香港《网络防卫评估框架》政策解读

一、 香港金管局推出“网络防卫计划 2.0”

为应对瞬息万变的网络安全形势，香港金融管理局（以下简称金管局）于 2016 年推出“网络防卫计划”，旨在提升香港银行体系的网络防卫能力。该计划的三大支柱为网络防卫评估框架（C-RAF，Cyber Resilience Assessment Framework）、专业培训计划（PDP，Professional Development Programme）、网络风险资讯共享平台（CISP，Cyber Intelligence Sharing Platform）。

香港金管局监督协调下辖认可授权机构从 2017 年开始实施网络防卫计划，并在 2019 年末基本完成了一轮 C-RAF 评估，通过市场研究、访问、问卷调查和广泛业界咨询的方式，完成了对“网络防卫计划”的全面检讨。检讨结果显示银行业非常支持“网络防卫计划”。超过 90％的银行认为“网络防卫评估框架”有助于他们发现以往未能识别的网络安全缺口，对银行网络防卫起正面作用。另外，所有银行都认同以风险资讯主导的“网络攻防模拟测试”（iCAST）有助防范网络攻击。

因此，香港金管局在完成了业界咨询后，于 2020 年 11 月 3 日发布增强型“网络防卫计划 2.0”（CFI 2.0），重点通过发布《网络防卫评估框架 2.0》（英文版）文件列出了行业反馈的关于增强 C-RAF 框架的实施细节。根据香港金管局的要求，“网络防卫计划 2.0”已于 2021 年 1 月 1 日生效，并将会在 2021 年中开始分阶段实施，之后会一直持续至 2023 年底。

二、 《网络防卫评估框架》实践解读

下面将由天融信带您对《网络防卫评估框架 2.0》（英文版）进行全面的政策解读。

1、C-RAF 框架：打造弹性

C-RAF 是一个结构化的评估框架,目的是通过基于风险的方法，评估认可机构的网络风险状况及防范网络攻击所需达到的能力水平。评估结果将作为制定提高网络防卫能力方案的依据，并让金管局能够全面掌握个别认可机构以至整个银行体系面对网络攻击的应变准备是否充足。通过该框架，认可授权机构根据控制

原则评估内在风险和网络安全措施的成熟度，更好地理解、评估、加强并不断提高他们的网络弹性。

C-RAF 框架重点包括两个文档和四部分内容。两个文档是《Final-Document of Cyber Resilience Assessment Framework》，规定了 C-RAF 评估要求的细节和过程，同时提供附录中的 C-RAF 评估模板；《CRAFT-D1toD7》是一个 Excel 电子表格形式的数据输入程序，载有完整的 7 个控制域的控制原则清单，认可机构应按照说明完成成熟度评估的所有七个领域。四部分内容是内在风险评估、成熟度评估、网络攻防模拟测试（iCAST）和改进工作。

2、内在风险评估：认清自己

内在风险评估是指认可授权机构根据多个因素评估本身的网络风险状况，然后以“高”、“中”或“低”三个级别显示其所属的自身风险程度。评估的因素包括为提供服务时使用的科技、惯例服务渠道、提供的产品和服务、组织架构特征以及以往防御网络攻击的记录。按照自身风险级别，认可机构会有相应的预期网络防卫成熟度。

