



公安部第一研究所

信息化顶层设计及 新形势下等级保护的工作思路



·李超

2015年6月 · 沈阳

公安部第一研究所信息安全等级保护测评中心

Contents

“互联网+” 大智移云的时代

顶层设计的概念

顶层设计的主要内容与方法

信息安全等级保护的主要内容

新形势下信息安全等级保护的工作思路

公安部第一研究所



大智移云时代的首要目标



公安部第一研究所

宽带化、移动化、泛在化

安全性、可用性、可信性

安全与
鲁棒性

可信互联网

具有移动性的
普适计算

移动互联网

跨越物理与
Cyber 空间

物联网

自治连网

泛在网

安全是“大智移云”时代的首要目标

Capability:

信息接入的
高可用性
与可信性

Capability:

无论何时
何地的无缝
接入

Capability:

实时接入
物理世界
的信息

Capability:

动态和挑战
环境的
信息接入



传递信息之一：体现了中国最高层全面**深化改革**、加强**顶层设计**的意志，显示出在保障网络安全、维护国家利益、推动信息化发展的决心。



2014年2月27日中央网络安全和信息化领导小组召开第一次会议

组 长：习近平

副组长：李克强、刘云山

成员：

国务院副总理 马凯

中央政策研究室主任 王沪宁

中共中央宣传部部长 刘奇葆

中央军委副主席 范长龙

中央政法委书记 孟建柱

中央办公厅主任 栗战书

公安部部长 郭声琨

中国人民银行行长 周小川

国务委员兼国务院秘书长杨晶

国新办副主任、国新办主任鲁炜（兼任中央网信小组办公室主任）

中央军委委员兼总参谋长房峰辉

外交部长 王毅

国家发改委主任 徐绍史

外交部长 王毅

国家发改委主任 徐绍史

教育部长 袁贵仁

技部党组书记 王志刚

财政部长 楼继伟

工信部长 苗圩

文化部长 蔡武

国家新闻出版广电总局局长蔡赴朝



传递信息之二：网络安全已经上升为**国家战略**，预示着信息化建设的新的**高潮**即将到来。



成立中央网络安全和信息化领导小组，标志着网络安全和信息化将成为全面深化改革的重要助力。习主席提出，**没有网络安全就没有国家安全，没有信息化就没有现代化。**

建设网络强国的战略部署要与“两个一百年”奋斗目标同步推进。



预示我国新的**信息化战略和网络强国战略**提上重要议事日程，在打赢一场信息技术和网络技术的翻身仗方面，也将迎来新的突破。

网络安全和信息化产业发展的大战略、大政策、大智慧，是新一轮网络安全产业革命的动员令和冲锋号，预示着网络安全和信息化发展的高潮即将到来。



传递信息之三：明确了实现网络强国的战略举措和方法

网络安全和信息化是一体之两翼、驱动之双轮，必须**统一谋划、统一部署、统一推进、统一实施**。

下大气力解决科研成果转化问题。要出台支持企业发展的政策，让他们成为技术创新主体，成为信息产业发展主体。要抓紧制定立法规划，完善互联网信息内容管理、关键信息基础设施保护等法律法规，依法治理网络空间，维护公民合法权益。



标志着：网络安全和信息化放在了同一重要的位置，还将积极倡导自主知识产权网络产品的开发，有目标、有步骤地提升重点领域网络产品的国产化率，**明确了网络安全发展的战略方向**。

安全是基石，离开了安全，再大的网络也不强。建设网络强国，首先就要过“安全关”，信息安全成为我们迈向网络强国的第一道关卡。

Contents

“互联网+” 大智移云的时代

顶层设计的概念

顶层设计的主要内容与方法

信息安全等级保护的主要内容

新形势下信息安全等级保护的工作思路



顶层设计的概念

1、顶层设计概念的解释-来源于系统工程学

顶层设计的定义：自高端开始的总体构想

顶层设计的概念：最初来自自然科学或大型技术工程领域，如人类基因组工程研究、航天工程研究等，是指为完成某一大型工程项目，要实现理论一致、功能协调、结构统一、资源共享、部件标准化进行**统一自上而下的设计**。

