## 章节

#### 00:00-07:11 信息系统密码应用高风险判定指引标准介绍

会议开始由专家介绍信息系统密码应用高风险判定指引标准，包括标准编制的背景、目的、历程和思路。讨论了密评机构面临的挑战，如何判定高风险问题，以及标准出台的必要性。同时介绍了标准的主要历程，从立项到专家审查会，再到收集反馈意见并最终形成发布稿的过程。讨论了标准的总体结构，包括章节和附录，以及其中的关键定义，如安全问题和缓解措施。最后，讨论了标准的判例结构和风险评价方法，强调了与基本要求的关联性和隐含前提。

#### 07:11-16:40 标准条款的解读及高风险问题的判定

继续深入解读标准条款，聚焦于高风险问题的判定。专家解释了标准的总体结构，并重点讲解了高风险判定指引的核心部分。讨论了安全问题的定义、缓解措施的含义，并强调了合规性、核心条款、以及密码应用正确性和有效性的重要性。此外，详细阐述了标准中关于密码算法、产品和服务、以及密钥管理等方面的安全问题和缓解措施，指出了一些常见算法的风险点，例如MD5、DES等。还讨论了物理和环境安全的适用范围，以及网络和通信安全中的数据机密性问题。

#### 16:40-27:49 高风险判定指引在测评和风险管理中的应用

深入探讨高风险判定指引在测评和风险管理中的具体应用。专家说明了在进行整体测评时，如何使用标准中的弥补措施，以及在风险分析期间，如何根据标准对发现的问题进行高风险判定。讨论了标准适用的时机，包括整体测评期间和风险分析期间。同时强调了标准中对新建系统密码应用方案的重要性，并对密钥管理中的安全问题提出了指导建议。最后，专家提出了关于标准应用的注意事项，包括对标准的合理解读和用户场景下的风险判断。

#### 27:49-33:25 标准制定背景、目的和实际应用情况

会议最后部分，专家总结了标准制定的背景和目的，强调了标准在规范和指导密码应用高风险判定中的重要性。讨论了标准的适用范围、核心要求、以及如何在实际测评中应用标准进行高风险判定。同时，强调了对标准内容的深入理解，并在应用时进行合理的风险判断。专家还提出了对于标准中未涵盖安全问题的处理方法，以及如何根据标准进行测评和最终结论的判定。最后，专家提出了标准使用时机的建议，并感谢了与会者的参与。

## 原文

未区分说话人 00:00

能看见我的这个屏幕吗？喂可以是吧？Ok好的。大家好，接下来的话由我来跟大家汇报一下信息系统密码应用高风险判定指引的标准的情况，我今天的一个汇报三块内容，第一块的话就是标准编制的一个背景和目的。第二块的话就是编制的历程和标准编制的一些思路。第三分条款的一个解读，因为今天来参加会议的大部分都是密评机构，相信大家也都有理解对吧？就是说密评还是一个专业性非常强的一项工作，他就是说对人的能力的要求非常高，因此的话大家在写密评报告的时候可能往往会比较纠结，尤其是在风险判定的时候，是不是如果说我们发现一个系统用的是国际算法或者是什么的，我到底要不要给高风险？

未区分说话人 01:03

也刚才罗老师也提到了，就是说我高风险的话，它实际上这个标准类似就是一票否决项的，你只要触碰了的话，很有可能那个结论就是一个不符合的。所以说基于这个的话，目前来说我们有可能不同的机构对于这种相同问题的一个风险判定的这种差异比较大，这样的话就会严重影响我们测评结论的一个准确性。因此的话我们就出台了就是说出台这个标准来对风险评价的环节来进行一个规划，这个标准的话是由工商所来牵头的，然后也联合了全国多家的密评机构和密码应用单位一起来起草的，我们的目标的话就是说给出密码应用各个环节中，可能出现高风险问题的一些场景目标，也就是说给全国的这些密评人员一个参考的尺度，也为了让我们的密评的工作更加的一个标准化和规范化。