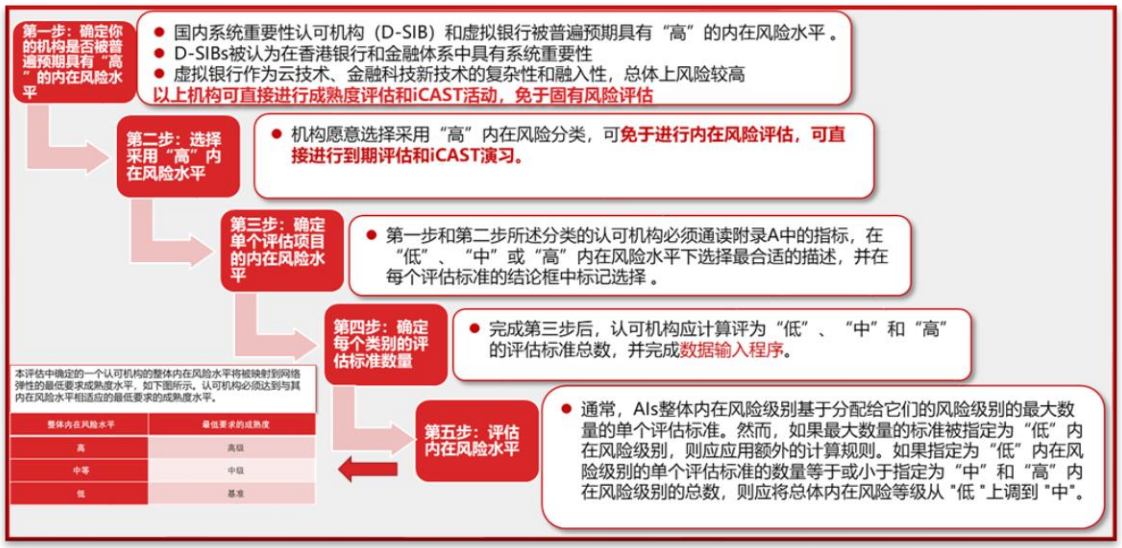
风险等级定义

框架对高中低风险等级解释定义如下表所示：

风险等级	描述
高内在风险	具有高内在风险的认可机构使用高度复杂的技术来提供大量的产品和服务。新兴技术被用于多种交付渠道，包括互联网和移动渠道，以及与其他组织的直接连接。认可机构可以在外部托管部分或大部分任务关键型系统或应用程序，并保持大量连接，使用不同的网络或通信协议与客户和第三方传输数据。
中内在风险	具有中等内在风险的认可机构通常采用相对复杂的新技术。认可机构可能会将一些关键任务系统和应用程序外包出去，但大多数都是在内部托管的。它通过多种渠道提供更多种类的产品和服务，包括互联网和移动渠道。
低内在风险	具有低内在风险的认可机构通常很少或根本没有采用新兴技术。它利用有限的互联网和移动渠道来提供产品和服务，并且拥有一个相对封闭的运营环境，外部连接的数量非常有限。它的产品组合中只有少数产品和服务。该认可机构的地理覆盖范围小，实体分支机构非常少。

风险自评过程

框架认为内在风险评估过程包括以下七个步骤，并根据自评结果匹配预期的网络成熟度。



3、成熟度评估：找到差距

成熟度评估是评估及判断认可机构实际的网络防卫能力成熟度，然后比照其预期的成熟度。一旦两者出现差距，即反映有待改善之处，有关认可机构即需采取适当措施提高实际的网络防卫能力，以达到至少与自身风险程度相对应的水平。

成熟度评估 7 个关键域

成熟度评估主要包括 7 个关键领域，如下图所示。这七个领域分为三个层次：治理（中心）；内部环境（如内圈所示，识别、保护、检测、响应&恢复）；外部环境（由外圈表示，态势感知和第三方风险管理）。成熟度评估旨在提供对整个运营环境的全面审查，并将重点放在健全的治理框架上。

成熟度评估 26 个安全组件

成熟度评估的 7 个关键领域包括 26 个安全组件，如下表所示：

成熟度	域	组成部分
治理	治理	网络弹性监督
		战略和政策
		网络风险管理
		审计
		人员配备和培训
内部环境	识别	IT资产管理
		网络风险识别、评估、处理与检测
	保护	访问控制
		基础设施保护控制
		数据保护
		安全发展
		修补程序与更改管理
		补救管理
	检测	漏洞检测
		异常活动检测
		网络事件检测
		威胁监测与分析
	响应&恢复	事件响应和恢复的治理与准备
		分析、缓解与恢复
		网络取证
		通信与改进
外部环境	态势感知	威胁情报
		威胁情报共享
	第三方风险管理	外部连接
		第三方管理
		持续监控第三方风险

成熟度评估四个步骤

成熟度评估分为 4 个步骤：

第一步：评估适用的控制原则

认可机构应根据要求的成熟度水平评估适用的控制原则。例如，如果一个认可机构受制于“基准”最低要求成熟度水平，它应该在“基准”水平上评估所有控制原则。如果认可机构符合“中级”最低要求成熟度水平，则应评估“基准”和“中级”水平的所有控制原则。如果认可机构符合“高级”最低要求成熟度级别，则应评估“基准”、“中级”和“高级”级别的所有控制原则。