顶层设计的思想内涵：用系统论的方法，以全局视角，对项目建设的各方面、各层次、各种要素素进行统筹考虑，和谐各种关系，确定目标，选择实现目标的具体路径，制定正确的战略战术，并适时调整，规避可能导致失败的风险，提高效益降低成本。

这一工程学概念，后来被西方国家广泛引用于军事和社会学领域，甚至成为政府统筹内政外交制定国家发展战略的重要思维方法。

主要是用系统论的方法，对信息化建设的各个方面、各个层次、各种参与力量、各种正面的促进因素和负面的限制因素**进行统筹考虑**，理解和分析影响信息化建设的各种关系，**从全局的视角出发**，对信息化建设的基本问题进行**总体的、全面的设计**，确定信息化**建设目标**，**选择和制定**实现目标的**路径和战略战术**，并**提出体制、法律和业务的改进建议**，从而尽量规避规划的缺陷和不足，从根本上减少风险。

顶层的第一层含义——整体和全局

顶层设计的定位是要跳出局部环境的束缚和影响，站在全国互联和全网通用的**整体高度和全局视野**，去分析和制定信息化建设的**战略战术**。

顶层的第二层含义——业务、政务的应用

顶层设计的重点是用信息工程的方法，从宏观上对业务需求进行收集、梳理和描述，按一定层次呈现，并以数据的形式保存在数据库中，形成丰富、清晰、完整的业务资料，通过系统开发和应用，从而转变业务职能，完善业务利益关系，推动业务决策。

顶层的第三层含义——政府绩效

顶层设计的核心是针对经济调控、市场监管、城市建设、社会管理、公共服务等政府职能，促进职能转变，优化管理模式，再造审批流程，提高政务效率，推动体制创新，实现政府绩效目标。

顶层设计不是什么？



公安部第一研究所

- 顶层设计不是总体设计
- 顶层设计不是概要设计
- 顶层设计不等于总体规划
- 顶层设计不能自下而上进行

- ◆ 信息化顶层设计的内容是信息化建设问题进行**总体规划**和**全面设计**
 - ◆ 包括网络建设、安全管理、信息资源建设与绩效管理等诸多技术层面的内容
 - ◆ 包括行政管理体制、政府职能及具体业务类型之间的关系。
- ◆ 没有顶层设计搞不好规划，应该是**先顶层设计，后编制规划**。