未区分说话人 01:59

同时的话我们大家如果读过这个标准的话，可能会有一些感觉，我们的基本要求其实是有很多条款的，但是在高风险判定指引里面它的条款并不多，所以说这个里面实际上是有一个条款选取的一些在里面的，我们只是把其中的一些核心要求给拿出来了，说这些是基础的，我觉得是必须要做到的，把它明确出来了，因此的话这个标准不仅仅是给命名机构可以用，同时的话给这些信息系统的使用单位的话，它同样可以用它在建设的时候，他就有和有意识的来用这个标准来规避一些相应的高风险的问题，那么这是我们标准编制的一个主要的历程，实际上标准是从去年的3月份3月下旬开始立项的，当时形成了一个标准草案。

未区分说话人 02:49

然后在5月份7月份和8月份的话，我们有参加过三次的立项标准的一个专家审查会，然后根据专家的意见对这个标准进行了一个完善。在10月份的时候我们收到了两份重要的反馈意见，是密联委的针对这两个反馈意见的话，我们对标准进行了一个最终的修改，然后形成了最终的发布稿出来了。这是两次发布的一个意见的汇总情况，大家可以看一下，就是说这个里面其实解释说明的意见特别多，为什么这么说？

未区分说话人 03:21

其实有很多举两个原因，一个的话就是说你比方说有很多机构说你这个标准的条款跟基本要求条款不一样，确实不一样，因为刚才是我不知道大家有没有注意测评要求，其实也有这个问题。我们跟测评要求是绑定的，就是说我们在标准的条款里面把一一和是拿掉了的，所以说这个标准的条款不一致。另外一个的话就是说可能受等保的一个高风险判定的影响，因为因为很多机构也提出来了，为什么说我们这个里面没有没有什么整改措施等等，这些也是我们经之后没有采纳一个内容，所以说也是给出了一个解释的说明。

未区分说话人 04:06

那么接下来的话就说一下我们这个标准的一个总体的思路，李老师你要共享一下屏幕，再共享一下屏幕，再共享一下是吧？好，我退出来了。数据现在可以吗？可以了。Ok好的，那么我们的1个总体思路的话，实际上是分为这么4个部分，第一部分的话就是说我们要研究一下国家对密码相关的一些发展的或者说管理的一些要求，主要关注的是什么？是我们的合规性的要求。因为合规性是我们的一个最大的要求，也是我们这个底线。

未区分说话人 04:58

第二个的话我们要关注密码发展的一些技术，你典型的你就像我们现在存在一些严重问题的算法，你比方说MD5夏旺等等这些，这都是我们未来制定高风险判定的一个重要的依据。那么第三部分的话，我们针对密码应用场景的话，提出一些高风险判定的规则，这些规则的话实际上就是我们要形成高风险标准的一些原则，那么最后的话就形成了结合我们的一个密评的经验，形成了我们的风险方面指引的标准。

未区分说话人 05:35

您刚才也提到了我们高风险判定这个原则怎么来设定，实际上是包括这么三个，第一个的话就是合规性的原则，那么如果说我们在信息系统在使用密码的时候，我们不符合法律法规的规定和密码相关标准的要求的时候，那么实际上你触碰的是什么？合规性，那么这个的话实际上它是不行的，因此的话它是毫无疑问是高风险，也就是说合规性是我们的底线，也是我们这个标准里面要设定出来的一个红线。那么第二个的话不符合或者说没有实现国标版的基本要求的核心条款，刚才也说了和基本要求它在4级的话实际上它有44条，但是在我们这只有16条，实际上是没有完全覆盖所有44条的，这也就是说我们把这个条款进行了一些抽取，把一些核心的条款拿出来了，这样的话强调我们的一些底线意识，就是说我们这些底线必须要做到，你不能触碰这些底线。

未区分说话人 06:38

第三块的话就是我们关注密码应用的一个正确性和有效性。就是说第一条我们关注了合规，那么我们密码的产品我们用了也是符有认证证书的，他如果说用的不对，用的没效，实际上这个也是我们要关注的。那么第三条和第二条实际上是绑定的，我们在测第三条的时候，二实际上就是在第二条里面来测，这个的话，之所以拿出来是要重点的来突出一下。那么接下来的话就是第三部分的内容，就是标准的一部分的条款的一个解读。

未区分说话人 07:11

先说一下标准的1个总体结构，10个章节1个附录，这个我就不念了，因为这个时间特别短。那么这里面有两个非常重要的一个定义，一个的话就是安全问题，我们这个标准里面的结构里面就有安全问题的这一个，我们这里面定义的安全问题的话，就是资产中能够被威胁利用的弱点，实际上我们也可以把它叫成脆弱性。第二个的话就是一个缓解措施，这里的缓解措施指的就是可以降低安全问题导就说利用安全问题导致安全事件发生可能性的一些措施，这是我们的2个，那么我们的标准的1个判例结构的话，主要包括5个方面的内容，我不一一念，我跟大家重点说一下。

