Deloitte.
勤業眾信

NIST Cybersecurity Framework概覽

報告人：萬幼筠

September/06/2019

簡歷

萬幼筠

現職
- 東吳大學法律研究所/ 科技法律組 - 兼任助教授
- 勤業眾信風險管理諮詢公司 – 執行副總經理

參與專業組織
- 國際資訊系統稽核協會(ISACA)
- 國際舞弊偵防協會(ACFE)
- 國際資訊安全專家協會(ISC2)
- 中華民國資訊服務管理協會(ITSMA)
- 台灣舞弊防治與鑑識協會 (ACFD)
- 中華民國科技法律經理人協會(TILO)
- 美國計算機協會 (ACM)

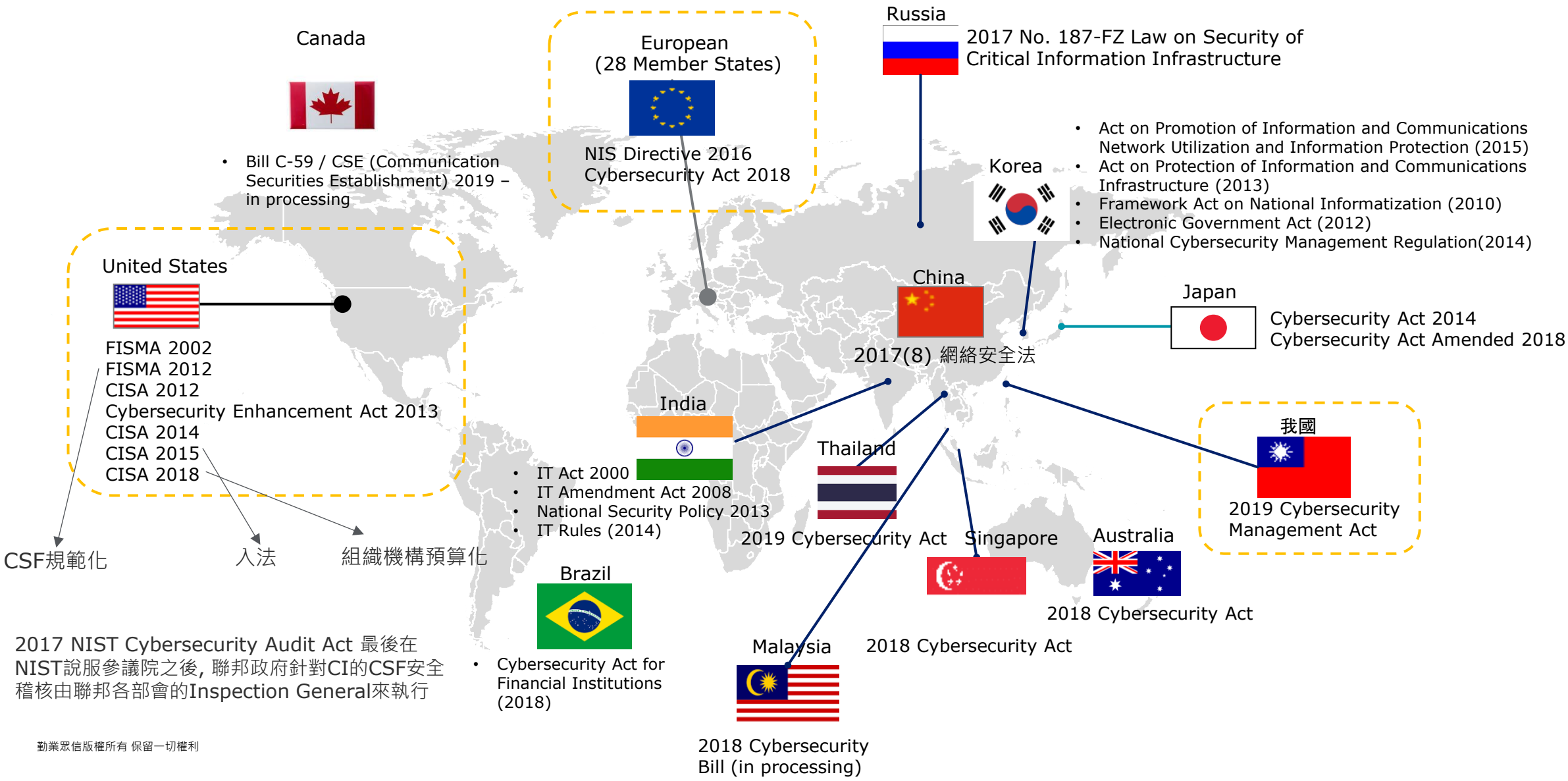
工作經歷
- Deloitte Risk Advisory – 勤業眾信風險諮詢公司
- III – 資訊工業策進會
- Ernst & Young LLP , U.S.A - 先進運算實驗室

學歷
- 國立政治大學法律研究所 – Master of Laws (LLM)
- University of Maryland, College Park - Ph.D Candidate
- University of Colorado, Boulder – Master of Science / M.B.A – Information Systems

公共事務
- 行政院資通安全會報 - 諮詢委員
- 行政院科技顧問會報 - 科技專案審查委員
- 台北市政府 - 市政顧問 (網路與數位城市類)
- 經濟部技術處 – 數位經濟新創計畫科技專案審查委員
- 經濟部工業局 - 行動APP 檢測制度諮詢委員
- 經濟部商業司 - 電子商務產業- 行政檢查委員
- 經濟部商業司 - 資訊服務業第三方支付跨境支付業務 -審查委員
- 法務部調查局 - 資訊安全與數位鑑識 – 諮詢委員

研究興趣與領域
- 資訊科技法律 (Cyber Law)
- 系統動力學 (System Dynamics) / 社會系統模擬
- 演算法與系統模擬 (Algorithm & system simulation)
- 資訊治理 (IT Governance)
- 資料庫逆向工程 (Data Base Reengineering)
- 風險治理與數據分析 (Risk Governance)
- 資訊系統安全/ 安全稽核與鑑識

NIST Cybersecurity Framework的出現, 是基於CIIP法制化與規範化的需要
並帶動全球針對Critical Infrastructure Protection立法保護的潮流



2017 NIST Cybersecurity Audit Act 最後在NIST說服參議院之後, 聯邦政府針對CI的CSF安全稽核由聯邦各部會的Inspection General來執行

Cybersecurity 法律的類型與分類 與受NIST CSF影響的法律

資安法律 保護法益 資安法律 制定功能別	國家法益 國家或政府 安全、監察與情資調查	社會法益 民生關鍵資訊 基礎建設保護	資料或隱私保護 隱私與 個人資料保護	犯罪預防 電腦或 網路犯罪
以保護原則 為目的法規 **Principle / Management Based Regulation**	▪ National Security Law (美) ▪ 國家安全法 (台) ▪ FISMA 2002 / FISMA 2012 (美) ▪ 資通安全管理法 (台-政府) ▪ Patriot Act (美) ▪ The Foreign Intelligence Surveillance Act · FISA) (美)	▪ The Security on Network and Information Systems Directive (NISD · 歐) ▪ Cybersecurity Act (歐) ▪ **Cybersecurity Information Sharing Act 2014 / Cybersecurity Act 2015 (CISA 2015)** ▪ **NIST Small Business Cybersecurity Act 2017(美)** ▪ 資通安全管理法 (台-基礎營運)	▪ 網路安全法 (中) ▪ GDPR (歐) ▪ 個人資料保護法 (台) ▪ Privacy Act of 1974 (美)	▪ 刑法 (台) ▪ Cybercrime Convention(國際) ▪ Computer Fraud and Abuse Act 1984 / National Information Infrastructure Protection Act 1996 (美)
組織設計與 執行效果的法規 **Performance Based Regulation**	▪ Telecommunication Act of 1996 (美) ▪ Foreign Sovereign Immunities Act (美) ▪ Intelligence Reform and Terrorism Prevention Act (美) ▪ Homeland Security Act 2002 ▪ Chemical Facility Anti-Terrorism Standards (CFATS · 2007 · 美) ▪ North American Electric Reliability Corporation (NERC · 2006 · 美)	▪ **Critical Infrastructure Research and Development Advancement Act of 2014(Bill 美)** ▪ **Federal Exchange Data Breach Notification Act of 2015 (Bill美)** ▪ **Cybersecurity Enhancement Act of 2014(美)** ▪ **National Cybersecurity and Critical Infrastructure Protection Act 2013 (美,為修正 Homeland Security Act 2002)** ▪ **Cybersecurity and Infrastructure Security Agency Act 2018 (美)** ▪ **GLBA(美)/HIPAA (美)/Bank Secrecy Act (美)** ▪ **Obama PPD-63 (行政命令 · 美)**	▪ Privacy and Electronic Communications Directive 2002 (2002/58/EC) (歐) ▪ Family Education Rights and Privacy Act – FERPA (美) ▪ Children's Online Privacy Protection Act (美) ▪ E-Privacy Regulation (2019 · Bill · 歐)	▪ Clarifying Lawful Overseas Use of Data Act (Cloud Act 2018) · (美) ▪ Cybercrime Convent Amendment (CETS -No.185) (歐) ▪ Uniform Trade Secret Protection Act (美) ▪ 營業秘密法 (台) ▪ The Directive on Protection of Trade Secret (歐)
資安技術基礎法規 **Technology Based Regulation**	▪ CAN-SPAM Act of 2003(美) ▪ 行政院及所屬各機關資訊安全管理要點 ▪ 行政院及所屬各機關資訊安全管理規範	▪ **Protection of Source Code Act(2018 · 美 · Bill)** ▪ **IoT Cybersecurity Improvement Act (2019 · 美 · Bill)** ▪ European Cybersecurity Certification Framework (歐)		

1. David Bernard Thaw, (2011), Characterizing, Classifying, and Understanding Information Security Laws and Regulations: Considerations for Policymakers and Organizations Protecting Sensitive Information Assets", Dissertation of Doctor of Philosophy, of University of California, Berkeley, Spring/2011, pp. 4 – 6.
2. Matthew C. Waxman, (2017), Cyber Strategy & Policy : International Law Dimension, Columbia Law Journal SSRN:https://ssrn.com/abstract=2926099.
3. 萬幼筠, (2018), 我國資訊安全法律之探討 – 以關鍵基礎建設保護為核心, 政治大學法律研究所論文

EU 將 CI主要的Cybersecurity全球標準, Mapping其Controls 於下述文件

- **ISO 27001**
  ISO/IEC 27001[2], part of the growing ISO/IEC 27000 family of standards, is an Information Security Management Systems (ISMS) standard published in October 2013 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). ISO/IEC 27001 formally specifies a management system that is intended to bring information security under explicit management control.