- 顶层设计必须由顶层做
- 谁来做——顶层亲自主持和领导
- 谁来主导——业务部门、监督部门和投资规划 1部门三结合
- 谁来参与——信息化部门

Contents

“互联网+” 大智移云的时代

顶层设计的概念

顶层设计的主要内容与方法

信息安全等级保护的主要内容

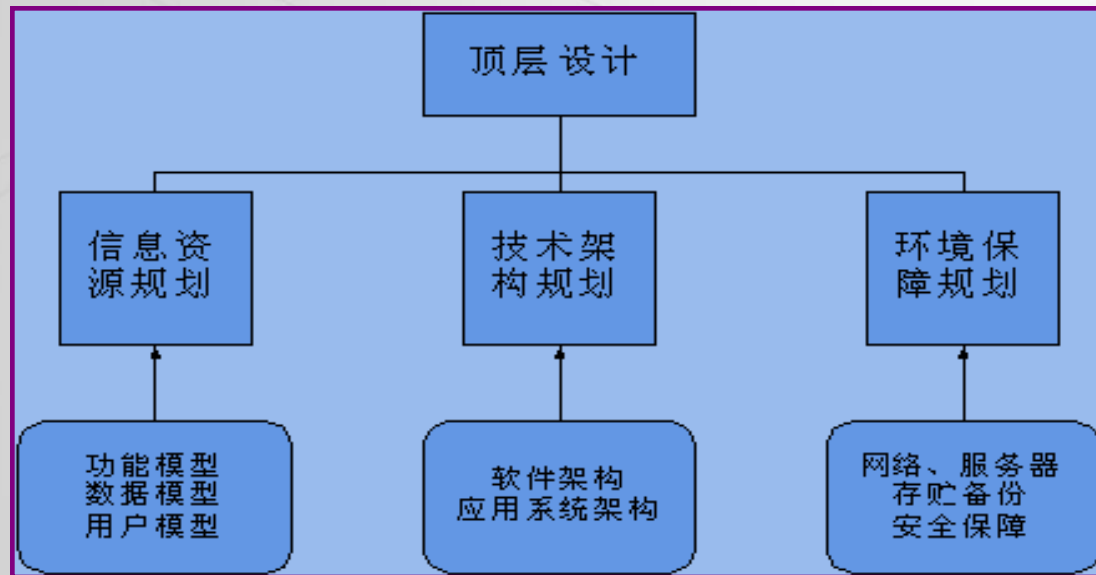
新形势下信息安全等级保护的工作思路

信息化顶层设计的主要内容



公安部第一研究所

顶层设计的主要内容：通过职能\绩效\服务\业务进行综合分析与抽象，以信息化综合体系为基础，构造信息资源共享与业务协同的信息化顶层体系，形成以指导信息资源建设，业务应用建设和运行环境建设为目标的信息化顶层设计专项成果。



信息化顶层设计的基本特点



公安部第一研究所

- 1、**履职业务和服务规划**是顶层设计的核心。
- 2、履职业务和服务规划注重部门履**职业务流程的梳理、整合与优化**，敢于突破传统观念，勇于创新。
- 3、顶层设计以**执行能力和服务水平**提升为第一要素，可以淡化部门概念，强调**业务协调和统一**。
- 4、关联、系统性是顶层设计的价值所在。
- 5、顶层设计必须应用相应的理论思路与技术方法。

