CYBERSEC 2025 臺灣資安大會 | 4/15-4/17 臺北南港展覽二館

SECURITY STRATEGY & CASE STUDY

SECURITY STRATEGY & CASE STUDY

海洋研究機構資安治理初探與未來展望

TEAM CYBERSECURITY

許友貞

財團法人國家實驗研究院/台灣海洋科技研究中心
資訊資安組 正工程師兼組長

國家實驗研究院
台灣海洋科技研究中心
Taiwan Ocean Research Institute

Agenda

1 背景簡介

3 稽核作業

2 資安治理初探

4 未來挑戰與展望

背景簡介

國家實驗研究院
台灣海洋科技研究中心
法規規範

國家實驗研究院

National Institutes of Applied Research (NIAR)

財團法人國家實驗研究院（National Institutes of Applied Research, NIAR），簡稱國研院，成立於 2003 年 6 月，隸屬於**國家科學及技術委員會（簡稱國科會）**，下轄 7 個國家級實驗研究中心，由院本部統合協調各單位之運作，以提升彈性與效率，促成國家科技發展體系之垂直整合。

建構研發平台

建構國內學術界無法獨立營運之大型技術平台，以及可以整合產業界及學術界共同進行創新研究之合作研發平台。

支援學術研究

以大型技術平台、先進科技研發能量與高度的服務熱忱，協助國內學術界進行全球頂尖之前沿科技研究。

推動前瞻科技

秉持「創新科技，守護台灣」之營運目標，以厚實的研發能量開創有利於民生福祉且具有世界競爭力的前瞻科研成果。

培育科技人才

增進大眾對科學、科技之興趣，並培養產業界所需之高科技人才，為國內學術界及產業界之進步奠定基礎。

多元且異質性高的組織，提供國內產、官、學、研界進行「地球環境」、「資通訊科技」、「生醫科技」、「科技政策」等領域所需之研發平台與技術服務。

- 國家地震工程研究中心
- 國家生物模式中心
- 國家儀器科技研究中心
- 國家高速網路與計算中心
- 科技政策研究與資訊中心
- 台灣半導體研究中心
- **台灣海洋科技研究中心**

七個研究中心地點

Locations

台北Taipei

- 財團法人國家實驗研究院
- 國家地震工程研究中心
- 國家生物模式中心
- 科技政策研究與資訊中心

新竹Hsinchu

- 國家儀器科技研究中心
- 國家高速網路與計算中心
- 台灣半導體研究中心
- 國家生物模式中心*

*Branch Office

台中Taichung

- 國家高速網路與計算中心*

台南Tainan

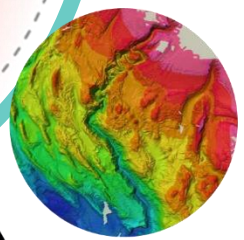
- 國家高速網路與計算中心*
- 國家生物模式中心*
- 國家地震工程研究中心*
- 台灣半導體研究中心*