[2] https://www.iso.org/isoiec-27001-information-security.html

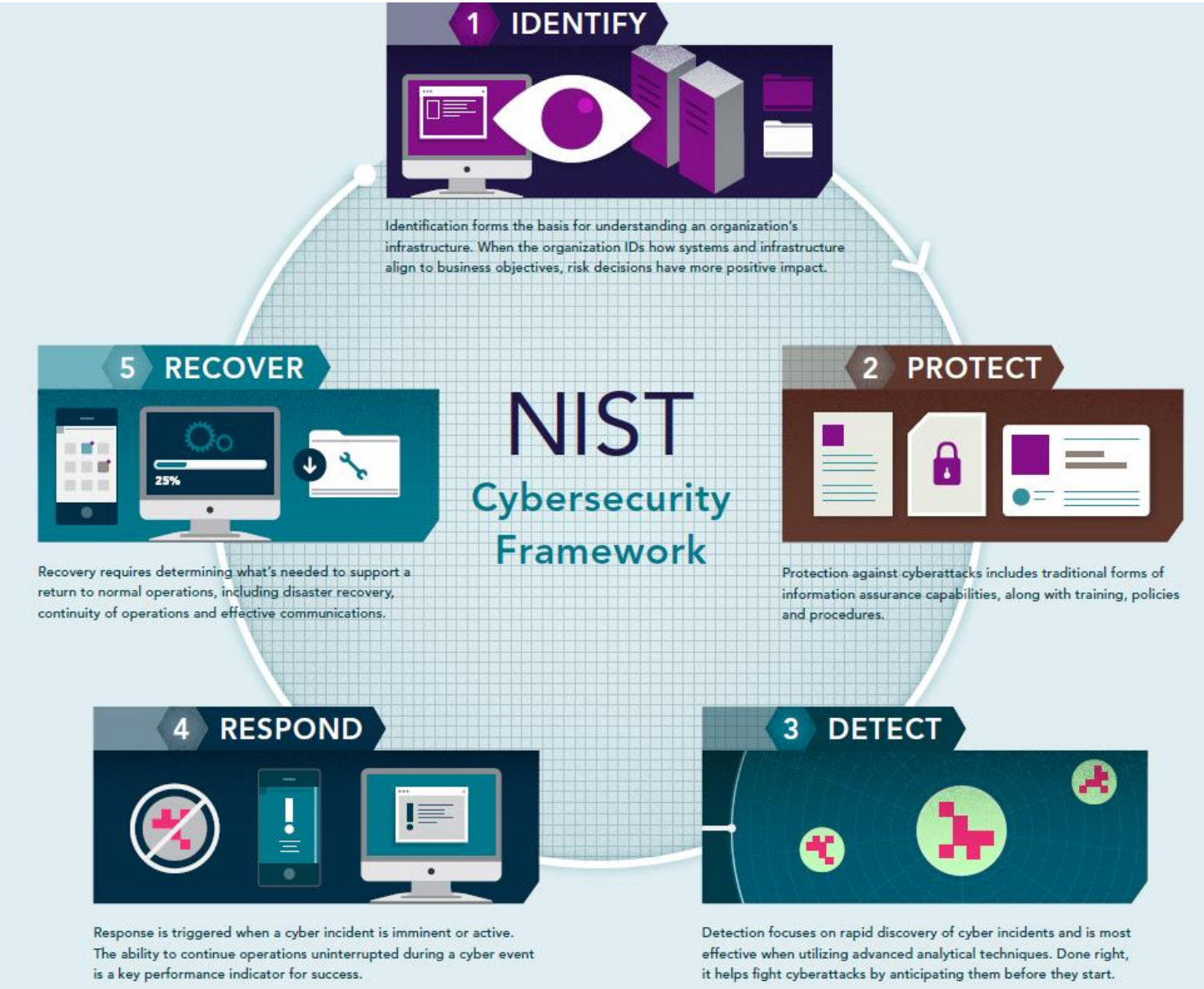
- **ANSI ISA/IEC 62443[3]**
  ISA (International Society of Automation) and IEC have developed the IEC 62443[4] series of standards in order to address the need to design cybersecurity robustness and resilience into industrial automation control systems (IACS). The concept of industrial automation and control systems electronic security is applied in the broadest possible sense, encompassing all types of plants, facilities, and systems in all industries. IEC 62443 targets people, processes, systems, solutions and components/products.
- **NIST Framework for Improving Critical Infrastructure Cybersecurity[5]**
  This Framework[6] enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure. The Framework provides structure to today's multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively in industry today. Moreover, because it references globally recognized standards for cybersecurity, the Framework can also be used by organizations located outside the United States and can serve as a model for international cooperation on strengthening critical infrastructure cybersecurity.

Mapping of OES Security Requirements to Specific Sectors

DECEMBER 2017

www.enisa.europa.eu European Union Agency For Network and Information Security

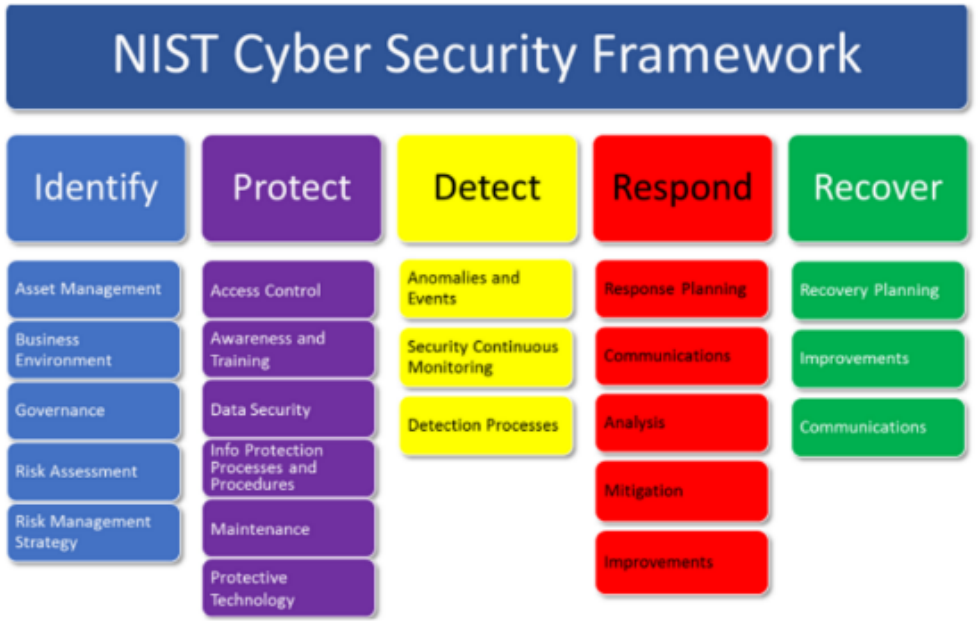
What is NIST CSF ?

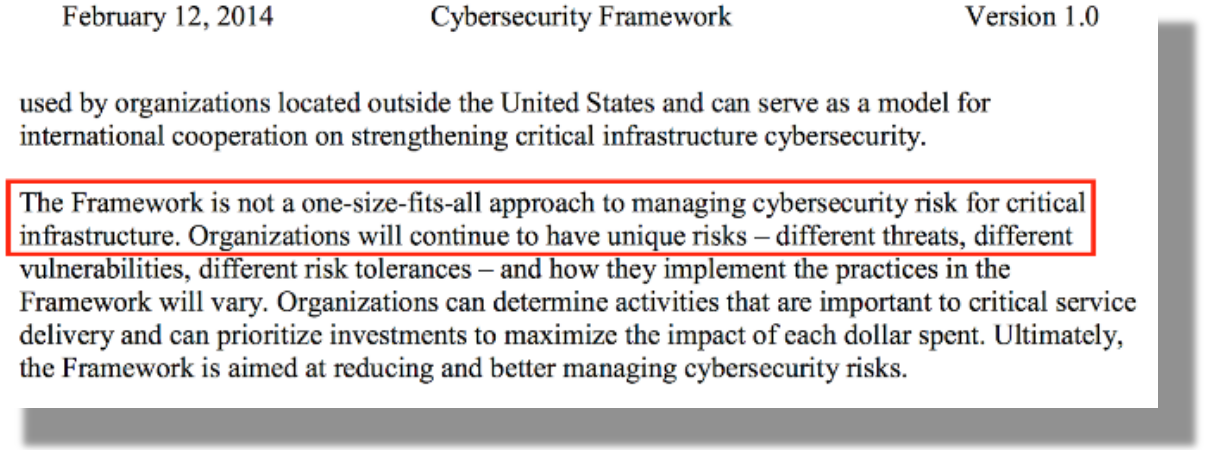


資料來源Ideos

美國NIST Cybersecurity Framework的核心想法

針對**Critical Infrastructure** 的Cybersecurity風險評估共通標準，以風險為導向、持續運作的管理架構





February 12, 2014 Cybersecurity Framework Version 1.0

used by organizations located outside the United States and can serve as a model for international cooperation on strengthening critical infrastructure cybersecurity.

The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances – and how they implement the practices in the Framework will vary. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent. Ultimately, the Framework is aimed at reducing and better managing cybersecurity risks.

