等保测评中高危风险判例与安全分析探讨

金铭彦

上海市信息安全测评认证中心

交流纲要

01 《高风险判例》编制背景

02 《高风险判例》要素及说明

03 《高风险判例》部分争议项探讨

04 《高风险判例》后续工作建议

01

《高风险判例》编制背景

《高风险判例》编制背景

通过全国等保报告抽查活动，发现全国各家测评机构的报告，对于相同问题风险判断的尺度差别较大。

主要原因可能是：

1、各测评对象的现场实际情况各不相同；

2、测评人员的个人能力、经验以及对标准的理解不同，导致对问题风险把控的不够准确。

《高风险判例》编制背景

受中关村测评联盟委托，上海市信息安全测评认证中心（以下简称上测）负责牵头，全国多家测评机构积极参与，共同完成《高风险判例》（初稿）的讨论及编制工作。

工作组讨论形成的相关成果能够成为一把“标尺”供各测评机构参考。

02

《高风险判例》要素及说明

《高风险判例》要素及说明

序号	要素名称	说明
1	安全控制点	等级保护基本要求中的控制点，用于帮助发现问题与标准条款的对应。
2	扩展说明	标明以下测评项属于通用要求还是某扩展要求，用于帮助发现问题与标准条款的对应。
3	测评项	等级保护基本要求中的测评项，用于帮助发现问题与标准条款的对应。
4	案例	测评过程中可能发现的问题描述。
5	案例说明	对于案例内容的补充。
6	风险等级	出现该案例情况，建议测评机构判定的风险等级。
7	适用等级	该案例适用的等级，部分案例只有在被测系统达到特定等级才会判为高风险。
8	适用范围	该案例适用的范围，主要指的是该案例是针对于的特定行业或用途的被测系统。
9	等效方案/补偿措施	该案例可通过等效方案的情况下可判符合，在补偿措施情况下可酌情降低风险等级。
10	推荐整改措施	该案例推荐整改的措施。

《高风险判例》要素及说明

等保测评-高风险判例合稿（初稿）

序号	*安全控制点*	*扩展*	*测评项*	*案例*	*风险等级*	*适用等级*	*适用范围*	案例说明	等效方案/补偿措施	推荐整改措施	备注
1	网络架构	通用要求	d) 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段；	对支付类系统的防火墙如果是租用运营商的，没有自己管理控制的防火墙，也无其他边界防护措施。	高	全	非金支付系统	非金支付系统租用运营商的防火墙，自己没有管理权限的，且无其他边界防护措施的，难以保证边界防护的有效性，可判高风险。 **同时满足以下条件：** 1、系统为非金支付系统； 2、边界防火墙没有管理权限； 3、无其他任何有效访问控制措施。	**补偿措施：** **1、无。**	部署自有的防火墙或租用有管理权限的防火墙。	**1、要求来源：** 非金支付系统检测判例 2、支付类系统不可使用无法管理的防火墙设备。
2				互联网出口无任何访问控制措施。如未部署防火墙、网络访问控制设备等。	高	全	全	互联网出口无任何访问控制措施。如未部署防火墙、网络访问控制设备等，判为高风险。 **同时满足以下条件：** 1、互联网出口无任何访问控制措施。	**等效措施：** 边界访问控制设备不一定一定要是防火墙，只要是能实现相关的访问控制功能，形态为专用设备，且有相关功能能够提供相应的检测报告，可判符合。	系统在互联网出口部署专用的访问控制设备。	
3				办公网与生产网无访问控制措施，任意员工可访问核心生产服务器和网络设备。	高	全	全	办公网与生产网之间无访问控制措施，办公环境任意网络接入均可对核心生产服务器和网络设备进行管理，判定为高风险。 **同时满足以下条件：** 1、办公网与生产网之间无访问控制措施； 2、办公环境任意网络接入均可对核心生产服务器和网络设备进行管理。	**补偿措施：** 无。	不同网络区域间应部署访问控制设备，并合理配置访问控制控制策略。	
4			e) 应提供通信线路、关键网络设备的硬件冗余，保证系统的可用性。	对可用性要求很高的系统，如支付系统、证券、银行等系统，无链路冗余。	高	3、4级	可用性要求很高的系统	例如涉及交易或支付的系统做等保测评，若网络链路为单链路，核心网络节点无冗余设计，则一旦出现故障，可能导致业务中断，对该类涉及资金的交易系统，无链路、核心网络设备冗余，判定为高风险。 **同时满足以下条件：**	**补偿措施：** 如系统采取多数据中心部署，或有应用级灾备环境，能在生产环境出现故障情况下提供服务的，可酌情降低风险等级。	核心网络节点和网络链路采用冗余设计和部署。	
5				对可用性要求很高的系统，如支付系统、证券、银行等系统，核心网络设备无冗余。	高	3、4级					
								与互联网互连的系统，边界处如无专用的访问控制设备或未对与互联网通信的接口	**等效措施：**		

简化 | 网络和通信安全 | 设备和计算安全（网络设备、安全设备） | 设备和计算安全（操作系统） | 设备和计算安全（数据库） | 应用和...

