创新领军工程博士在读，北京赛博英杰科技有限公司创始人，正奇学院创办人，前360集团技术总裁、首席安全官，曾任MySpace中国首席技术官、首席运营官，雅虎中国首席技术官。

担任中国计算机学会(CCF)理事、副秘书长，CCF YOCSEF秘书长；获2018年获中国互联网发展基金会网络安全优秀人才， 2012年获中关村高端领军人才称号。

深刻认识：国际网络安全形势日益严峻

2022年，百年变局和世纪疫情交织叠加，国际环境日趋复杂，网络霸权主义对世界和平与发展构成威胁，全球产业链供应链遭受冲击，网络空间安全面临的形势持续复杂多变，网络空间对抗趋势更加突出。开年伊始俄乌冲突的爆发使得网络超限实战正在成为全球政治战略的焦点，实战化、体系化、常态化的网络对抗将成为未来主场景。

深刻认识：国内安全监管要求密集出台

国家在等级保护、F级保护、商M保护的基础上，围绕关键信息基础设施安全、数据安全、供应链安全、密码安全、个人信息安全等方面，相继出台了相关法律法规及政策标准。近年，监管要求从三年一发到一年多发的密集出台，安全运营单位亟需考虑如何将新政策与现体系进行有效融合，如何有序落地。

深刻认识：顶层、全局、重点视角都要兼顾

在安全形势严峻，监管日趋严格，数字化依赖度越来越高的情况下，我们深刻认识到，大平台、大系统、大数据、大安全已是必然趋势，传统的从单维视角出发考虑问题已无法应对当前复杂的环境，新形势需要建立顶层及全局视角，全面整合资源投入，识别关键要素，突破共性问题&共性顽疾，提出综合解决途径。

1. 顶层视角
2. 全局视角
3. 综合视角
4. 多维视角

五个亟待回答的问题

如何应对严峻的国际网络安全形势

如何满足新增的国内安全监管要求

如何有效融合新政策要求与现体系

如何匹配数字化转型下的业务发展

如何构建网络安全顶层及全局视角

方法论

- **“道”**

  是自然环境、事物的自然规律和发展方向；即“天道”

- **“法”**

  是为循“道”、成事、达到目标制定的方法；即“人法”