信息化顶层设计的主要成果



公安部第一研究所

顶层设计的基本目标：通过规范数据和业务应用系统来实现资源共享与业务协同。

顶层设计的主要目的：提出信息资源共享与业务协同的基本技术框架，以规范和指导信息化的建设和发展。

顶层设计的成果体系 = 顶层体系 + 专项成果

顶层设计
成果体系

由顶层体系和专项成果（技术标准、准则与指南、建设与管理政策与规章和标准化软、硬件产品）构成，综合形成一个解决信息资源共享与业务协同的顶层整体技术方案。

信息化顶层设计的主要成果



公安部第一研究所

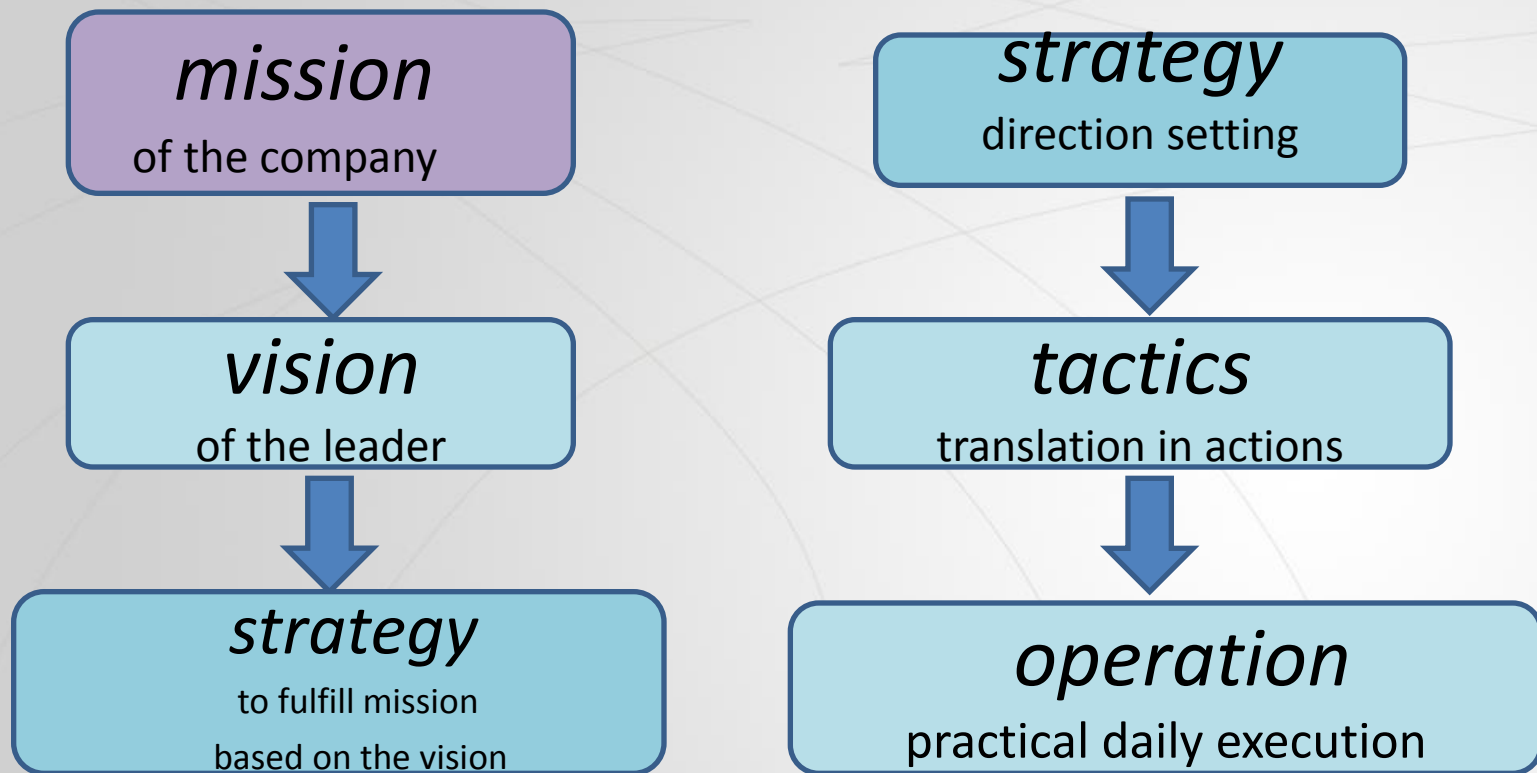
顶层体系：在宏观层次上细化信息化综合体系，阐明信息资源建设和各类务应用建设中的规划与设计的基本技术原则，针对不同层次的资源共享和业务协同，重点考虑业务的系统需求。

专项成果：在顶层体系的规范和指导下，针对具体的业务需求，进行的标准和指南层次或通用软、硬件层级设计形成的成果。这些成果包括技术标准、技术指南、建设与管理规章和标准化软、硬件产品。