高雄Kaohsiung

- 台灣海洋科技研究中心

海洋中心核心任務

Our Mission



勵進研究船營運

支援學研計畫、執行深海工作型ROV任務、海洋沉積物採樣作業以及高精度與全深度海底地形測繪、海床底質資料的蒐集等。

海洋長期觀測設施維運

- 海氣象資料錨碇浮標觀測系統
- 深海錨碇式沉降顆粒收集器平台
- 岸基海洋雷達測流系統

海洋探測設備維運

- 深海工作型水下無人載具(ROV)
- 海底地震儀(OBS)
- 長支距多頻道震測系統(LMCS)
- 長岩心採樣器

海洋環境資料彙整

海氣象資料浮標、岸基高頻雷達海流、船測及多音束水深等等多元資料彙整

海洋自主技術研發

- 海底地震儀(OBS)
- 輕型ROV
- 自動焦點堆疊顯微拍照系統
- 深拖測繪系統
- 相位陣列海洋雷達

勵進研究船

Research Vessel Legend

臺灣海洋科學與科技發展之重要載台

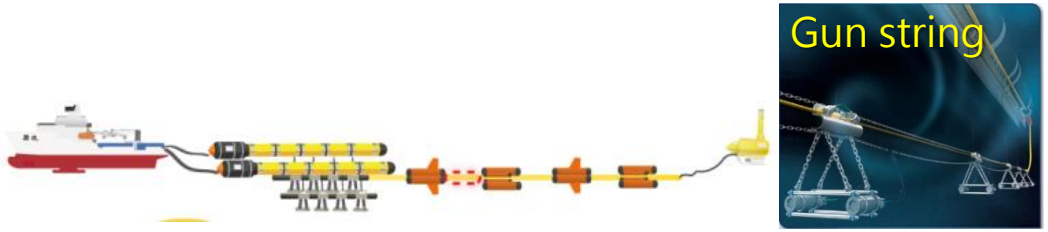
全長 ..... 76.23 m
模寬 ..... 16 m
模深 ..... 5.6 m
總噸位 ..... 2,629 T

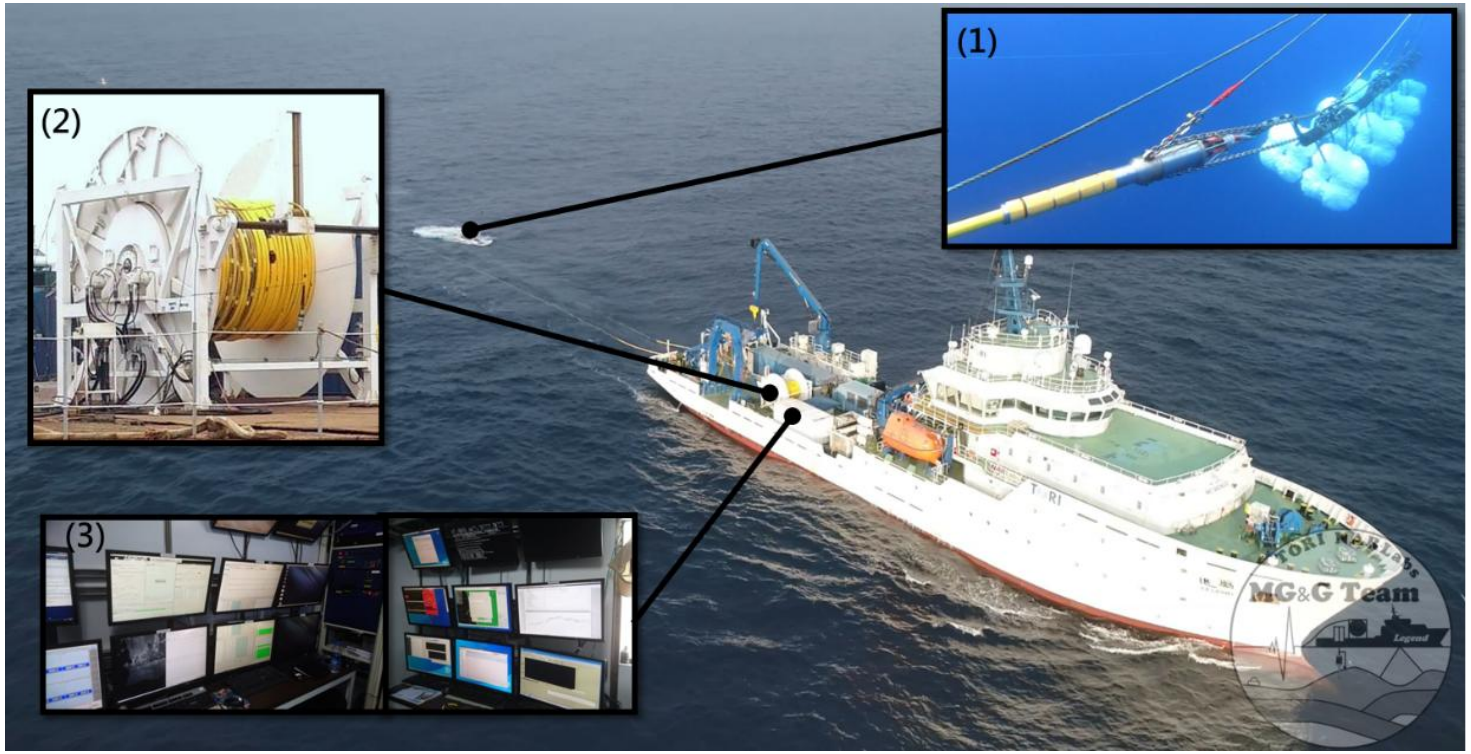
最大船速 ..... 12 kts
巡航船速 ..... 10 kts
連續航行天數 .... 30 days
船員/研究人員 ... 19 / 24