未区分说话人 07:56

第四，风险评价实际上我们是结合安全问题，结合安缓解措施，一起来综合考虑，然后确定我们安全问题，如果说被威胁利用后造造成的一个危害程度，是这样的一个意思，那么这里面的风险评价跟我们的风险评估规范的实际上是有一些差异的。就是说标准编制的时候它有一个差异，有一个特点是什么？就是说它可能会有一个隐含的前提，这个前提就是什么？

未区分说话人 08:25

我们的威胁可能一定要比就是说我们的脆弱性可能一定要被威胁来利用，是基于这样的一个前提来做的，包括我们的基本要求也是一样的对吧？我为什么要设定这个条款？是因为我们要应对威胁，所以说我隐含的前提就是说我威胁有可能会被利用，所以我们这个标准也是一样这么来写的。举个例子，你比方说数据传输对吧？数据传输我们要求加密，为什么要加密？为什么基本要求要提这一条？是因为我们要对抗一种威胁是什么？有可能会被窃听对吧？

未区分说话人 08:59

所以说整整个标准是这样的一个结构来写的。那么接下来的话我们就说一下具体的一些条款，这里面列了一些典型的条款，也是这个标准里面我想要跟大家讲的一些关键的点，不是说我们其他的条款不重要，就是说通过这些条款，我能把一些关键的点跟大家汇报一下。第一个的话就是在通用部分的一个密码算法，这里面大家先看第一个，就是我们标红的适用范围，适用的是所有的信息系统，不是说你是第一级也好，从第到第四级也好，这是都适用的，所以说大家要注意。

未区分说话人 09:37

另外一个的话这里面没有标出来的就是说我们的通用部分不仅仅是适用于所有级别的系统，我们同时还会适用于所有的技术条款的测评，在后面我会继续再说，这是第一个。第二个的话我们的安全问题这里面列了两个出来了，所以说这个地方要跟大家讲一下，就是说安全问题整个高风险判定指引的安全问题这一块，没有就是说大当时有很多人在问我，你到底是两条要同时满足还是只满足一条，这里面跟大家汇报一下，就是说这里面是任意一条满足都可以，所以说因为是任意一条，所以我们上面可能也是大家受一些其他的标准的一个影响，所以如果说我们会有两个问题叠加起来，形成一个高风险的话，一般是在同一条里面用用且的这种方式来写的，所以大家在读标准的时候要注意。

未区分说话人 10:35

第三个的话是安全问题一定是明确的经过验证的，是这样的一种情况。现在能听见吗？喂？可以听见。能听见是吧？我刚看好像给我发信息说听不到了，行，这样这是刚才说的就是说这些问题一定是明确的，所以说我们在这里面列出来的都是非常明确的，如果说这些问，如果说你在测评的过程中发现这个问题，你你就是说没有在这个里面，你可以结合你的实际情况来进行一个判定，好吧？但是这里面明确列出来的一定是就是说经过验证了的一些。

未区分说话人 11:31

那么四第五个的话，这里面有两个条款我大致解释一下，第一个的话就是采用存在安全问题的密码算法，那么刚才也提到了，你比方说我们的MD5，我们的des，我们的下望等等，还有包括我们的IC，不这里面注意是不足2048位，也就是说你IC1024实际上也是不允许的，所以说这是一个存在安全问题的算法。第二个的话就是安全强度不足，实际上指主要是指的我们的所以说好理解，第三个的话就是我们对重要数据这里面要明确，一定是对重要数据进行一个保护，因为你别到时候就是说我们在测评的时候，有可能用户对吧？

未区分说话人 12:14

他做了一些非重要的数据，可能是根本就不重要的一些信息来进行一个保护，刚好它恰恰恰恰好用的是一个des或者说是一个MD5。像这种情况下，实际上我们要做区分，就是说我们这里面提到的一定是我们要保护的是重要数据。那么第二块的话是什么？采用安全性未知的一个算法，这里面也提到了就是说自行设计的算法，就是说我们没有经过检测认证的，另外一个的话还有刚才马老师也提到的对吧？密码产品中未经安全性认证的一些密码算法，你典型的就是我们的一些密码产品对吧？