- **“术”**

  是为使“人法”得到落地实施采取的技术层面的技巧和方法

- **“器”**

  是为使“术”取得更好、更有效率的结果所必需的工具

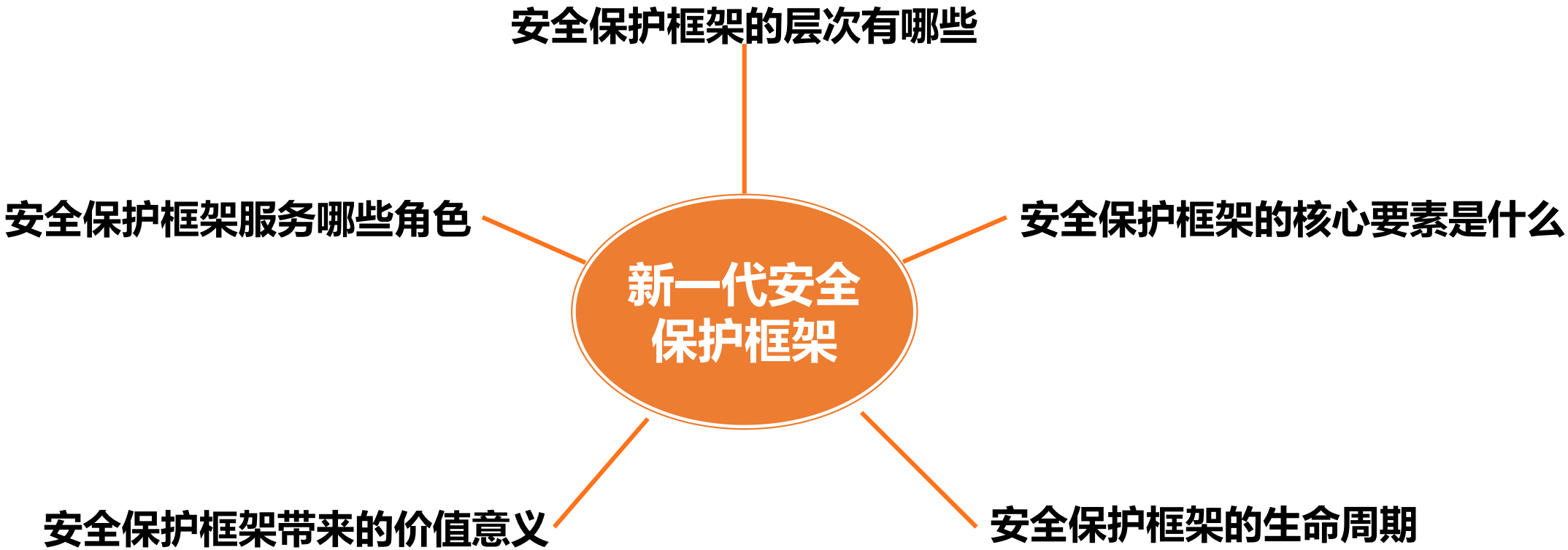
道——对问题建模

- **科学模型** 是科学研究中对一类研究方法的通称，使用数学公式、电脑模拟或简单的图示来表示一个简化的自然界，透过分析这个模型，以期能够进一步了解科学，包括说明、验证假说、或分析资料。

法、术——建立解决问题的框架

- A **framework** is a generic term commonly referring to an essential supporting structure which other things are built on top of.
  框架是一个通用术语，通常指的是其他东西建立在其之上的基本支撑结构。
- A system of rules, ideas, or beliefs that is used to plan or decide something
  用于计划或决定某事的规则、想法或信念系统

新一代安全保护框架要回答的五个问题



深刻思考：安全保护框架的价值意义

安全保护框架汇聚了各行业实践力量和各产业研究力量的经验与智慧，其出台将大力推动网络安全知识共享、经验共享和智慧共享，做到共性顽疾共生解决。

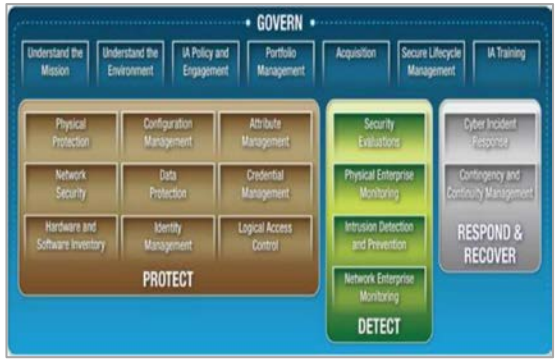
知识共享

经验共享

智慧共享

深刻研究：国际安全框架的演变

持续关注国际上网络安全趋势的发展，深刻研究了国际安全框架的演变，可以看到：各个国家从安全的各个维度建立了网络安全保护框架，各大国际权威研究机构也持续推出网络安全架构。以Gartner为例，自2014年起持续逐年向全球发布自适应安全架构（V1.0~V 2.0~V3.0……），不断敏捷迭代以适应快速变化的安全形势。