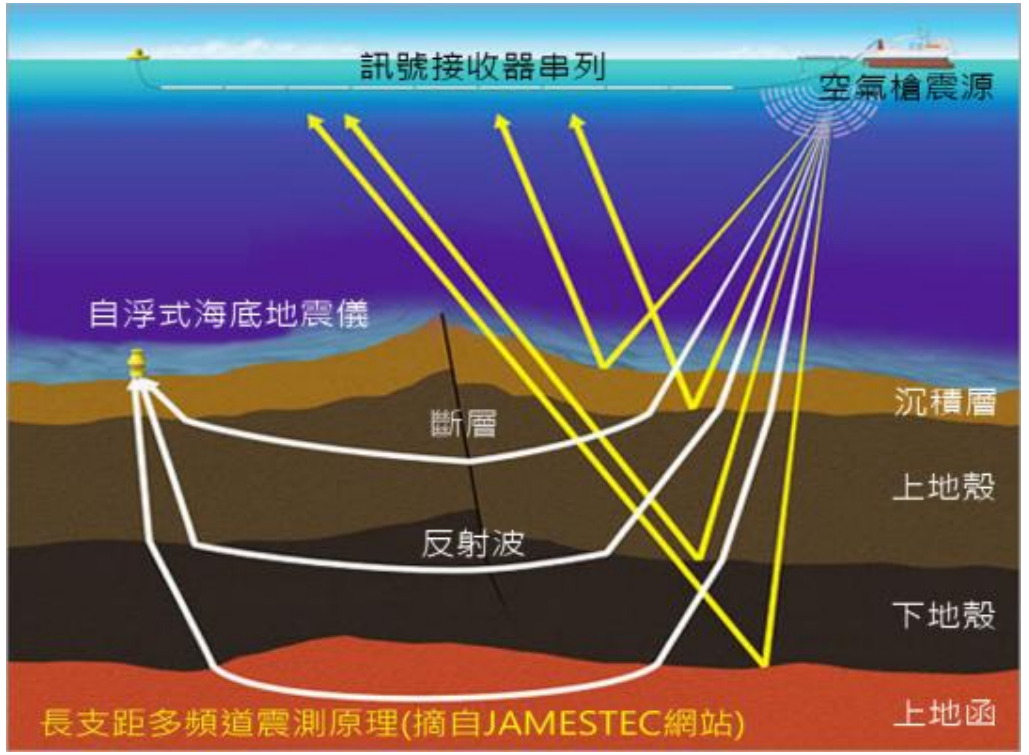
正式啟用 ..... May 2018
國內目前最大噸位之研究船
國內第一艘通過ISO 27001研究船

長支距多頻道震測

Long offset Multichannel Seismic System (LOMCS)