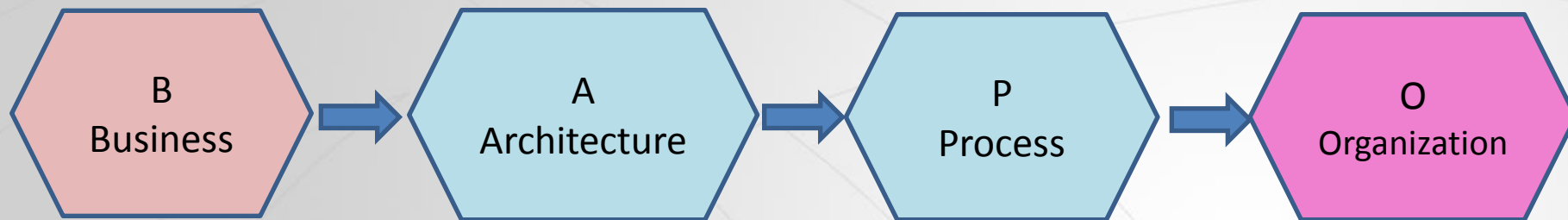
顶层设计成果体系的管理

在顶层体系的约束下，把成果按技术标准、准则与指南、建设与管理政策与规章和标准化硬件软件（数据）产品三个体系编码，进行有序组织和管理。

使命、远景、战略、战术和执行



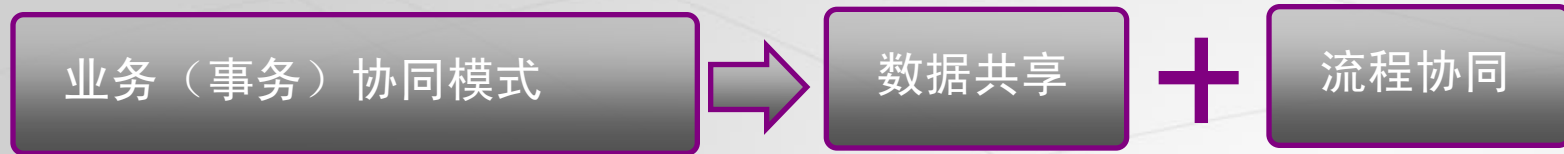
业务、架构、流程、组织



BAPO framework

信息化顶层设计必须强调业务协同

设计协同模式



数据共享模式：指不同业务（事务）之间仅通过共享数据，即可满足需求的协同模式。这种单向信息共享模式，仅需信息获取渠道畅通和政策授权条件即可。

流程协同模式：指不同业务（事务）之间不仅需要共享数据，而且需要共享业务（事务）操作流程的协同模式。

这种信息双向共享前提下的业务协同模式，不仅需要单向获取信息，而且需在业务协同中获取新的信息。不同业务（事务）之间环环相扣，互为制约，紧密协同协同表现为同层级或不同层级业务与业务、业务与事务、事务与事务的流程协同。