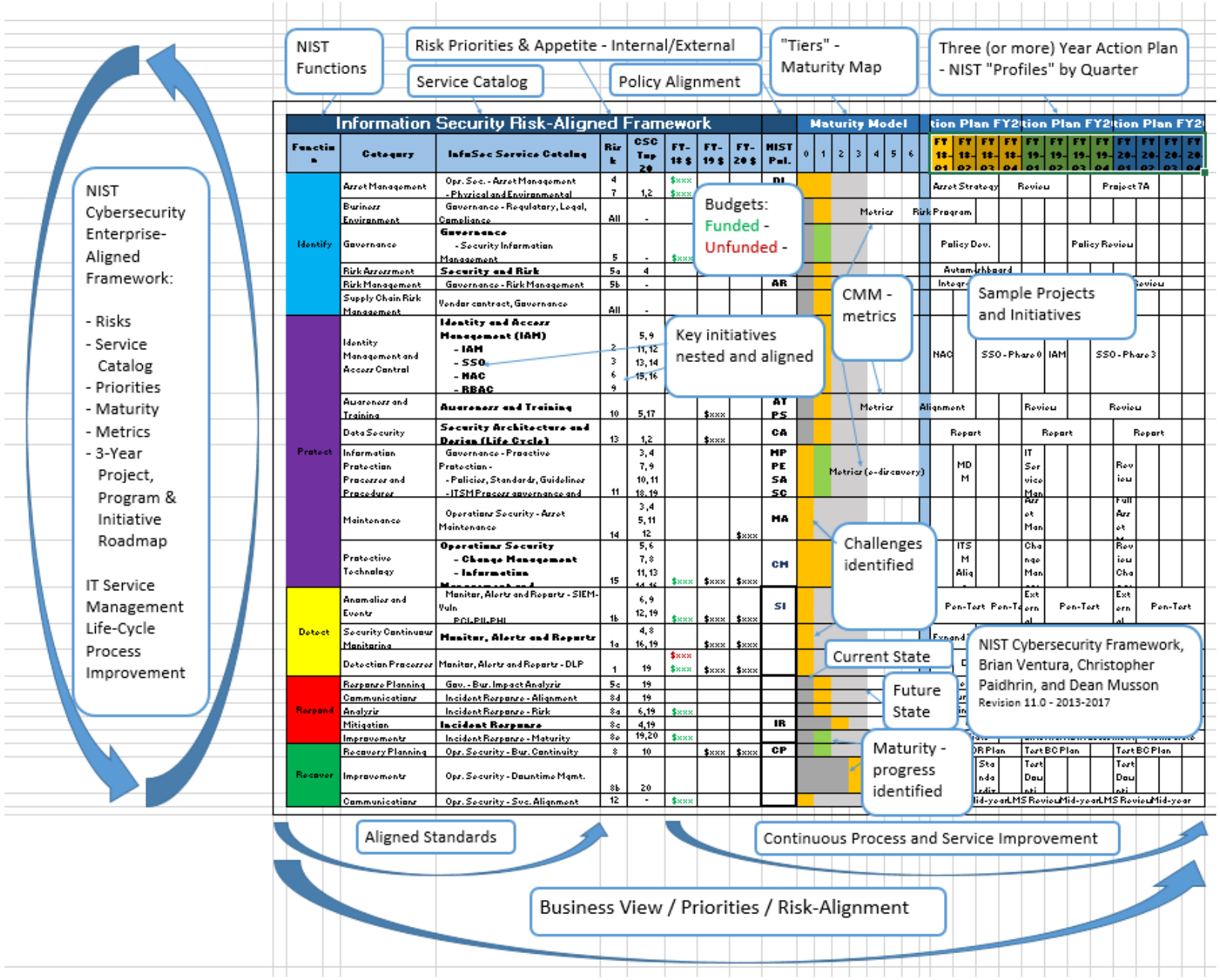
2017 V1.1改版重點

1. **安全控制面**
   - A. 資訊供應鏈安全風險管理(CSRM，亦為本次改版最大重點)
   - B. 硬體完整性/整合管理
   - C. 存取控制強化”身分識別與授權”之控制內容
   - D. 開始明確使用”Cyber Threat Intelligence”此一名詞
2. **CSF導入/使用面**
   - A. 強調新增量測(measurement)之重要性
     - a) Tier之使用
     - b) The 7-step
   - B. 強調”開發與採購”階段均應適用本框架
   - **C. 聯邦政府單位**都應考量使用CSF

Information Dependency是重要觀念

1. US 與 EU資安法對CI的定義差異, 2. 美國資安立法的核心想法

NIST CSF 實務上在Enterprise-Wide的執行樣態



NIST Cybersecurity Framework 的內涵

Framework

Framework Core

- Activities, outcomes & applicable references
- Industry standards, guidelines & practices
- 5 concurrent and continuous Functions

Identify | Protect | Detect | Respond | Recover

Identify	Understanding to manage cybersecurity risk to systems, assets, data, and capabilities
Protect	Safeguards to ensure delivery of critical infrastructure services
Detect	Identify the occurrence of a cybersecurity event
Respond	Action regarding a detected cybersecurity event
Recover	• Maintain plans for resilience • Restore any capabilities or services

Framework Implementation Tiers

- Cybersecurity Risks
- Manage Risks

Partial | Risk Informed | Repeatable | Adaptive

	Risk Management Process	Integrated Risk Management Program	External Participation
Partial	• Not formalized • Reactive	• Limited awareness • Irregular risk management • Private information	No external collaboration
Risk Informed	• Approved practices • Not widely use as policy	• More awareness • Risk-informed, processes & procedures • Adequate resources • Internal sharing	Not formalized to interact & share information
Repeatable	• Approved as Policy • Update regularly	• Organization approach • Risk-informed, processes & procedures defined & implemented as intended, and reviewed • Knowledge & skills	• Collaborate • Receive information
Adaptive	Continuous improvement	• Risk-informed, processes & procedures for potential events • Continuous awareness • Actively	Actively shares information

- Consideration
  - Risk management practices, threat environment, legal & regulatory req., objectives & constraints

Framework Profile

- Alignment of Framework Core and business requirements, risk tolerance & resources
- Establish roadmap to reduce risk aligned with organizational and sector goals
- Describe current and desired state of specific events
- Action plan to address gaps

資料來源: Tandhy Simanjuntak

NIST CSF 在各CI產業別的參考資源

Italy's National Framework for Cybersecurity

American Water Works Association's *Process Control System Security Guidance for the Water Sector*

The Cybersecurity Framework in Action: An Intel Use Case

Cybersecurity Risk Management and Best Practices Working Group 4: Final Report

Energy Sector Cybersecurity Framework Implementation Guidance

23

Texas, Department of Information Resources
- Aligned Agency Security Plans with Framework
- Aligned Product and Service Vendor Requirements with Framework

North Dakota, Information Technology Department
- Allocated Roles & Responsibilities using Framework
- Adopted the Framework into their Security Operation Strategy

Houston, Greater Houston Partnership
- Integrated Framework into their Cybersecurity Guide
- Offer On-Line Framework Self-Assessment

National Association of State CIOs
- 2 out of 3 CIOs from the 2015 NASCIO Awards cited Framework as a part of their award-winning strategy

New Jersey
- Developed a cybersecurity framework that aligns controls and procedures with Framework

24

範例 (金融服務業)：美國FFIEC Cybersecurity Assessment Framework

風險評估構面

組織既有風險

1. 技術和連接類型
2. 資訊傳遞途徑
3. 線上/行動產品和技術服務
4. 組織特徵
5. 外部威脅

CAT
評估構面

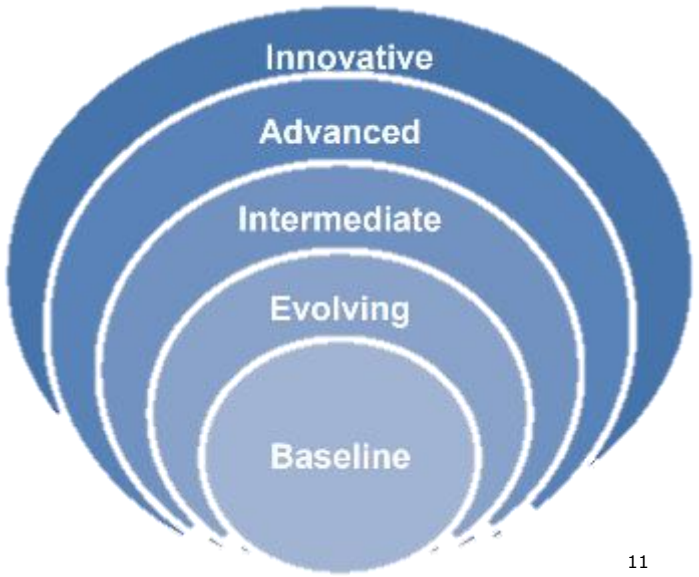
組織網路安全成熟度

1. 網絡風險管理與監督
2. 威脅情報與協同作業
3. 網絡安全控制
4. 外部依賴管理
5. 網絡事件管理與彈性

成熟度層級定義

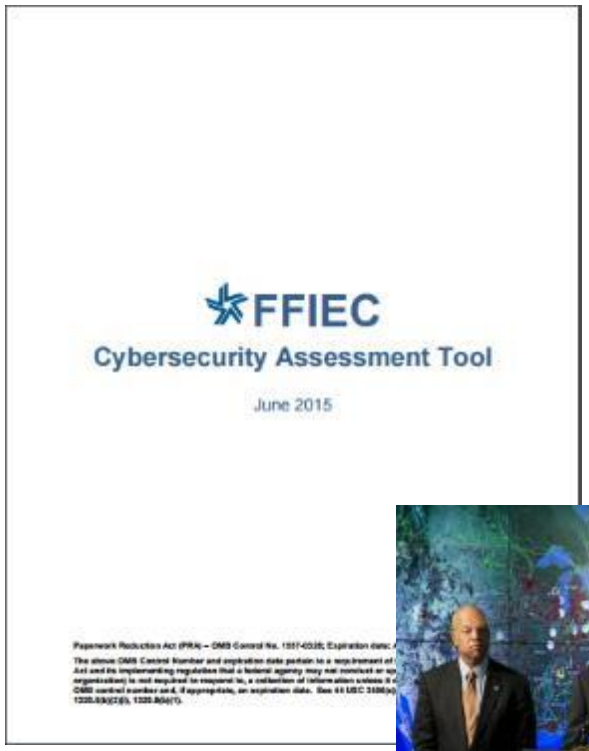
Augmented Cybersecurity

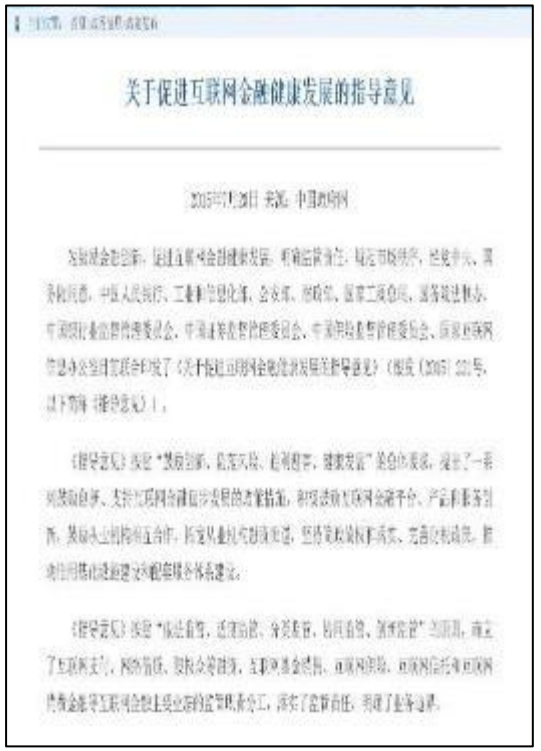
創新	促進機構和行業的人員以創新的流程和技術來管理網路風險
高級	大多數風險管理流程皆自動化，包括持續的流程改進
中等	風險控管正式、詳實、具一致性且受認證
發展中	開始推動並擴大資訊資產和系統的控管、客戶資訊的保護，但尚未要求額外的文件化程序和政策遵循
底線	遵循最低限度法律法規要求，或者在監督指導下引進控管