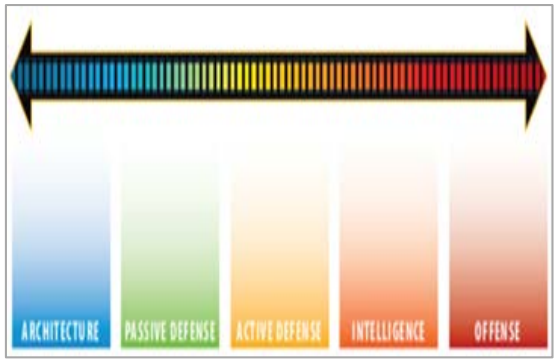


《美国国家安全体系黄金标准》（CGS2.0）

网络空间安全（治理-保护-监测-响应与恢复）

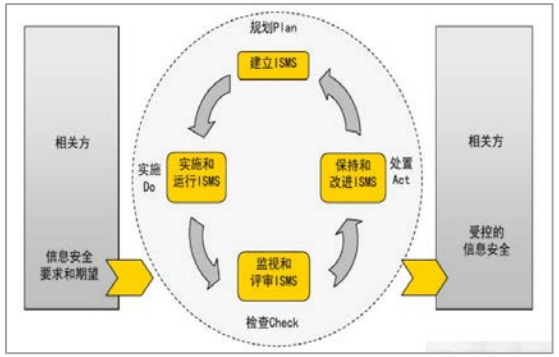
美国网络安全框架（CSF）

围绕国家关键基础设施，基于风险，核心（识别、保护、检测、响应、恢复）-概要-实现层



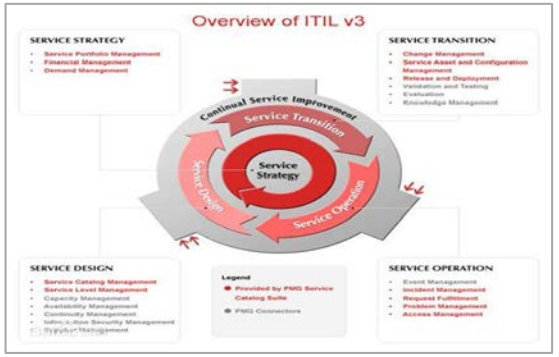
网络安全滑动标尺模型

架构安全-被动防御-主动防御-威胁情报-进攻



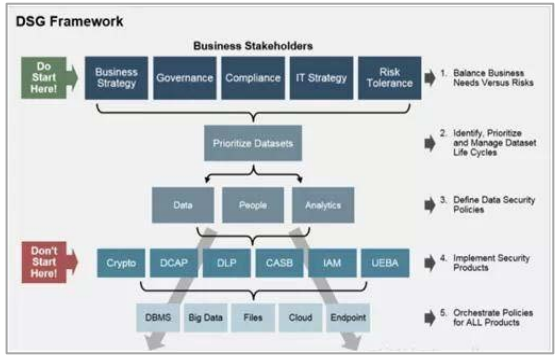
英国ISO IEC 27001

PDCA，方针、原则、目标、方法、过程、核查表