03

《高风险判例》部分争议项探讨

《高风险判例》部分争议项探讨

物理和环境安全

讨论争议点：

1、一些机房受限于地理条件、历史遗留问题，导致无法满足相关的要求，如果严格要求，可能导致整个地区都无法通过；

2、机房整改成本较高，一旦出现高风险，要求被测方整改的难度也会很大；

3、部分要求，如温湿度控制、防水防潮、防静电等，就实践上来说发生安全事件的概率较小，也不宜多判为高风险。

《高风险判例》部分争议项探讨

物理和环境安全

建议：

1、可根据当地的实际情况以及补偿措施中列举的内容酌情降低风险等级，但建议在报告中明确说明理由或相应的风险分析；

2、物理和环境安全层面，各测评机构应重点关注物理访问控制、防火、电力供应等关键控制点上，严格把关，其余控制项，在补偿措施或防护总体较好的情况下，可根据实际情况酌情处理；

《高风险判例》部分争议项探讨

网络和通信安全

测评项：（边界防护）应能够对内部用户非授权联到外部网络的行为进行限制或检查，并对其进行有效阻断；

高风险判例：主要针对核心重要服务器设备、重要核心管理终端，若没有措施控制USB接口或无线网卡，或者没有任何网络连接日志用于审查的情况，易造成数据泄漏等安全事件的，可判高风险。

同时满足以下条件：

1、系统为3级及以上系统；
2、机房、网络等环境不可控，存在非授权外联可能；
3、对于核心重要服务器、重要核心管理终端存在私自外联互联网可能；
4、无任何控制措施，控制措施包括限制、检查、阻断等。

《高风险判例》部分争议项探讨

网络和通信安全

讨论争议点：核心服务器通过安装安全管理产品进行管控难度较大，涉及到防护产品的兼容性等问题，对于核心管理终端进行管控相对容易。

建议：在机房、网络等环境均受控，机房运维制度完善，且落实到位，相对非授权外联可能性较小的情况下；可以弱化服务器的违规外联阻断，而加强管理终端等相关设备的管控。

《高风险判例》部分争议项探讨

设备和计算安全

测评项：（身份鉴别）当进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听；

高风险判例：通过不可控网络环境远程管理的网络、安全等设备，鉴别信息明文传输，容易被监听，造成数据泄漏，可判高风险。

同时满足以下条件：

1、网络、安全等设备通过不可控网络环境远程进行管理；
2、网络、安全等设备管理帐号口令以明文方式传输；
3、使用截获的帐号可远程登录网络、安全等设备。

《高风险判例》部分争议项探讨

设备和计算安全

讨论争议点：对于一般的边界设备，是有可能管理WEB对互联网开放的，而该WEB管理平台的口令以明文方式传输，通常在实际测评时，如果发现有漏洞或者弱口令可直接互联网登录的，判高风险，如果没有漏洞或弱口令情况的，一般判为中风险。

建议：

1、目前大部分网络、安全设备都已注意到了鉴别信息明文传输问题，并支持HTTPS协议，但一些老设备可能不支持该功能。

2、如无特殊原因，不建议边界设备的管理界面向互联网开放。

3、可根据被测对象的作用以及重要程度，根据实际情况，酌情调整风险等级。

《高风险判例》部分争议项探讨

设备和计算安全、应用和数据安全

测评项：应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现；

高风险判例：核心网络设备、安全设备、涉及资金交易、重要操作的系统，在进行重要操作前应采用两种或两种以上方式进行身份鉴别，如只采用一种方式进行鉴别，可判为高风险。

同时满足以下条件：

1、系统为3级及以上系统；

2、核心网络设备、安全设备或应用系统涉及资金交易等重要操作前未启用两种或两种以上鉴别技术对用户身份进行鉴别。

《高风险判例》部分争议项探讨

设备和计算安全、应用和数据安全

讨论争议点：就目前情况看，对于大部分3级系统，要实现操作系统、网络设备、应用系统双因素认证的要求仍然偏高。

建议：

1、采用两重用户名/口令认证措施，且两重口令不可相同等情况，可酌情降低风险等级。

2、可根据被测对象中用户的作用以及重要程度，网络环境是否安全可控等角度进行风险分析，在口令策略和复杂度、长度符合要求的情况下，可酌情降低风险等级。

3、在完成重要操作前的不同阶段两次或两次以上使用不同的方式进行身份鉴别，可根据实际情况，酌情降低风险等级。

4、主管部门认可的业务形态，例如快捷支付、小额免密支付等，可酌情降低风险等级。

《高风险判例》部分争议项探讨

安全建设管理

测评项：应要求开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。

高风险判例：对于涉及金融、民生等重要行业的业务核心系统由外包公司开发，上线前未对外包公司开发的系统进行源代码审查，外包商也无法提供相关安全检测证明，可判为高风险。

同时满足以下条件：

1、系统为3级及以上系统；
2、涉及金融、民生等重要行业的业务核心系统；
3、被测单位为对外包公司开发的系统进行源代码安全审查；
4、外包公司也无法提供第三方安全检测证明。

《高风险判例》部分争议项探讨

安全建设管理

讨论争议点：考虑到知识产权等问题，要求开发公司提供软件源代码进行代码核查有很大难度。此外，对于核心系统采用国外成熟产品的，要求源码审查的难度可能会更大。

建议：外包开发的代码质量安全以逐步被相关行业所重视，许多银行、证券公司已经要求开发商提供第三方专业机构的检查报告，因此，从风险防范的角度考虑，我们建议在一些涉及金融、民生的重要行业的核心系统加强相关要求，同时针对国外产品源代码审查操作上有难度的，可考虑通过明确安全责任或加强技术防控等方式降低安全风险。

04

《高风险判例》后续工作建议

《高风险判例》后续工作建议

《高风险判例》是一把供参考的“标尺”，但不可能覆盖所有情况；建议各测评机构在参考的同时，也需要考虑被测对象的实际情况，以及被测单位所在的主管部门的意见；

建议有更多的测评机构，安全专家能够参与我们的编制及讨论工作，各抒己见。

建议《高危风险判例》的编制工作能成为每年一个常态化的工作，成为动态的风险判例库，为各测评机构统一尺度，提高测评对象安全等级，提供借鉴。

谢 谢！

THANK YOU