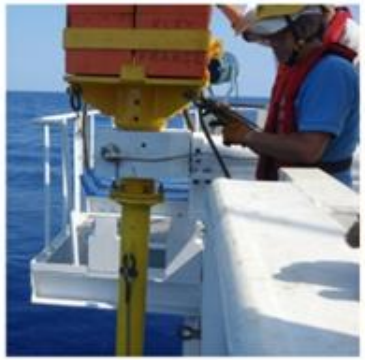
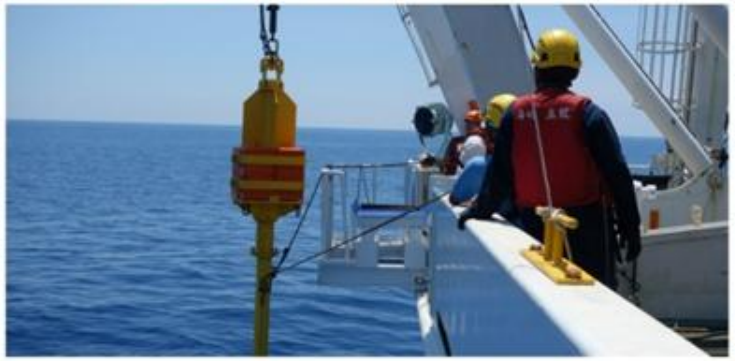




海洋岩心庫暨實驗室

Marine Core Repository and Laboratory (MCRL)