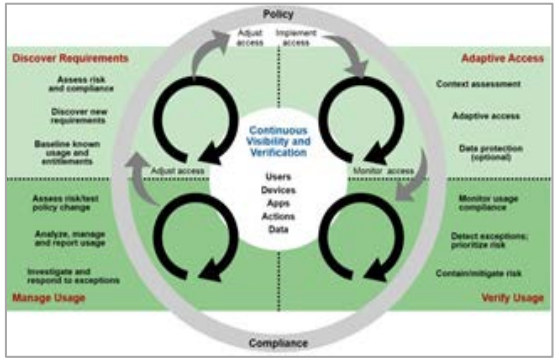
英国ITIL框架

服务生命周期（设计、转换、运营、改进）



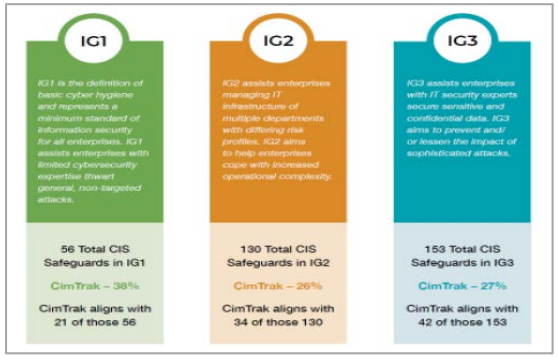
Gartner数据安全治理框架DSG

自上而下，从治理前提、具体目标到技术支撑



Gartner自适应安全架构

防御-检测-响应-预测



CIS控制框架

18个控制组（资产、数据、漏洞、邮件、应急……）

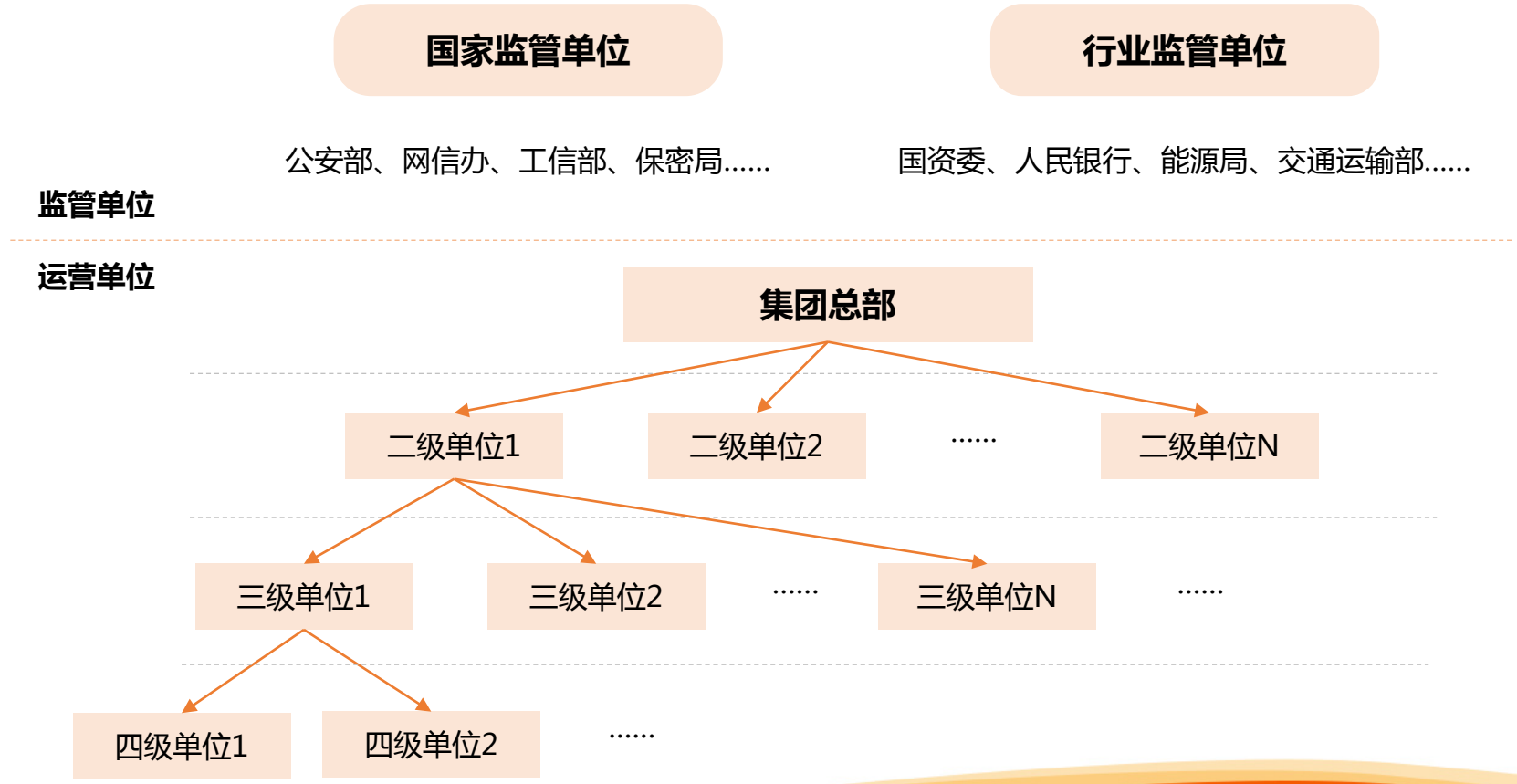
深刻思考：安全保护框架的维度与层次

对于国家层面、行业层面、公共及个人层面等不同领域，应针对性的建立不同安全保护框架。本次发布的安全保护框架主要聚焦于行业安全层面，为各行业的安全运营单位/组织提供共性难题的解决方向及思路。