未区分说话人 12:49

我们经过检测认证的时候认证的是什么？其中的国密算法很并不是认证能力里面的国际算法对吧？所以说像这种情况下都是属于我们的高风险的问题。那么在这里面的话还有一点就是说跟马老师那边刚才提到的量化评估的一个关系，实际上大家也可以看得到，我们用了一些非认证的一些算法对吧？比方说我用的是国际算法，在量化评估里面可能会给出分数来，实际上也不是一个矛盾，就是说高风险判定跟量化评估实际上是一个有一定的关系的，但是它们本质上不是一个矛盾的一个情况，就是说量化评估它更多的我就是说从鼓励大家用密码技术，但是从高风险判定的话，它是从风险的角度来划定红线，所以说这是两个不同的维度。

未区分说话人 13:44

同时对于我们的密评的最终结论的判定来说，它也是两个不同的维度，对吧？分数是一个维度，风险分析的是一个维度。所以说我们这边来的标准的话主要是解决红线的问题，然后还有一个第四个块内容的话，可能的缓解措施这里面是无的，也就是说通用部分也就是说整个密码算法技术产品和服务这一块都没有缓解措施，就是说你只要存在了触碰了红线，没有和缓解的没有商量。

未区分说话人 14:18

针对密码算法这一部分，第二块的话针对密码的产品和服务，这里面要注意一点，就是说在密码产品的时候，大家看到了没有在这里面看不见对于检测认证的要求，这个就是说我们在写高风险判定指引的时候的一个差异点，刚才马老师实际上也强调了，我们在写标准的时候是有所考虑的，因为通用要求刚才说了，他不仅仅适用于就是说所有的级别就是所有的它两者都同时适用，如果说我们在这个地方来提的检测认证的一个要求的话，有可能会导致在有一些层面，它并没有那种成熟的产品做支撑的时候，会触碰高风险，直接就导致测评的结果的话，可能就是一个不符合了，同时的话用户可能还没有办法来整改。

未区分说话人 15:19

所以说基于这个情况的话，大家在读这个标准的时候，一定要注意在产品和服务这个地方，同样的安全问题一定也是列出来了，我们一些就是说能够经过验证的一些安全问题。对于产品的检测认证，我们是放在了网络和应用两个层面来考虑，待会会单独来提，那么这里面对于第四条的话也提到了密码要求需要有相关的一些资质对吧？刚才也提到了我们现在的密码服务可能主要的还是电子认证的服务，未来可能也会加入这种检测认证的机制是吧？

未区分说话人 15:49

目前来说的话可能还主要是国密局这边来统一使用的相应的证明文件等等这些。然后第五条要重点关注，因为第五条指向的是什么？密钥管理。在目前来说密钥管理的话，我们在这个标准里面放在的是附录a附录a是一个规范性，就是资料性附录，并不是一个规范性附录。但实际上我们在检查的时候，因为密钥非常重要，非常关键，而且密钥的话它本身跟这个产品是紧密的做了一些绑定的，所以说我们在测产品的时候，一并的要核查一下密钥这一部分是不是也会触碰附录a的一些高风险的问题。

未区分说话人 16:40

那么第三块的话就是物理和环境安全的这一部分，我们举了一个例子，就是身份鉴别，这里面的话第一个点的话就是适用范围写的是第二二级以上，为什么是第二级以上？跟大家解释一下，也就是说整个标准的写的思路。这里面的第二题，大家如果去看最新版的国标的基本要求的时候，你会发现第二题是一条款，也就是说整个高风险判定指引针对的都是一级一和一的一些条款来写的，就是说如果说你第二级是一条款，我们就是第二级开始的，如果你第三级是一条款，我们第三级开始的，因为乙本身适不适用的话，这个是在我那个方案的阶段就能明确，但是从我们从标准的角度来说的话，目前来说你的仪实际上是相对于仪，因为仪是有试用的这种情况出现的，这是第一块。

未区分说话人 17:38

第二块的话就是安全问题，大家可以看一下第一条，也就是说后面的所有的技术层面的标准的安全问题的一个设置，第一条都是指向了通用要求，就是说你在核查这一条的时候，你首先要核查它是不是存在通用要求这一些问题，密码算法技术产品和如果说你有这些问题，你实际上已经就触碰了高风险。第二块的话，我们关注的是什么？就是说你用了没有，也就是我们的第二条有没有采用，以及第三条我们用的合不合适，那么基于这三条的话，就来设定了我们的一个高风险的判定。