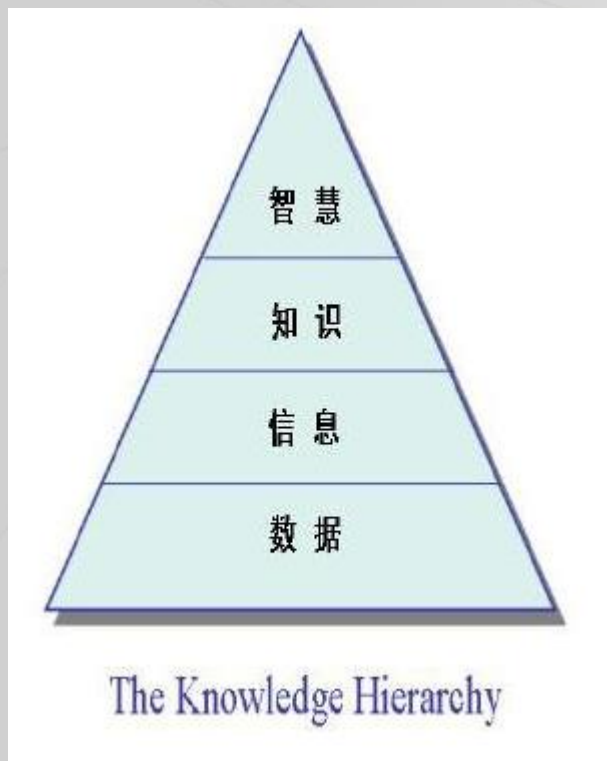
业务应用的层次结构

信息系统的层级结构划分为：日常业务+协同与综合分析

日常业务层次——业务应用的基本特点：以在线事务处理为主，满足单一业务部门日常业务处理需求。协同需求较少，信息集成度不高，开发利用层次较低。

协同与综合分析层次——业务应用的基本特点：以在线分析为主，满足多个业务部门之间业务协同需求和行业信息综合分析，并逐步发展为某专业 领域综合决策支持系统。

顶层设计中的架构规划



数据是使用约定俗成的关键字，对客观事物的数量、属性、位置及其相互关系进行抽象表示，以适合在这个领域中用人工或自然的方式进行保存、传递和处理。

信息是具有时效性的，有一定含义的，有逻辑的、经过加工处理的、对决策有价值的数据流。

通过人们的参与对信息进行归纳、演绎、比较等手段进行挖掘，使其有价值的部分沉淀下来，并于已存在的人类知识体系相结合，这部分有价值的信息就转变成知识。

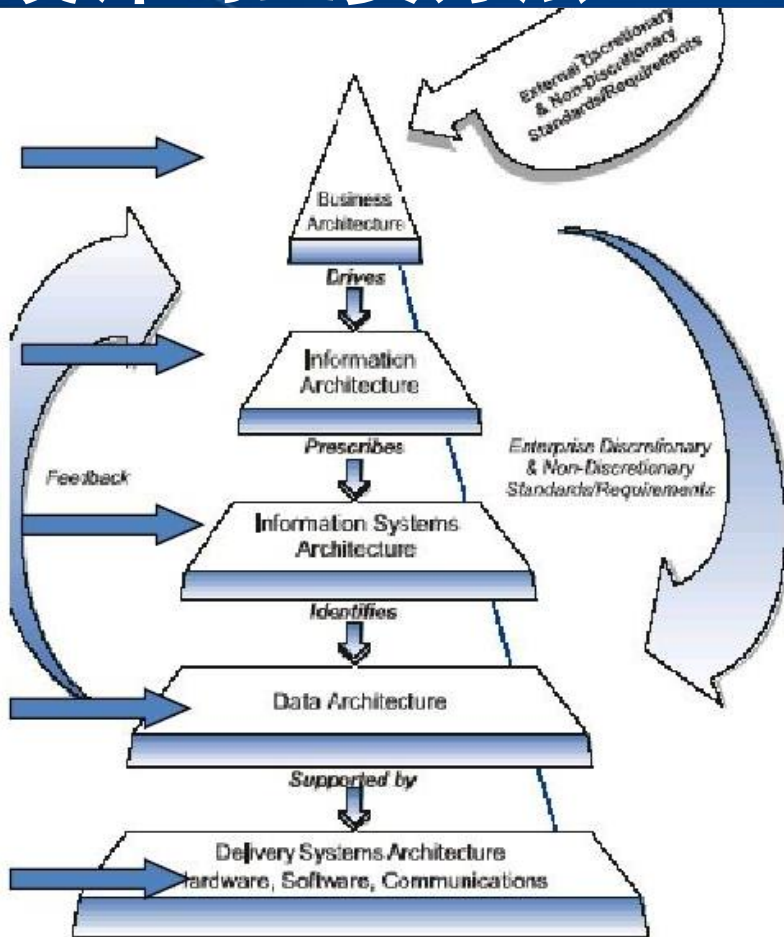
智慧是人类基于已有的知识，针对物质世界运动过程中产生的问题根据获得的信息进行分析、对比、演绎找出解决方案的能力。这种能力运用的结果是将信息的有价值部分挖掘出来并使之成为知识架构的一部分。