全球主要國家金融監理機構紛紛發布金融科技Cybersecurity相關要求

(日本與香港均採用NIST/FFIEC Cybersecurity Assessment Framework)





美國政府除設置網路安全部門、網路威脅情報整合中心、資安長外，2017年資安預算達190 億美元，比2016年高出35%。

NYDFS CRR 500 VS NIST Cybersecurity Assessment Framework

儘管與NIST提出的Cybersecurity Assessment Framework有一些相似之處，但是NYDFS CRR 500並不完全符合該框架

與NIST CSF之比對

NYDFS CRR 500	概要
網路安全計劃	▪ 總的來說，本節與NIST CSF中的識別，保護，檢測，響應和恢復功能相一致 ▪ 然而，DFS還包括對監管報告義務的要求
網路安全政策	▪ NIST CSF沒有規定DFS特別提出的各種政策領域 ▪ 此外，DFS需要董事會/同等機構批准政策
CISO	▪ NIST CSF不包括指定CISO監督和實施網絡安全計劃的DFS要求
滲透測試和漏洞評估	▪ NIST CSF包括執行風險/脆弱性評估（VA）和滲透測試（PT）的相同要求， ▪ 然而，DFS還規定了最低要求頻率（年度PT和每年一次的VA）
稽核軌跡	▪ NIST CSF需要記錄和審查稽核軌跡 ▪ DFS還需要稽核日誌，以完成和準確重建財務事務，特權帳號存取軌跡，稽核紀錄 (Trails and logs)保護，並保留至少五年(更為特定)
取存權限	▪ DFS對取存要求基於 “need to know” (Segregation of Duties) ▪ NIST CSF 要求與DFS一致
應用程序安全	▪ DFS比NIST CSF對安全開發更加規範，並且需要： ▪ 評估/測試外部採購的安全 ▪ CISO至少每年審查和更新程序/指南/標準
風險評估	▪ 廣泛對齊NIST CSF; 雖然原來的DFS提案規定至少每年進行一次風險評估，但更新的提案只規定定期進行此類評估，並根據被覆蓋實體的信息系統，非公開信息或 “ 商業運作

NYDFS CRR 500	概要
網路安全人員和情資 (Intelligence)	▪ NIST CSF 要求只大致涵蓋人員訓練與認知提升部分 ▪ DFS需要明確雇用足夠數量的合格人員，這是NIST CSF不涵蓋的
第三方信息安全政策	▪ 與供應商選擇盡職調查和第三方定期重新評估相關的DFS要求 ▪ 此要求不在NIST CSF範圍內
多重因子認證	▪ NIST CSF僅間接引用多因素認證 ▪ DFS要求更具規範性
數據保留限制	▪ 數據不再需要時, 其銷毀的要求與NIST CSF一致
培訓和監測	▪ 監測使用者活動和安全訓練認知的這一要求與NIST CSF相一致
非公開信息的加密	▪ NIST CSF需要保護(靜止數據)和(數據傳輸) – (回應歐盟隱私盾規範) ▪ NYDFS對非公開信息的加密更具規範性 (強度, 金鑰管理與解密準則)
事故因應計劃	▪ 事件因應 (incident response) 相關的要求, DFS與NIST CSF一致 ▪ 但DFS對通報機構的要求與時間性更嚴格 (畢竟是金融監理)
通知監督	▪ DFS要求在確定發生以下事件後72小時內通知監督：（1）需要向任何政府機構，自我監管機構或其他監督機構提供通知的事件，或（2） ）具有 “實質上危害正常操作的任何材料部分的合理可能性” 的事件 ▪ NIST CSF對此無細部要求

不一致　部分一致　全部一致

HKMA Cyber Resilience Assessment Framework評估架構 (擴增NIST Cyber CSF)

Inherent Risk Assessment [Low/Medium/High]				
• Technologies	• Delivery Channels	• Products and Technology Services	• Organizational Characteristics	• Tracked records on cyber threats

Maturity Assessment [**Y/AC/RA/N/NA**]						
Governance	**Internal environment**				**External environment**	
Governance	**Identification**	**Protection**	**Detection**	**Response and Recovery**	**Situational Awareness**	**Third Party Risk Management**
• Cyber resilience oversight • Strategy and policies • Cyber risk management • Audit • Staffing and training	• IT asset identification • Cyber risk identification and assessment	• Infrastructure protection controls • Access control • Data security • Secure coding • Patch management • Remediation management	• Vulnerability detection • Anomalies activity detection • Cyber incident detection • Threat monitoring and analysis	• Response planning • Incident management • Escalation and reporting	• Threat intelligence • Threat intelligence sharing	• External connections • Third party management • Ongoing monitoring on third party risk

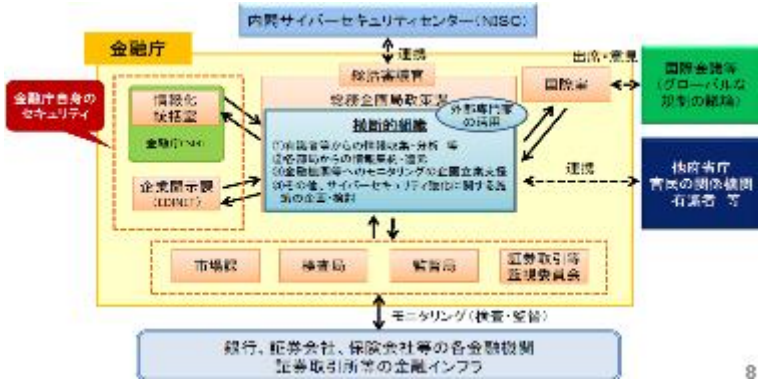
Inherent Risk Level	Minimum required maturity level
High	Advanced(A)
Medium	Intermediate(I)
Low	Baseline(B)

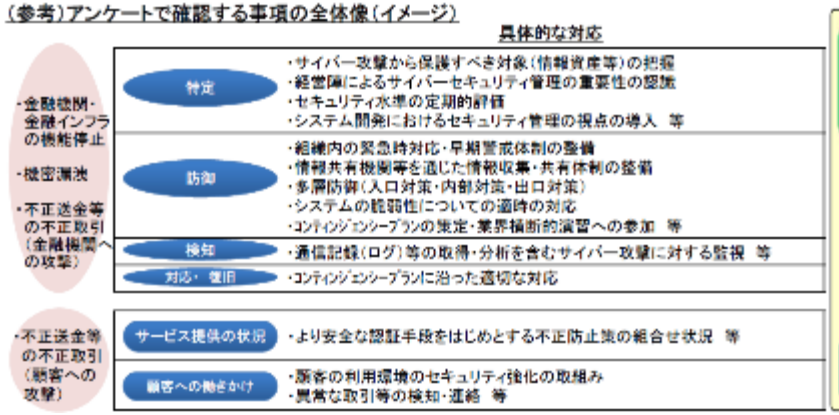
4.1.5. AIs which aim to attain the "intermediate" or "advanced" maturity level are required to execute the iCAST during the "maturity assessment" process.

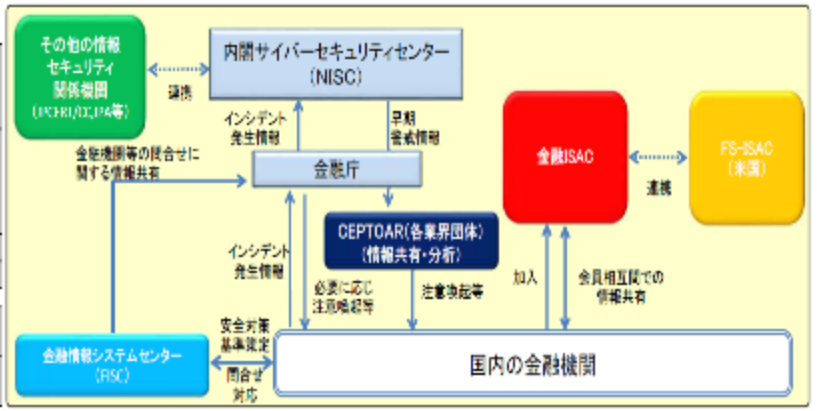
全球資安管理趨勢，日本金融廳加強金融業Cybersecurity政策措施

日本金融庁 金融分野におけるサイバーセキュリティ強化に向けた取組方針

1．サイバーセキュリティに係る金融機関との建設的な対話と一斉把握
2．金融機関同士の情報共有の枠組みの実効性向上
3．業界横断的演習の継続的な実施
4．金融分野のサイバーセキュリティ強化に向けた人材育成
5．金融庁としての態勢構築







中國網路安全法

企业应对《网络安全法》的重难点的一般要求

- 1 安全策略和管理制度
- 安全建设管理
  - 1 3 产品采购和使用
  - 1 开发实施
  - 1 安全方案设计
  - 1 测试验收
- 1 安全管理机构和人员
- 安全运维管理
  - 1 安全监测与防护
  - 1 6 数据安全
  - 1 备份与恢复管理
  - 1 风险评估

关键信息基础设施（CII）的运行安全

- 1 CII的规划建设
- 1 CII的管理机构和人员
- 1 3 CII产品和服务采购
- 1 CII的风险测评

网络信息保护

- 1 个人信息保护
- 4 5 网络内容管理
- 1 注册实名制
- 1 2 个人信息和重要数据跨境转移

网络安全事件及应急管理

- 1 安全事件处置
- 1 应急预案管理

外部监管和沟通

- 1 为国家提供技术支持和协助
- 1 配合应急协同演练
- 1 配合安全检查评估
- 1 安全事件沟通上报

1 网安法　2 个人信息和重要数据出境安全评估办法　3 网络产品和服务安全审查办法　4 互联网信息内容管理行政执法程序规定　5 互联网新闻信息服务管理规定　6 密码法

NYDFS Cybersecurity Regulations 23 - NYCRR 500框架 (因此我國公股銀於紐約有分行者, 皆有類似建置

目的

NYDFS為了促進對受監管之企業組織的消費者資訊以及資訊技術系統的保護，免受駭客攻擊之侵擾，因而於2016年9月13日更新了第一份國家擬議的法規。

1	**網路安全計畫(Cybersecurity Program)。**
2	**網路安全政策(Cybersecurity Policy)。**
3	**執行紀錄(Audit Trail)。**
4	**資安長與資安人員 (CISO & Cybersecurity Personnel)。**
5	**法規其他相關資訊 (Regulation's Additional Info)。**