未区分说话人 18:20

那么第四块的可能的缓解措施这一部分的话，这里面给出了两个缓解措施，这里面要也要跟大家汇报一下的是什么？就是说整个标准的缓解措施这一块，尽量的会避免使用非密码技术，就是说因为咱们是一个密码相关的标准，如果说我们大量的这种缓解措施都是非密码技术的话，实际上你这个就只导向性可能就有问题，因此的话在这里面的话只有两个地方，一个的话身份鉴别，一个的话数据完整性这一块的话，我们是考虑了这种非密码技术的这种缓解措施的，基于之所以这么考虑的话，也是考虑到目前来说，你像咱们用的这种生物识别技术对吧？

未区分说话人 19:08

它本身也是一种安全性相对总技术，如果说你用了这种计划，可能就不是特意刻意的去强调，你还必须要用密码技术来实现，所以说这里面会涉及到我们用来非密的这种技术的一个环节措施，那么除了这两块内身份鉴别和数据完整性之外，其他的大家看的话，可能基本上都是缓解措施，也一定是密码方一些措施好吧？另外一个的话这里面有一个风险评价里面标红的，就是说酌情降低风险，这个也是要注意的，说刚才也讲了整个标准引导的还是大家要尽量的要用密码技术，那么如果说你真的确实是用了这种非密码技术的话，你也只是酌情的降低风险，并不是说你把这个风险给给消灭掉了，或者是什么，并不是这种完全替代的意思，目的还是说要鼓励大家来用。

未区分说话人 20:10

第四个的话就是网络和通信安全，这里面举了一个例子，就是通信过程中数据的一个机密性安全问题，第一条刚才也大家也看到了指向的是通用要求，那么第四条重点关注一下，就看到了提到了产品认证证书的一个要求，刚才在通用部分已经说了对吧？在通用部分的时候我们没有提产品认证证书的要求，那么在网络层面在应用层面都提了这个要求，也就是说藏在安全问题里面的最后一条，这个里面提到了有检测，那么多了三个字就有三个字试用时，试用时大家要注意一下的是什么，这个也是考虑到目前的一个使用的情况，这里面的试用时不并要跟大家讲强调一点就是说是有产品可用的时候它一定是适用的，并不是说你用了密码产品才适用，这是两个不同的概念。

未区分说话人 21:08

另外一个的话之所以写试用时，主要是考虑到目前你比方说提向公众提供服务的一些系统，比方说像公众服务的一些网站对吧？这种的话你要求你可以做成这种国密的浏览器，但是你很难要求这种公众用户也用这种国密的浏览器来访问。所以说像这种情况下的话，它才有这种条件的一个限定，好吧？另外一个的话还有等效措施对吧？刚才也提到了就是说网络层面跟应用层面的一个相互弥补的关系，这里面注意一下，就是说等效措施是他们两者保护的范围完全一致的时候才是等效，并不是如果说他们保护范围不一致，不一定是等效对吧？

未区分说话人 21:56

我们要对重要数据进行一个保护，如果说你应用层对吧，你对一些非重要的数据来进行保护，然后你网络层来明传的话并不属于一种等效措施。那么设备和计算层面的话，这个就不特意提了，有一点的话在缓解措施里面，就是说我们主要是用IP4 f VPN或者是建立这种集中管理通道，如果说像这种的话，目前来说是可以视为这种等效措施的。

未区分说话人 22:30

然后在应用和数据安全层面讲一个数据重要数据存储的完整性，这个的话是最后才加上去的，因为存储的完整性刚才夏老师在讲国标的时候也看到了完整性，基本上都是三级的话都是一的一个要求，那么在这里面的话，标准最后发布之前加了这一条，也是目的还是鼓励就是说单位去应用这种密码技术来实现完整性的一个保护。同时的话刚才也说了，在缓解措施里面也给出了这种非密码技术的一个一个弥补的情况，反正就是说总的想法来说还是鼓励大家来用，那么在密码应用管理这一部分的话，主要是列出来了一个就是制定密码应用方案，这里面大家要注意一点的是什么？