第二步：将评估结果输入到数据输入程序中

认可机构应在完成成熟度评估后，将每个控制原则的评估结果输入到数据输入程序，按照下表对比控制原则。

选项	解释	说明
[Y]	是	控制原则已得到有效完成。
[AC]	替代控制	控制原则被认为是通过实施被认为是有效的替代控制来实现的，尽管实现方法与矩阵中所描述的不同。在这种情况下，评估员应在 "理由 "栏中提供替代控制的细节。
[RA]	接受风险	控制原则被认为是通过风险缓解措施来实现的，认可机构根据其风险偏好和风险处理计划正式接受与未实施控制原则相关的剩余风险。在这种情况下，评估员应在“理由”一栏中提供风险缓解措施和剩余风险接受的详细信息。
[N]	否	控制原理没有得到有效的实现。在这种情况下，评估员应在 "理由 "栏中提供补救计划和时间表的细节。
[NA]	不适用	控制原则不适用于认可机构，因此，已从组件成熟度的确定中排除。在这种情况下，评估员应在 "理由 "栏中提供排除该控制原则的理由。

第三步：计算完成百分比

应计算每个组成部分的实现百分比，该百分比应为（i）完成的控制原则数量（标记为“Y”）加上（ii）实施的替代控制数量（标记为“AC”）加上（iii）“接受风险”数量（标记为“RA”）之和，加上（iv）不适用于 AI 的项目数量（标记为“NA”）。这个总数除以该成熟度级别的控制原则总数，结果以百分比表示。如下图所示：

控制原则数量						成绩百分比
总计	[Y]	[AC]	[RA]	[N]	[NA]	
8	4	1	1	1	1	7/8x100%=87.5%
10	5	3	1		1	10/10 x 100%=100%

第四步：确定需要改进的地方

对于每个组成部分，所达到的成熟度水平取决于该组成部分在不同水平上的适用控制原则的完成程度。

为了使某一特定组件达到以下成熟度水平组成部分	一个认可机构需要为该组件实现以下条件		
	基准控制原则执行情况（%）	中级控制原则执行情况（%）	高级控制原则执行情况（%）
基准	100%	n/a	n/a
中级	100%	100%	n/a
高级	100%	100%	100%

确定成熟度级别示例

为了说明确定认可机构成熟度水平的过程，下面三张图分别显示了最低要求成熟度水平为“高级”（A）、“中级”（I）和“基准”（B）的示例

域	组成部分	成熟度水平			
		B	I	A	总体成绩
治理	(i) 网络弹性监督	100%	100%	100%	高级
	(ii) 战略与政策	100%	100%	20%	中级

银行A预计将达到 **“高级”成熟度**水平。任何没有达到 “高级”成熟度水平的部分都是差距，因此，**战略与决策组件**需要由**“中级”** 提高到**“高级”**。

域	组成部分	成熟度水平			
		B	I	A	总体成绩
保护	(i) 访问控制	100%	100%	n/a	中级
	(ii) 基础设施的保护控制	100%	20%	n/a	基准

银行B预计将达到 **“中级”成熟度**水平。任何没有达到 “中级”成熟度水平的部分都是差距，因此，**基础设施的保护控制组件**需要由**“基准”** 提高到**“中级”**。

域	组成部分	成熟度水平			
		B	I	A	总体成绩
保护	(i) 风险资讯	100%	n/a	n/a	基准
	(ii) 风险资讯分享	50%	n/a	n/a	基准以下

银行C预计将达到 **“基准”成熟度**水平。任何没有达到 “基准”成熟度水平的部分都是差距，因此，**风险资讯分享组件**需要由**“基准以下”** 提高到**“基准”**。