法規之要求

每家公司評估其具體的風險狀況，並設計一個以穩健的方式解決風險的計畫。高級管理層必須認真對待此問題，對組織的資訊安全計畫負責，並提交年度認證以證明符合這些規定。

法規適用範圍：
美國紐約州

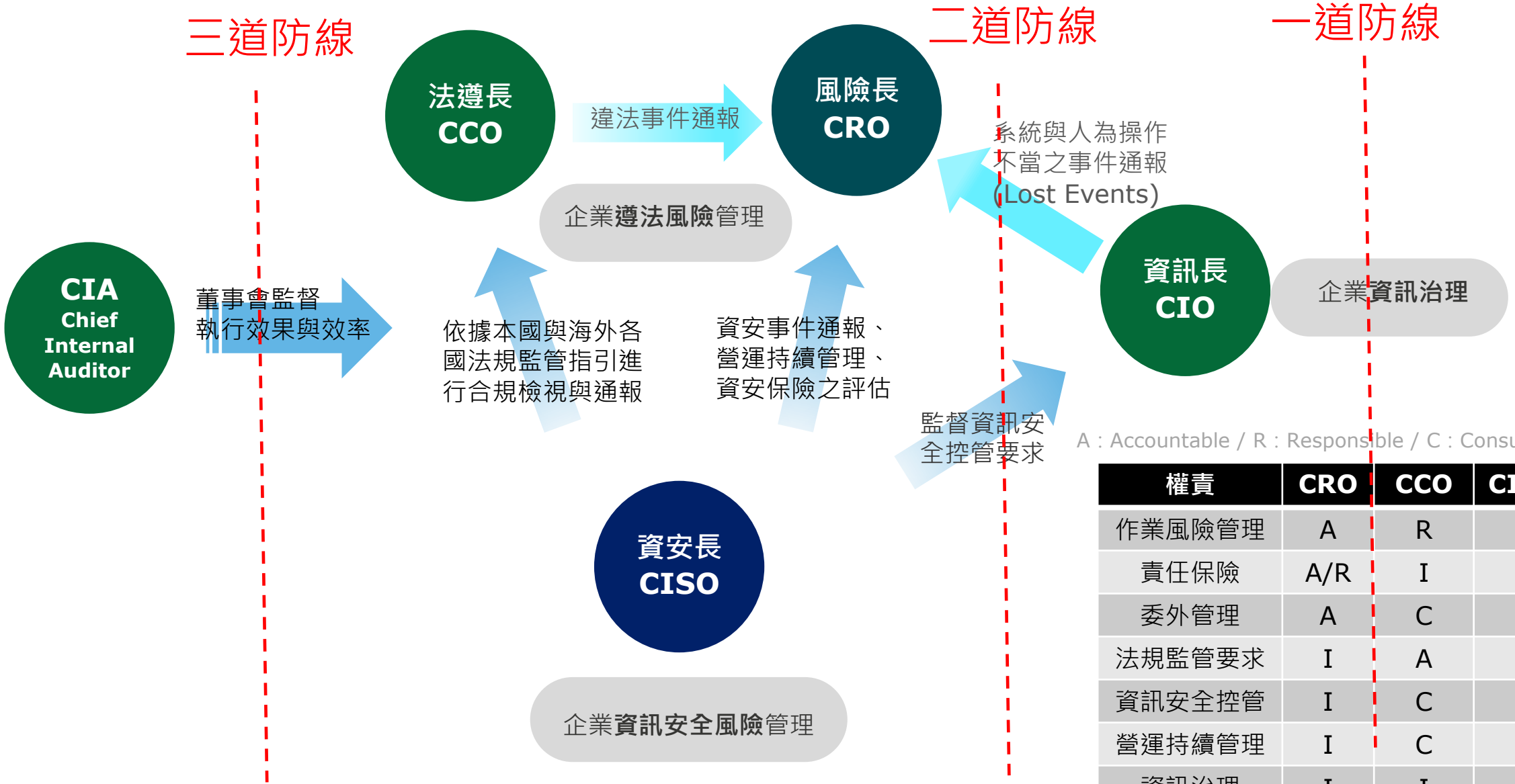
法規生效時間：
2017年03月01日

法規負責單位：
紐約州金融局(NYDFS)

NYDFS Cybersecurity Regulations 23 NYCRR 500 主要要求

- 500.3 實施並保持一份書面資運安全政策
- 500.4 企業組織的CISO應至少每年向其董事會或同等理事機構提交書面報告。
- 500.5 應每年執行滲透測試及每半年執行弱點評估。
- 500.6 企業組織應保存資訊安全事件檢測和響應的審查軌跡不少於五年。
- 500.7 應限制訪問非公開的資料系統的用戶訪問權限，並應定期審查此類訪問權限。
- 500.8 CISO定期審查、評估和更新與資訊安全計畫相關之程式、準則及標準。
- 500.9 應定期風險評估且風險評估應根據書面政策和程式進行，並應形成檔紀錄
- 500.11與協力廠商服務商有關的盡職調查及合約保護的相關準則。確保協力廠商服務商可存取或持有的非公開資訊系統及資訊系統的安全。
- 500.12 對於從外部網路訪問企業組織內部網路的任何個人，應使用多重身份驗證，除非其CISO已書面批准使用合理等效或更安全的訪問控制。
- 500.13 應包括定期安全處理500.01(g)(2)-(3)中確定的任何不再需要業務操作或其他合法商業目的非公開資料的政策和程式，除非法律或法規要求保留這些資料，或由於資料的維護方式導致對目標的處置不可行。
- 500.14 應提供定期資訊安全意識教育訓練。
- 500.15 應針對外部網路使用實施包括加密在內之控制措施，若採用補償性控制，應至少每年由CISO進行審查。
- 500.16 應建立一個書面事件響應計畫。
- 500.17 資安事件之通知需要提供給各機構；每年應在2/15之前向監督單位提交書面聲明。
- 500.21 每年準備並向監督單位提交一份符合紐約州金融服務資訊安全法規並根據2018年2月15日開始的第500.17（b）條規定的證書。
- 500.22 須自本部分的生效日期後計有180天之時間以符合本部所載的規定。

金融資訊安全在權責劃定與公司治理框架相整合 – 三道防線趨勢 (北美,歐盟, 日本, 港/新)



A : Accountable / R : Responsible / C : Consult / I : Inform

權責	CRO	CCO	CISO	CIO
作業風險管理	A	R	R	R
責任保險	A/R	I	C	C
委外管理	A	C	R	R
法規監管要求	I	A	R	R
資訊安全控管	I	C	A	R
營運持續管理	I	C	A	R
資訊治理	I	I	C	A/R

威脅場景不斷增加，被動防堵將難以應對數位時代的Cybersecurity風險

威脅來源

威脅來源之對象

- 黑帽/灰帽駭客
- 新生不滿員工
- 恐怖份子
- 駭客主義
- 駭客犯罪組織
- 自然災害
- 國家資助駭客軍隊
- 競爭對手

過去 現在

攻擊向量

攻擊之構面

- 人員
- 流程
- 科技

威脅類型

攻擊手法

- 惡意程式
- 系統弱點攻擊
- 阻斷式攻擊
- 社交工程
- 勒索軟體
- 鎖定式惡意軟體
- 先進技術(GSM,IOT等技術)

威脅目標

威脅之背後目的

- IP
- 信用卡卡號資訊
- 個人隱私資訊
- 實質金錢/虛擬貨幣
- 企業聲譽/形象
- 商業資訊/股市訊息
- 營業秘密/配方/設計圖

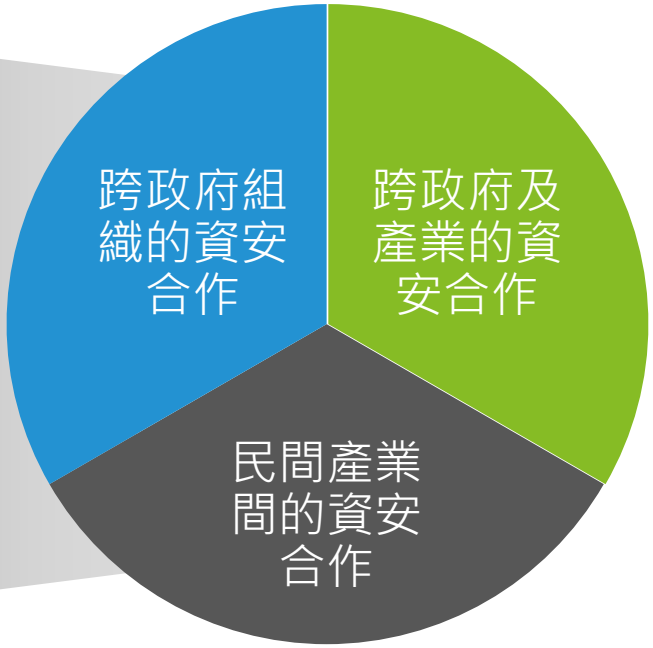
2019 年網路資訊安全趨勢預測 – 關鍵字：PPP , Info-Sharing , Cyber-Resilience

美國聯邦調查局探員於2018年 CLOUDSEC 企業資安高峰會中即預測，”網路犯罪可能來自世界上任何地區，並造成無數人受害，因此國際合作格外重要”。

美國聯邦調查局局長也在2017年3月提出了局內對抗網路犯罪的五大策略：

- 關注組織內部運作及僱用的同仁
- 縮小調查限制、建立國際合作
- 限制及制裁網路犯罪者的活動
- 透過教育、任務指派及硬體設備強化同仁的數位能力
- 加強與私部門的合作