未区分说话人 23:22

这里面针对的是新建系统，虽然这一因为密码应用方案特别重要，如果说你的方方案有做或者说是方案没有经过评审，很有可能你未来建设完成的系统会存在各种各样的这种密码应用的问题，因此的话只是把这一条作为一个高风险的判例列出来，目的还是说要强调我们方案的一个重要性，那么这里面提到的是针对的是新建系统，所以说大家在用的时候要注意一下，因为我们平常会接触到很多单位对吧？它的系统里老但是它建设的时候建的可能比较晚拖沓沓的，然后等到你去测的时候，你就会发现它没有应用方案或者是什么的，因为他在立项的时候可能压根就没有考虑这些，所以说大家在选取高风险的这个的时候，我觉得要注意一下像这种情况，不要用这一条来，也就是说你在做指标选取的时候要有意识的进行一些区分。

未区分说话人 24:23

最后一个的话就是密码密钥管理的一个安全问题，因为密钥管理非常重要，所以说这个标准在附录a的话，针对密钥的一个产生分发、存储、使用等等这些环节都给出了一些可能造成安全隐患的一些问题。那么这里面举了两个，一个是密钥产生的对吧？产生是要通过认证的一些设备来产生，这实际上强调的是什么？我们要求的是真随机数，而不是那种伪。一个的话就是我们的密钥在不可控的环节里面，生成的话也是存在非常严重的问题的，你包括国标的话，我们要求的是37092对吧？

未区分说话人 24:55

符合37092的这种产品等等。那么密钥分发的话，实际上在密码测评的时候是一个非常重要的测评点，就是说你可能你你用的产品都是合规的，你用的算法也都是对的，但是你密钥分发很是可能就不合规了，你典型的你比方说用普通的U盘是吧？直接把密钥给好出来了，而且密钥也不加密，明文全，像这种的话都是一些高风险的问题。那么最后的话我们就说一下我们这个标准的一个情况，首先第一个的话刚才也提到了，就是说我们纸选取的指标的话，只是基本要求里面的一些核心条款选取出来了，那么对于其他的一些条款对吧？

未区分说话人 25:39

因为基本要求有4，你像4级有14条对吧？我们这里只有16条，还有剩下的这些条款怎么办？对于剩下的这些条款一定要核查第五章通用要求，也就是说你在剩下的那些条款，尤其是技术条款的时候，你在核查的时候，你同样也要参考高风险判定指引的第五章的通用要求，就是说你不能触碰通用要求的这些问题，这是第一个点。第二个点的话就是说因为密码应用场景比较复杂，目前这个标准也针对安全问题这一块的话，也只是把这种非常明确的给列出来了，有一些未来的话可能也不一定是列全了，对吧？

未区分说话人 26:21

所以说没有办法涵盖所有的这些安全问题。如果说你在实际的测评中发现了它的安全问题，然后你也分析这个安全问题，确实会造成这种严重的安全隐患，那么你也同样的可以作为一些高风险来判定。好吧？另外一个的话还要注意的就是说有一些问题的话，可能我们这里面列出来了，但是在他的用户的那些场景下面，他可能觉得对抗的威胁确实完全不存在，或者说是威胁发生的概率非常就是说非常小，这种情况下有可能会导致就是说我们这标准要列出来的是一个高风险，但是在它的实际情况下可能形成不了高风险，也有可能会有这种情况，那么对于这种情况下的话，我们也是在测评的时候要进行一个合理的判断。

未区分说话人 27:15

最后的话就说一下标准应用的一个时机，我想就是说主要是两个针对密评的话，主要是两个，一个的话就是我们整体测评期间，另外一个的话就是风险分析期间，整体测评期间的话，实际上就是我们在做整体分析的时候对吧？我们标准里面有很多弥补措施，实际上体现的就是这种整体测评的这种思路，对吧？你比方说6层的一个方相互弥补，实际上我们在做整体测评的时候就是需要穿好的。第二个的话是这个标准最最终要用的一个位置，对吧？

未区分说话人 27:49

你最后发现了很多问题，那么这些问题到底有没有触碰红线？你是要根据这个标准来进行一个一一对照的，你如果说他命中了，比方说他碰着了这个标准里面的某一个条某一个红线问题，那么它很有可能你问题就是一个高风险的问题，这就是这个标准的一个使用时机，我要汇报的内容就这么多，谢谢大家。