安全分类	领域	热点和重点	涉及
1 国家层面	网际空间	网络空间安全治理、捍卫主权、国际超限战	监管单位
	网络社会	社会综和治理、雪亮工程、平安城市、智慧+移 动+大数据警务、网综、态势感知、通报预警	政法、公安监管行业
2 行业层面	关键信息基础设施	电力、交通、能源、金融、卫生、政务....APT及超限战	国家重要行业
	企业信息化	商业秘密及数据资产保护	核心商业
3 公共及个人层面	平台数据资产	公共平台数据安全、云上资产保护	群体
	个人隐私保护	个体隐私保护 智能终端保护	个体

深刻思考：安全保护框架服务的角色

安全保护工作主要涉及多种角色，国家监管单位、行业监管单位主要为安全工作提供方向指引及标准约束，而安全运营单位主要负责落实安全保护工作，满足刚需+合规需求，本次出台的安全保护框架主要面向行业安全运营单位。



深刻思考：安全保护框架的核心要素

从覆盖要素角度上来看，安全保护框架主要囊括公共要素和共性要素，为安全运营者提供明确的范围边界以及共性问题与顽疾的解决思路，而行业特色要素将在行业安全保护框架中进一步研讨。

公共要素	共性要素	行业特色要素
保护对象	资产及供应链	金融行业要素
服务对象	数据安全	能源行业要素
保护措施	智能安全	医疗行业要素
……	……	……

深刻思考：安全保护框架的生命力

安全保护框架的出台可指导安全运营者未来3-5年的安全建设、管理及运营工作，并具备持续迭代更新的能力，从而适应未来网络安全形势、技术的迅猛发展。

适度前瞻性

敏捷迭代性

结束语

呼吁：作为网络安全从业者，亟待构建行业安全圈，形成开源、开放、共享的平台及机制，凝聚各行各业顶级安全专家经验与智慧，共同推动安全生态发展，助力国家安全。

发挥纽带及桥梁作用 组织各类安全活动	研究安全共性问题及需求 创新解决共性顽疾及落地	网络安全产业领域调查研究、资源对接与行业咨询	行业研究和企业分析	信息化培训、咨询、专业化的知识与资源服务

初步奠定基础

行业安全圈

鸣谢

本次《数字时代—基于行业最佳实践的安全保护框架》的研究工作也是得到了能源、电力、金融、交通、电子政务、建筑、地方大数据局等众多行业实践力量和众多产业研究力量的支持，在此表示深切的感谢！！！

产业研究力量

中国信息协会 信息安全专业委员会	叶红、赵进延等
PCSA安全研究院	郭峰、徐玉慧、淮华瑞、金锴、李鹏飞、沈传宝及相关联盟成员单位人员
数世咨询	李少鹏、刘宸宇、靳慧超等
数说安全	谭晓生、于江等
CIO时代/安全学院	姚乐、刘晶等

行业实践力量

能源、电力行业	8家单位安全专家
金融行业	3家单位安全专家
交通行业	5家单位安全专家
电子政务行业	8家单位安全专家
建筑行业	4家单位安全专家
地方大数据局	4地单位安全专家

……

感 谢

欢迎各个单位与研究团队建立联系，共同研讨，感谢参与

联系人1：徐研究员 <xuyuhui@cnpcsa.org>

联系人2：淮研究员<huaihuarui@cnpcsa.org>