紐約法學院近期報告指出，目前跨產業合作的方式主要分為三大主軸：



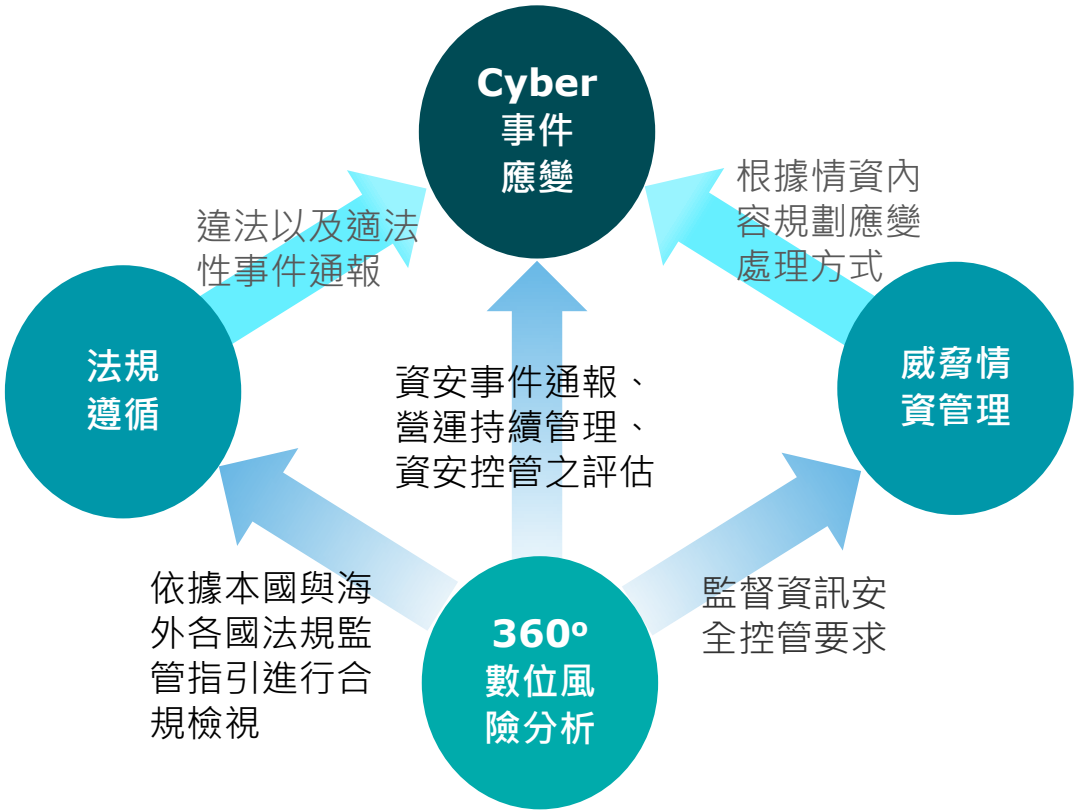
資料來源：紐約大學法學院，FBI
Cybersecurity Partnerships: A New Era of Public-Private Collaboration

身處數位時代，NIST CSF 強調需要發展的Cybersecurity能力

管理能力

治理 Governance	• 依據目標規劃組織架構 • 訂立安全目標與資訊交換政策
溝通 Communication	• 建立與內外部溝通有效的資訊傳遞方式
能見度 Visibility	• 確保組織掌握科技控管方式 • 瞭解關鍵基礎設之管控
情資 Intelligence	• 完整瞭解威脅來源之情資 • 提升規劃弱點管理與事件應變之能力
回應 Response	• 識別、分類、調查、減緩威脅事件
量測 Metrics	• 供量測之控管目標 • 應變回應之目標

核心功能



Cybersecurity + Analytic

非政府機構如何思考 NIST CSF - 全機構的360° Cybersecurity風險評估

企業基本屬性

- 公司營業項目
- 上市地點
- 區域、業務特性

發展趨勢

- 同業發展趨勢
- 產業環境
- 技術發展趨勢

策略面

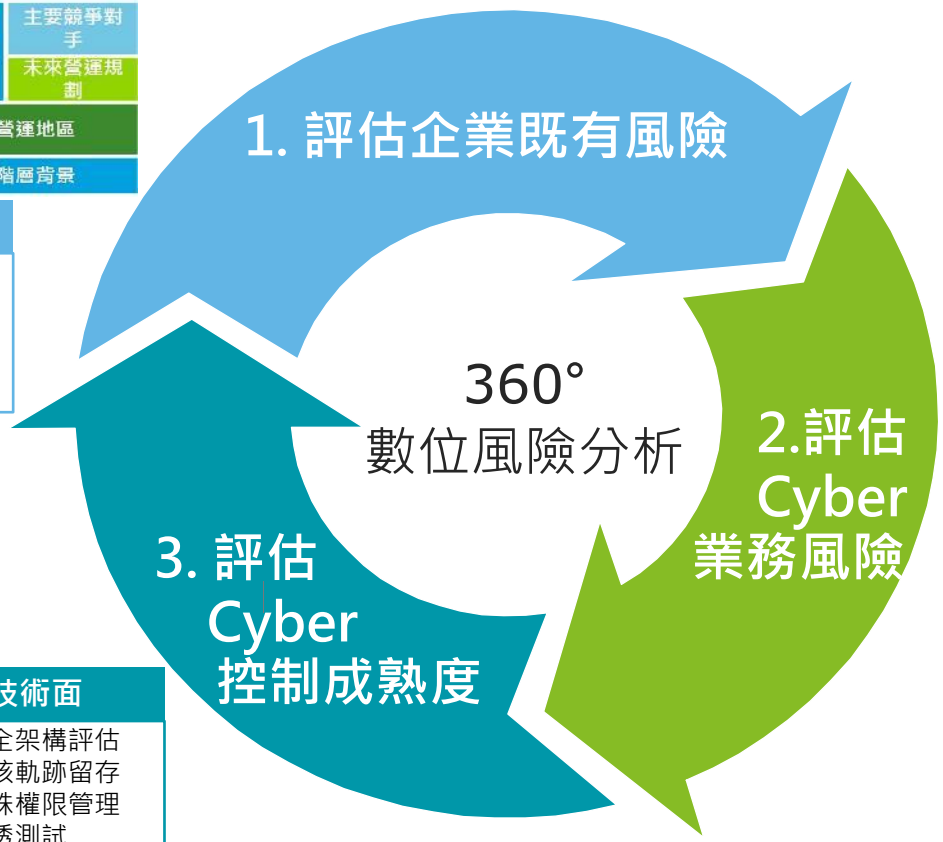
- 實施範圍
- 董事會報告
- 安全策略
- 治理組織
- 資安預算
- 人力資源配置

管理面

- 風險評估
- 資料保護
- 第三方管理
- 威脅情資管理
- 事件應變
- 營運持續

技術面

- 安全架構評估
- 稽核軌跡留存
- 特殊權限管理
- 滲透測試
- 弱點掃描
- 資安監控

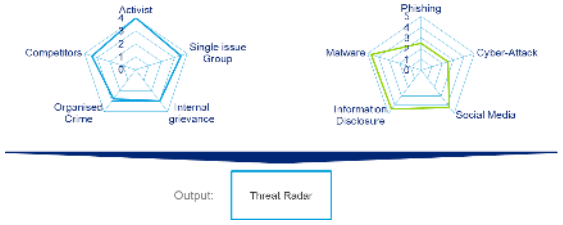


業務發展

- 業務策略發展
- 營運發展
- 企業政策策略
- 法規要求

Cyber應用

- 既有資訊資產利用狀況
- Cyber領域應用發展



NIST CSF 在立法適用後, 效果如何? –國土安全部- 聯邦基礎架構與安全局報告

Fiscal Year 2018 -2019
FISMA Metrics

May 15, 2018

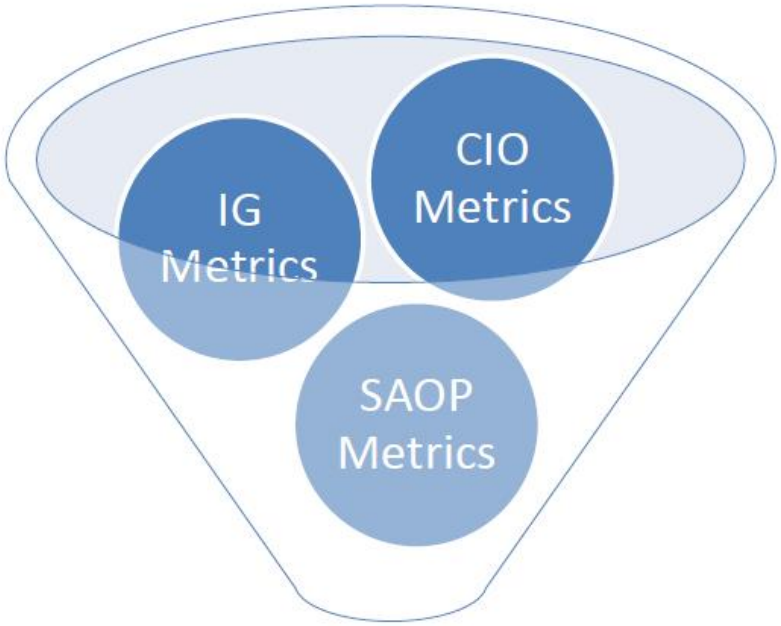
Craig Chase – DHS
craig.chase@hq.dhs.gov

Homeland Security

以NIST CSF 評估美國政府的資訊安全成熟度

NIST 使用 IEEE的定義, Metrics - 「對一個系統、元件或流程所具有的某個既定的屬性給予一個量化程度的測量。」

FISMA Metrics Trilogy



FISMA Report to Congress
CAP Reports
Quarterly Risk Management Assessments
President's Management Council