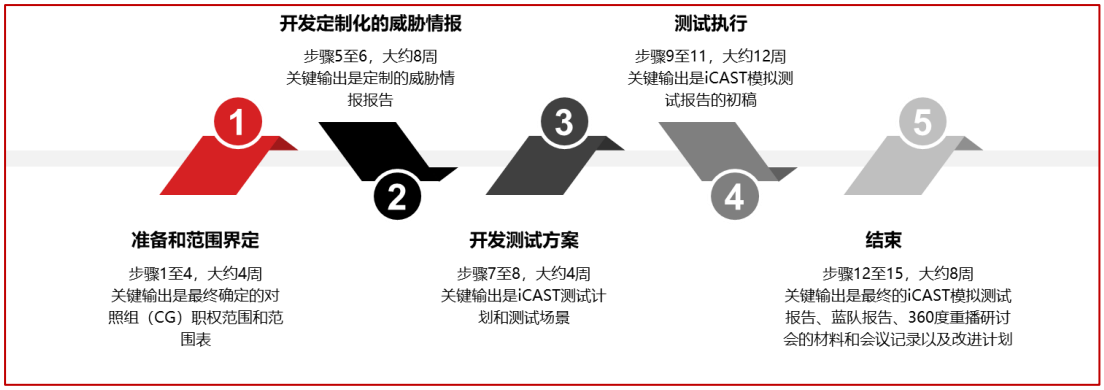
4、iCAST 测试：实战演练

风险资讯主导的网络攻防模拟测试（iCAST 测试）是在传统渗透测试的基础上额外加入以风险资讯为本的模拟测试。测试采用的假设情境根据特定及最新的风险资讯，来模拟当前实际的网络攻击。若认可机构拟需符合“中级” 或“高级”成熟度要求，均需进行 iCAST 模拟测试。

iCAST 测试在传统渗透测试的保护范围上增加了治理、识别、检测、响应&恢复、态势感知、第三方风险等范围。在 iCAST 演习中，传统渗透测试使用威胁情报来增强和制定端到端测试方案；认可机构采用基于风险的方法识别相关攻击场景，并确保在 iCAST 模拟中对其进行测试，以模拟真实攻击。

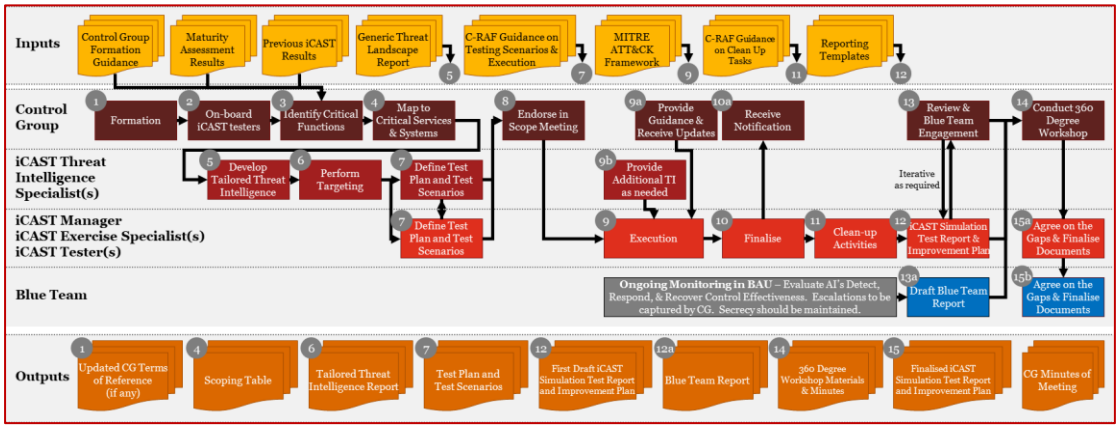
iCAST 测试五个阶段

iCAST 测试一般分为五个阶段，如下图所示。一般来说，每个阶段所需的持续时间是指示性的，仅供参考。认可机构应根据其 iCAST 演习的需要进行调整。



iCAST 工作任务流程

iCAST 测试用标准化、流程化、精细化的思想描述了参与各方及其在每个阶段的相关任务、输入和输出等，如下图所示。



iCAST 工作成果

通过完整的 iCAST 测试，最终可以形成以下输出成果，并通过改进计划大大增强网络攻击防御能力。

- ✓ CG 职权范围
- ✓ 范围界定表
- ✓ 定制的威胁情报报告
- ✓ iCAST 测试计划和场景
- ✓ iCAST 模拟测试报告草案
- ✓ 蓝色团队报告
- ✓ 360 度重播研讨会
- ✓ iCAST 模拟测试报告终稿
- ✓ 改进计划

C-RAF 框架除了以上内容外，还必须使用独立的、专业的第三方人员进行评估和测试。整个框架提供了一套完整的、战术和实操结合的银行业网络防卫能力评估实践，为香港金管局下辖的银行机构给与了网络防卫评估的政策支持，也为安全服务厂商开展网络评估服务提供了政策指导。各厂商应尽快开发基于 C-RAF 的安全服务体系咨询服务，提供完善的、体系化的服务产品和方案。