信息化顶层设计的主要方法



公安部第一研究所

业务架构
信息架构
信息系统架构
数据架构
物理系统结构



信息架构就是对信息的分类、分层的组织。例如：分层信息有决策层、管理层、操作层等信息；分类信息有财务信息、营销信息、生产信息等

数据架构就是对数据的分类、分层的组织。例如：分层数据有概念数据模型、逻辑数据模型、物理数据模型

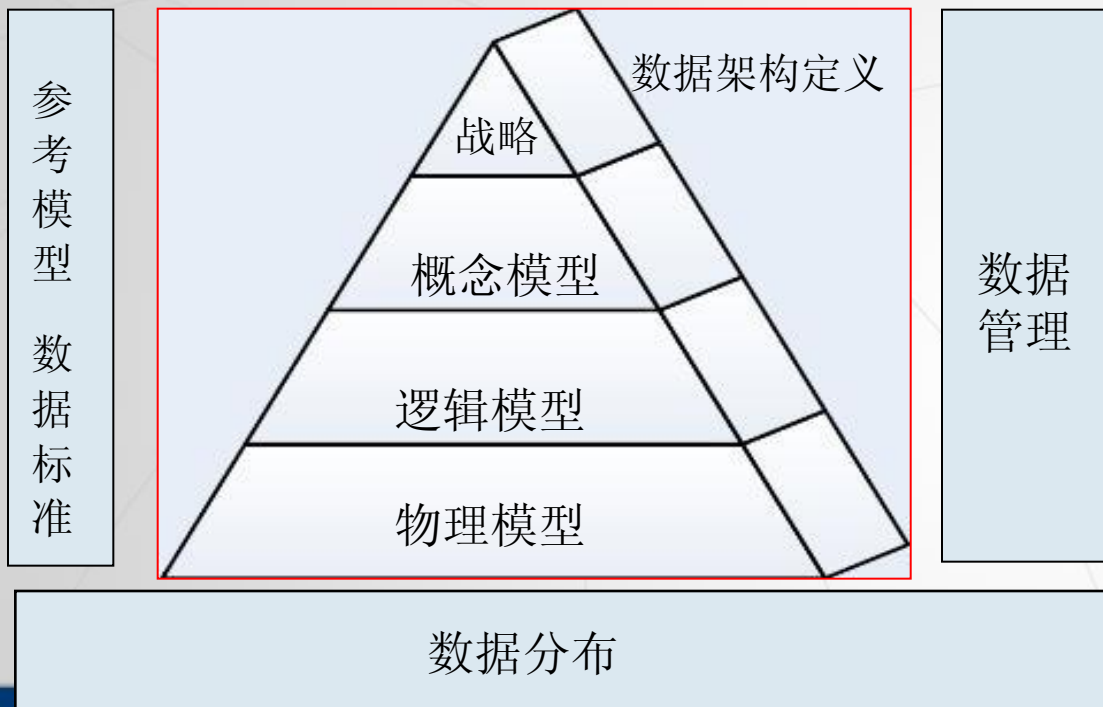
信息化顶层设计的主要方法



公安部第一研究所

信息架构是组织中所有人员完成自己工作所需信息的集合，分层分类管理。

数据架构描述了一个组织的逻辑、物理数据资产和数据管理资源的结构，它是一组分层的模型，为战略性的计划提供坚实的基础。



信息安全保障体系也需要顶层设计



公安部第一研究所

一、落实信息安全的等级保护制度

二、建立健全信息安全保障体系

三、做好信息安全监测、通报预警工作

四、做好系统应急和灾备工作，及时
应对突发事件和灾难

技术保障体系

- 做好纵深防御工作
- 建立动态防护策略
- 加强基于密码技术的网络信任体系建设
- 强化系统内部审计（内控机制）

管理保障体系

- 要从全局观的角度构建信息安全管理体系统；
- 要重视信息安全管理体系统建设的标准和方法。

Contents

“互联网+” 大智移云的时代

顶层设计的概念

顶层设计的主要内容与方法

信息安全等级保护主要内容

新形势下信息安全等级保护的工作思路

- 对国家秘密信息、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护、分等级监管。
- 对信息系统中使用的信息安全产品实行按等级管理。
- 对信息系统中发生的信息安全事件分等级响应、处置。

■信息安全等级保护是基本制度、基本方法。

- 信息安全等级保护是国家信息安全保障工作的基本制度。
- 信息安全等级保护是国家信息安全保障工作的基本方法。

“明确重点、突出重点、保护重点”。将有限的财力、物力、人力投入到重要信息系统安全保护中。有效保护基础信息网络和关系国家安全、经济命脉、社会稳定的重要信息系统的安全，维护国家信息安全。

- 电信网络、广电网、互联网、卫星系统
- 能源、金融、交通、税务、海关、卫生等重点行业的信息网络和重要信息系统
- 云计算系统、物联网、大数据、工业控制系统
- 全国5.6万个县级以上政府网站
- 为全社会提供服务的大型商业网站