Homeland Security

Summary of FY 2018 CIO Metrics Update Results

CIO Metrics

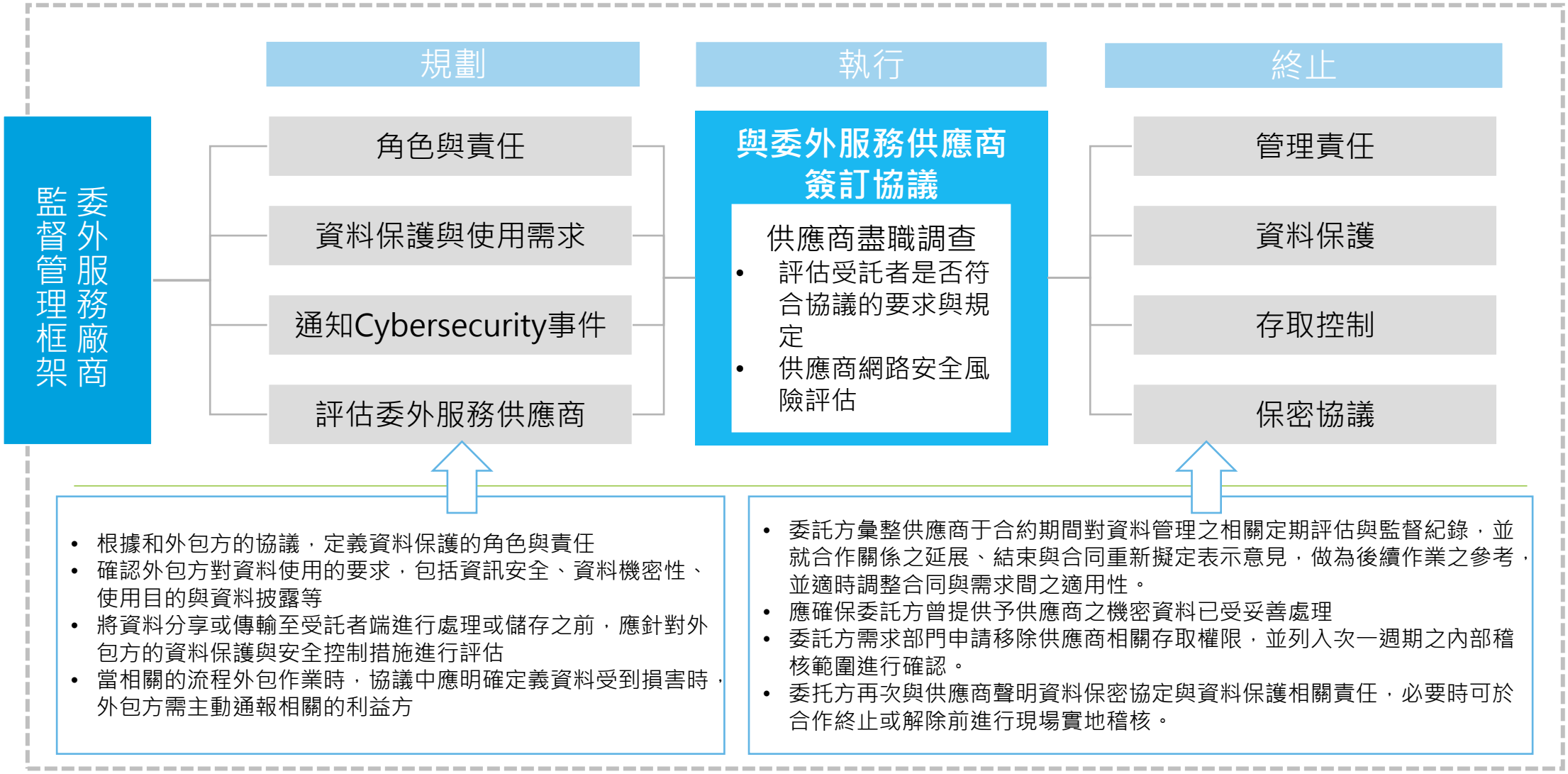
Results	# of FY 2018 Metrics	# of Added Metrics	# of Modified Metrics	# of Removed Metrics	# of Updated FY 2018 Metrics
Identify	22	2	8	(6)	18
Protect	51	3	18	(17)	37
Detect	17	0	12	(3)	14
Respond	12	1	3	(7)	6
Recover	9	1	2	(7)	3
Total	111	7	43	(40)	78

*The total number of revised FY 2018 CIO Metrics represents a **30% decrease** from the total number of FY 2018 CIO Metrics total.*

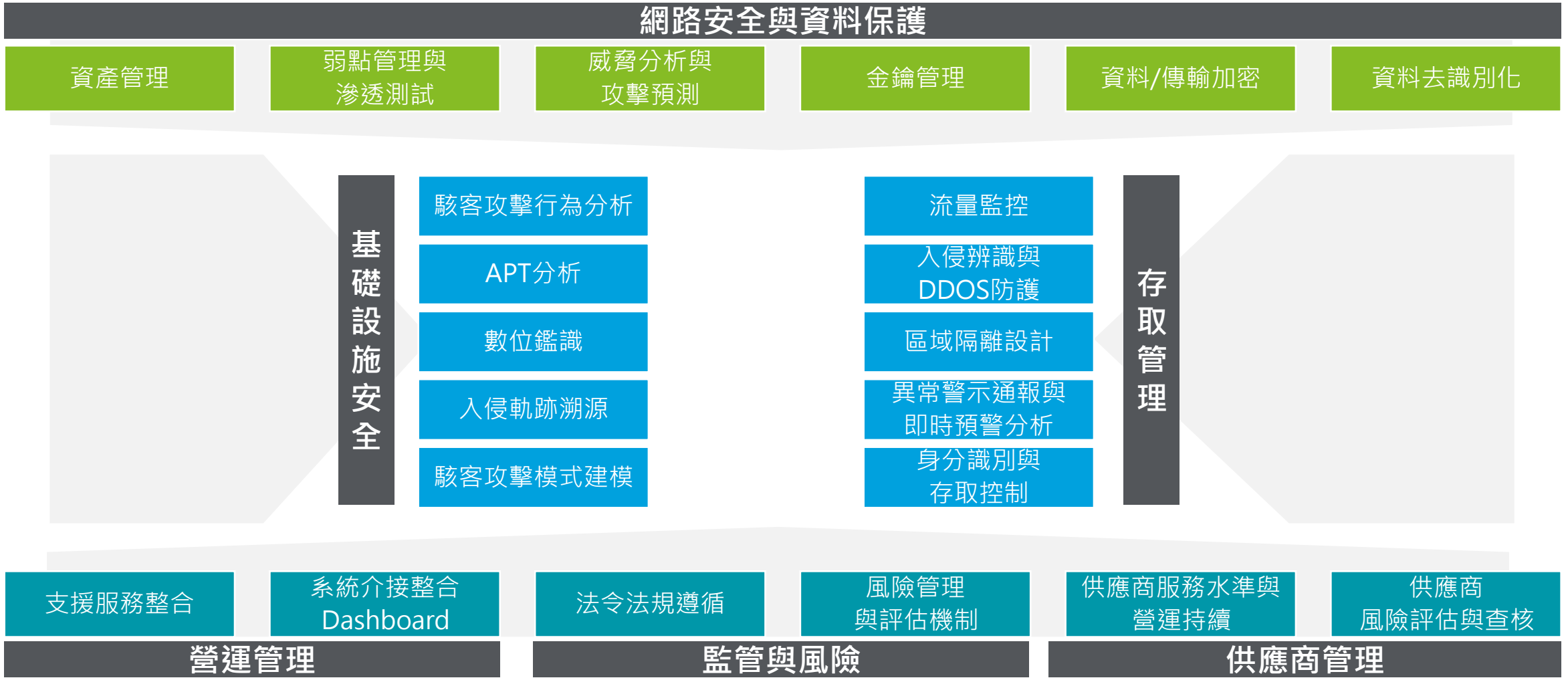
Office of Inspector General

Evaluation of CPSC's
FISMA Implementation for FY 2018

額外探討 – 資訊服務供應鏈：資通訊供應鏈管理與委外服務廠商安全管理



額外探討 – Cybersecurity 懶人包



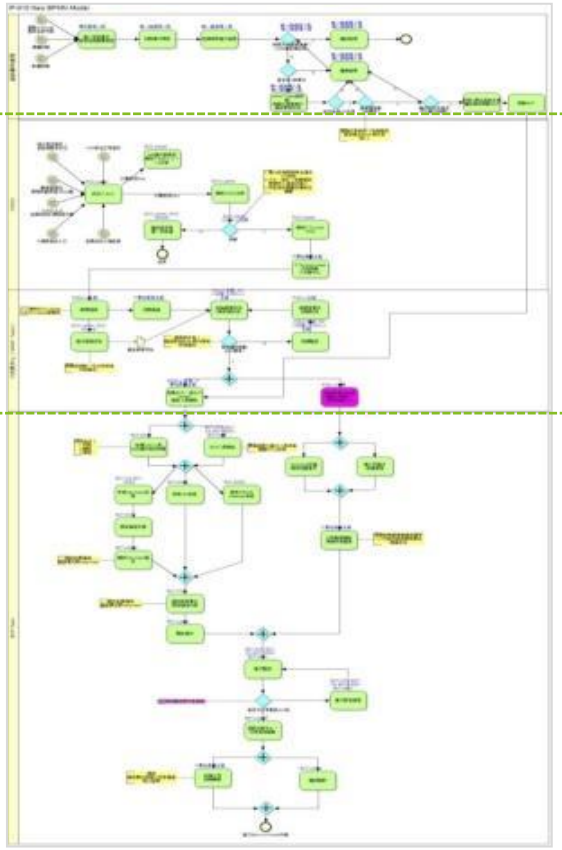
額外探討 – NIST CSF 稽核包

資安管理週期(規範) 資安保護標的(資訊資產)	資訊安全政策與 治理職能(Plan)	資訊安全規範準則 與執行 (Do)	資訊安全定期查驗 或稽核 (Check)	資訊安全事件應變 與改善 (Act)
(產業別)經營場景 營運流程 (Process)	▪ 管理資訊安全的組織與政策 ▪ 評估新科技帶來的資安風險策略 ▪ 合理的資訊資產安全保護計畫 ▪ 資訊安全評估、管理與監控的角色與權責 ▪ 溝通以達於一致資訊安全風險觀點與風險降低計畫	▪ 資訊安全風險評鑑程序 ▪ 新進或委外人員對資安權責與義務認知訓練規範 ▪ 關鍵營運流程之營運持續規劃與復原程序 ▪ 資訊安全相關控制執行之SOP (Standard of Procedure)	▪ 評估/管理與監控資安風險的報告與(自動化)工具 ▪ 資訊安全稽核軌跡留存程序 ▪ 符合程序法的資安鑑識程序 ▪ 稽核團隊的組成與報告執行規範 ▪ 資安法遵 (Compliance)查核	▪ 資安事件調查、通報與情資分享 ▪ Red Team/Blue Team演練 ▪ 資訊安全事件分析與通報 ▪ 矯正預防措施及改善落實 ▪ 資訊安全確信(Assurance)或認證(Certification)流程
支援作業活動的 資訊應用系統(軟體) (Application)	▪ 安全的資訊系統開發程序與政策 ▪ 軟體籌獲與採購之安全評估規格、方法/軟體來源國與設備來源評估	▪ 新系統上線之使用者訓練之程序 ▪ 事先訂定之應用系統修改的核准與授權程序 ▪ 軟體弱點評估與滲透測試	▪ 系統發展週期方法論與工具 ▪ 原始碼版本與程式修正控管軟體 ▪ 應用系統或主機型取存控制軟體 ▪ 應用處理之排程管理軟體	▪ 應用系統相關之除錯、關鍵風險指標(KRI)管理、容錯律、資料品質改善 ▪ 資料應用例外情況之監視與因應
資料庫管理 或大數據應用 (Data Management)	▪ 資料的所有權(Data Ownership) ▪ 資料庫的設計與管理 ▪ 資料跨境的管理與評估 ▪ 個人資料保護措施 (去識別化評估)	▪ 資料結構改變之責任與流程 ▪ 資料取得、修正與核准之程序 ▪ 去識別化方法(匿名化、假名化) ▪ 資料取得與分析的適法性落實	▪ 資料庫管理系統之管理與權責授予 ▪ 資料庫效能之監控與問題解決 ▪ 雲端安全查核與資料庫安全檢核 ▪ 去識別化方法有效性驗證與查核	▪ 資料儲存、品質與安全相關之資安監控方法與工具管理 ▪ 資料外洩事件的鑑識與調查 ▪ 資料安全情資分享、跨國蒐證(MLAT)的標準程序
作業系統平台或 雲端服務 (Platform)	▪ 硬體與軟體平台使用與上線標準 ▪ 取存控制的管理流程與責任 ▪ 平台規劃、設計、備份與安管責任	▪ 系統建置上線與測試之執行 ▪ 系統更新與版本控制處理落實 ▪ 復原計劃之建置、測試與演練	▪ 資訊平台或雲服務安全稽核 ▪ 資訊系統參數設定稽核(GCB) ▪ 系統安全自動化稽核與分析	▪ 系統效能、品質與安全相關之意外事件與外界趨勢之評估流程 ▪ 雲端安全事件應變與調查
網路或網際網路 (Networking)	▪ 合格供應商資格、服務或產品之規格(Service Level Agreement) ▪ 網路規劃/設計/備份與安全之責任	▪ 網路設定、效能與安全管理之流程 ▪ 網路流量分析與來源及端點驗證 ▪ 網路安全管理程序之落實	▪ 網路安全稽核 ▪ 網路安全防禦系統佈建 ▪ 網路分隔與拓樸查核	▪ 網路效能、品質與安全相關之意外事件與外界趨勢之評估流程 ▪ 網路安全事件應變與通報=
場址實體與資訊 (硬體)設備安全 (Hardware/Physical)	▪ 資訊處理所在地與設備安全管理與權責設計 ▪ 移動式設備(可攜媒體)之保護政策 ▪ 訊號合理範疇外之管理 ▪ 場所外之資訊內容之保護規範	▪ 工作場所與設施之實體安全設計 ▪ 必要環境控制設施之規畫 ▪ 支援資訊營運的基礎支援(電力、水、醫療、交通疏散與緊急支援安排)程序與演練。	▪ 替代電源與電壓保護裝置查驗 ▪ 資訊營運區域之防火與防水等機制 ▪ 實體進出之管理門禁機制測試 ▪ 實體設備除錯軌跡(logs)分析 ▪ 可攜式媒體的攜出入檢測	▪ 實體安全滲透測試 ▪ 防災演練與改善及教育訓練 ▪ 緊急疏散與通報應變查驗 ▪ 實體設備監控與安全設定查驗