信息安全等级保护的五个规定动作



公安部第一研究所

定级：将信息系统（包括网络）按照重要性和遭受损坏后的危害性分成五个安全保护等级；

备案：等级确定后，第二级（含）以上信息系统到公安机关备案，公安机关审核后颁发备案证明；

测评：备案单位选择符合国家规定条件的测评机构开展等级测评；

建设整改：备案单位根据信息系统安全等级，按照国家政策、标准开展安全建设整改；

检查：公安机关定期开展监督、检查、指导。

信息安全等级保护工作体系框架图



公安部第一研究所



等级保护工作中涉及的服务内容



公安部第一研究所

等保定级
阶段

等保规划
设计阶段

等保实施/
实现阶段

等保运行
管理阶段

等级保护导入培训

系统IT安全需求导出

等级保护解决方案设计

阶段性风险评估

系统业务安全域划分

等级保护差距评估

安全技术体系等保整改

安全状态监控

业务安全需求导出

信息系统安全规划

安全管理体系等保整改

系统可持续性安全服务

信息系统辅助定级

安全建设规划

通过等级测评

配合用户完成系统自查

协助定级备案

整改方案制定及实施

配合主管单位、用户
完成安全检查

安全岗位培训

Contents

“互联网+” 大智移云的时代

顶层设计的概念

顶层设计的主要内容与方法

信息安全等级保护主要内容

新形势下信息安全等级保护的工作思路

网络安全关系到：

➤七个重点：意识形态安全、技术安全、数据安全、应用安全、边防安全、资本安全、渠道安全。

➤四个层面：国家安全（政权、国防、经济、文化）、关键信息基础设施安全、社会公共安全、公民个人信息安全。

- 中央网络安全和信息化领导小组：领导和统筹。制定法律、政策，出台战略、规划
- 网络安全职能部门：侦查打击，安全监管，在产业发展、技术研究、产品应用、经费、装备、项目等方面提供保障
- 行业主管部门：谁主管谁负责，行业统筹
- 运营使用单位：谁运营谁负责，落实措施
- 技术支持单位、专家：提供支持、服务。



一是在中央新的网络安全领导体制下，建立完善 协调配合机制

- 由中央网信办统筹协调，建立由公安、工信、发改、财政、科技、安全、保密、密码等多部门参加的网络安全配合机制。
- 构建统筹协调、分工负责、各司其职、资源共享的网络安全工作格局，加强领导、统筹和顶层设计
- 加强军警、军地配合，共同维护网络安全



二是切实推进关键信息基础设施**自主可控**

- 建立由工信部和发改委牵头、公安部监督、有关部门和军队参加的信息基础设施自主可控战略实施机制，加大力度，建立自主可控战略的实施、监督机制，组织开展试点示范，全面组织对芯片、操作系统、大型数据库等核心软硬件技术的研发和应用，分步、分类实施自主可控战略。
- 实施网络安全审查制度。



三是切实加强对国家级重要信息系统和政府网站的安全保障和监管

- 按照中央领导批示精神，将国家级重要信息系统和政府网站作为国家和行业的重点保护对象。
- 公安部、发改委、工信部、财政部、科技部等有关部门将研究出台加强国家级重要信息系统安全的具体政策，采取有力的支持办法和措施予以落实。



四是建立打、防、管、控一体化的网络安全综合防控体系

- 积极发挥网络安全职能部门的管理职能，发挥专家、社会机构、互联网企业等各层面的资源优势和技术优势，建立打、防、管、控一体化的网络安全综合防控体系，切实提高维护网络安全的能力与水平。
- 将等级保护工作常态化、制度化，进一步落实公安机关的监管责任，落实公安机关工作责任制
- 健全完善国家网络安全监测预警机制，以及监管部门与重要行业部门、社会机构企业的联合应急处置机制。



五是重要行业认真**研究落实重大措施**

- 以国家网络安全法律、政策、标准为依据，搞好行业网络安全规划，出台政策标准
- 落实网络安全与信息化建设三同步要求。“同步规划、同步设计、同步实施”
- 依据国家、行业政策标准，结合生产、业务、管理等实际，从信息安全工作和重要信息系统保护两方面，“定制”信息安全策略。



- 以保护本行业生产业务安全、国家和社会稳定为目标，以等级保护作为抓手，从行业管理体制机制、政策体系、技术体系、标准体系、实施指南和规范等多层面进行认真规划，并实施一系列重大专项加以落实。
- 全面梳理网络信息安全工作 and 重要信息系统安全保护中存在的突出问题
- 全面梳理本行业、本部门网络和信息系统基本情况，掌握其数量、分布、应用和安全保护状况，作到“底数清、情况明”。



- 切实重视和加强行业监管，大力开展监督检查，有效落实安全责任。
- 落实开展信息系统定级备案、安全建设整改、等级测评等工作的有效措施。
- 深入开展安全监测、通报预警、远程技术检测、应急演练等重点工作
- 加强网络安全机构、队伍建设，加强培训，提高整个行业、队伍开展网络安全工作的能力。



公安部第一研究所

感谢！

THANKS



公安部第一研究所
信息安全等级保护测评中心
• 李超 13810021043