本研究整理

額外探討 – 資通訊安全事件應變(IR)機制

沒有任何組織可以實現100%的資通訊安全



事件通報與等級識別

應急處置與影響範圍控制

事件應變措施

事件通報與應變處理路徑圖

事件發生前

準備

- 網路安全監測與預警
- 網路安全應變計劃
- 網路安全應變演練

事件發生時

回應

- 損害評估
- 損害控制
- 輿情監控
- 危機公關
- 資源協助
- 關聯方通報

事件發生後

恢復

- 業務或系統恢復
- 證據保全
- 分析與報告
- 持續改進

額外探討 – 資通訊安全攻防演練 (紅藍大對抗) – NIST CSF最知名的演練 (曙光計劃)

確認範圍
- 識別主要功能
- 識別關鍵服務或系統
- 選定測試目的危害手法

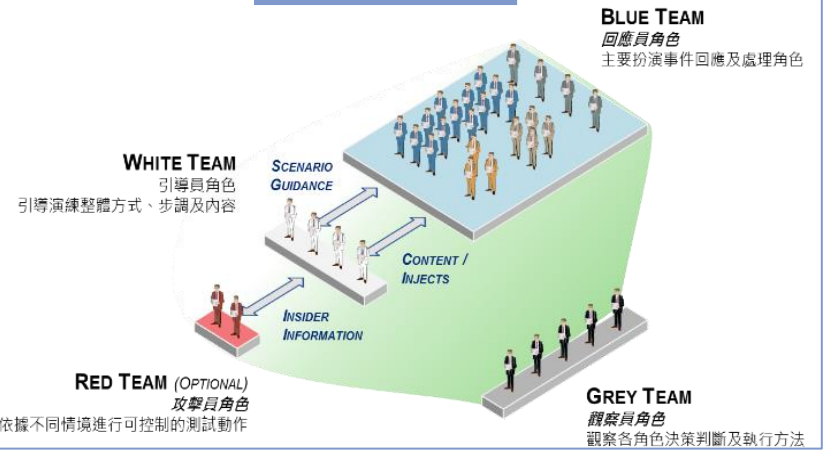
威脅情資分析
- 威脅情資報告的選用
  - 一般通用性報告
  - 客製化報告

設計演練情境
- 測試演練目標
- 測試演練起始狀態
- 工作項目關聯清單
- 演練時程與里程碑
- 中止與終止演練條件

執行演練
- 實地測試演練
- 工作小組溝通

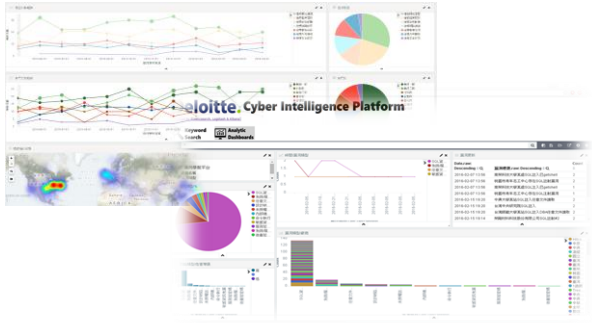
報告與檢討
- 測試演練概覽報告
- 威脅情資模擬測試報告

演練角色規劃



演練情境規劃

考量威脅情資擬定演練情境



演練作業分工

階段 \ 角色	AI – Management	AI – Control Group	Threat Intelligence team	Red team
Scoping	Form control group	Determine scope and goal		
Threat Intelligence		Provide necessary information	Perform threat analysis	
Testing Scenarios				Create scenarios
Test		Monitor progress Review issue list	Provide progress update Provide feedback / instruction	Conduct testing Draft issue list
Reporting	Endorse report	Prepare testing report for management approval including remedies		Draft report

額外探討 – 數位證據保全及鑑識分析 (主權特質的資安風險考慮)

識別

- 尋找：找出任何可能潛藏證據物件
- 辨識揮發性：優先處理判別存在的斷電就消逝資料

蒐集

- 封裝：將數位證據妥善保護封緘
- 運送：以防震防撞防高溫高濕方式專人親送至實驗室

擷取：必要時在事件現場進行

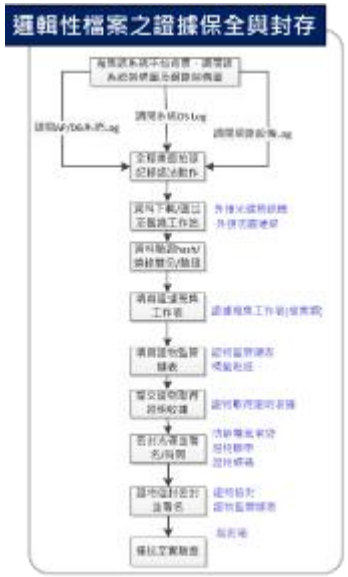
- 產出複本：以專有方式複製硬碟，以做為後續分析目標
- 同一性驗證：建立比對硬碟雜湊值，以證明內容未竄改

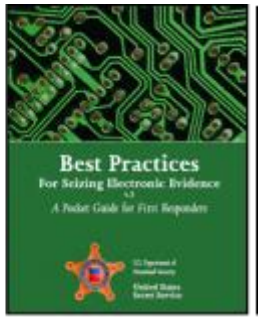
實驗室數位鑑識分析

- 靜態媒體分析：以還原/搜尋/比對方式調查硬碟內容。
- 即時系統分析：以模擬電腦系統方式進行環境重建

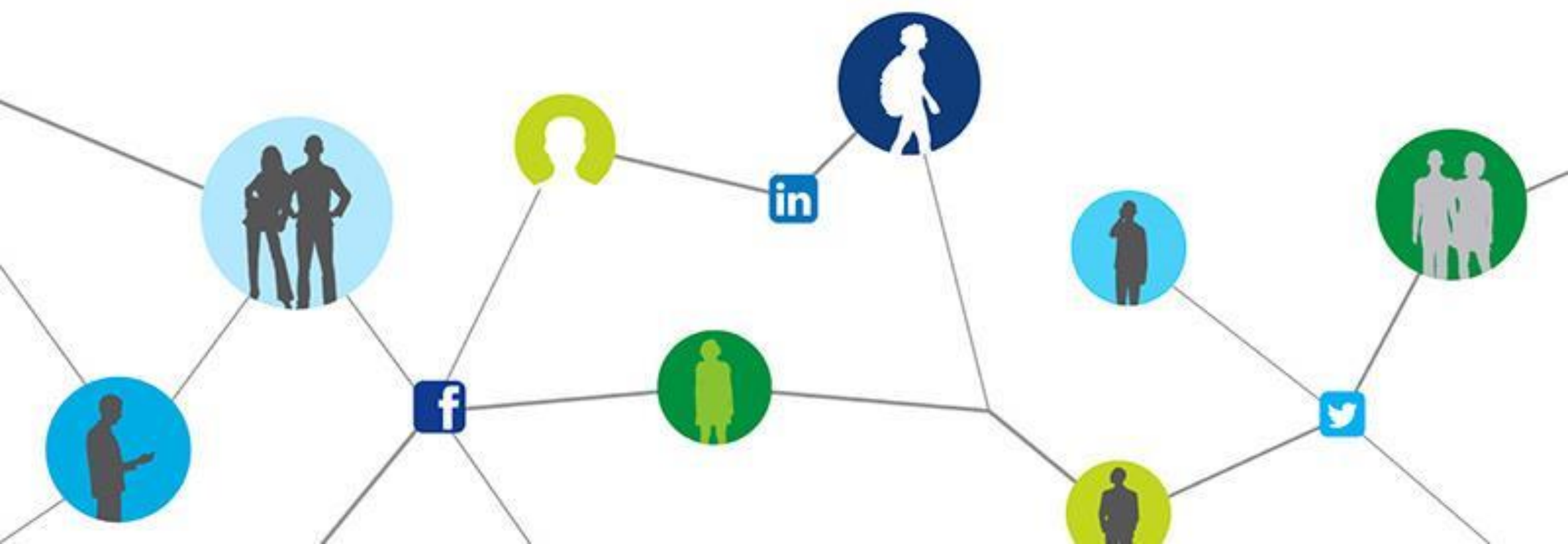
記錄 ：全程攝影與文字記錄下相關資訊

保存 ：嚴謹處理證物妥善保存，以證據監管鏈保持當責人員





Q & A



Deloitte.

勤業眾信