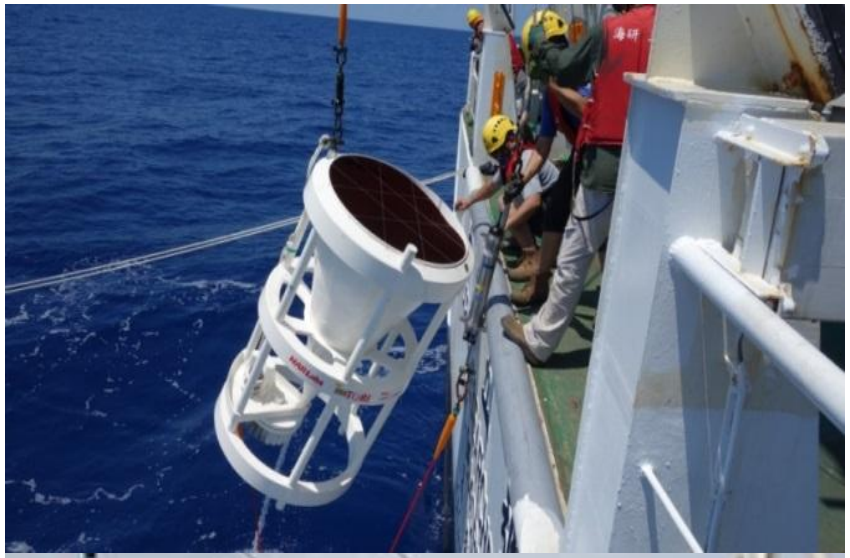


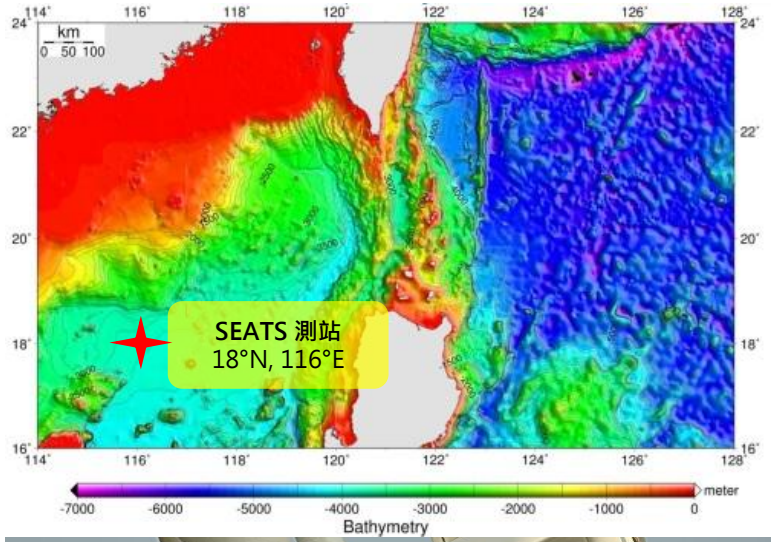




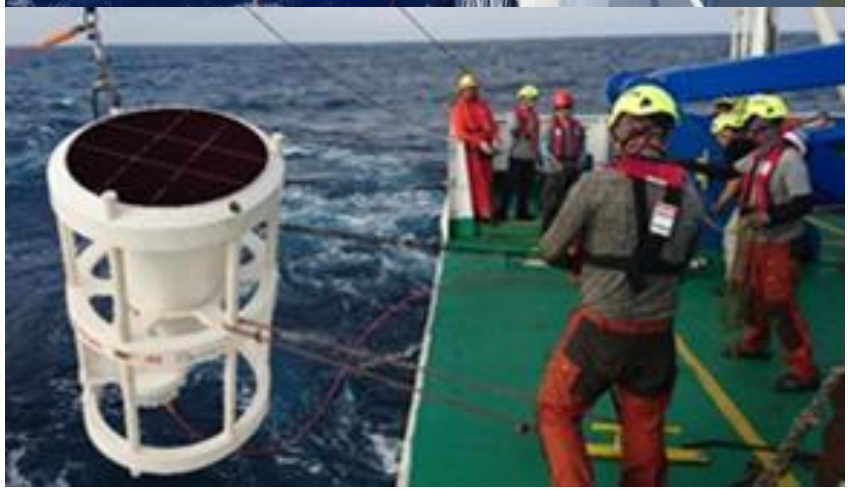
沉降顆粒收集器

Sediment Traps

南海時間序列測站（South East Asian Time-series Study；SEATS）





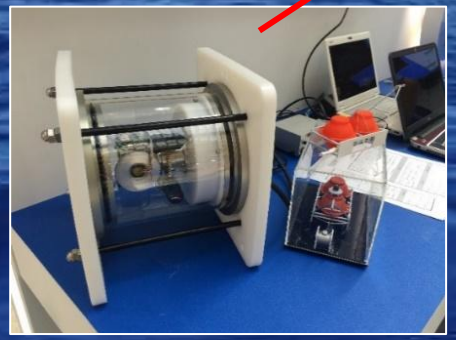


自主海洋研發科儀

Independent development of marine exploration instruments

海底地震儀 Ocean Bottom Seismometers (OBS)

Instrument Sphere



Sensor with auto Leveling

Maximum depth capability: 6,000meters

CYBERSEC 2025
臺灣資安大會

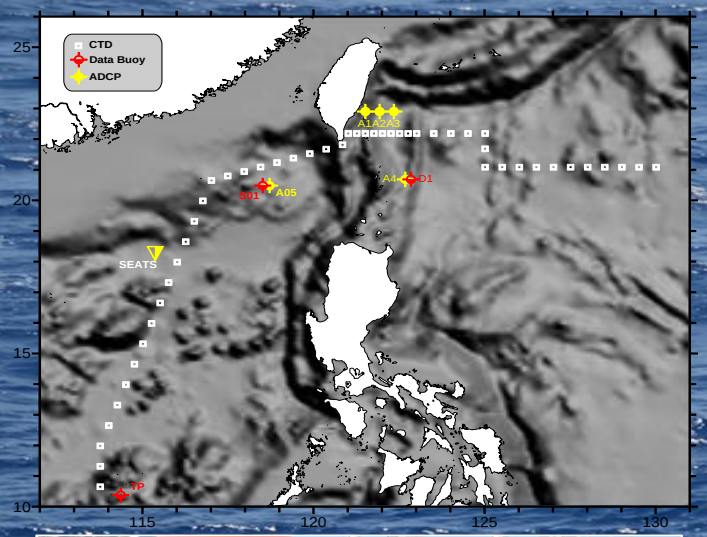
國家實驗研究院
台灣海洋科技研究中心
Taiwan Ocean Research Institute

近即時氣象資料錨碇浮標

Near real-time Data Buoys

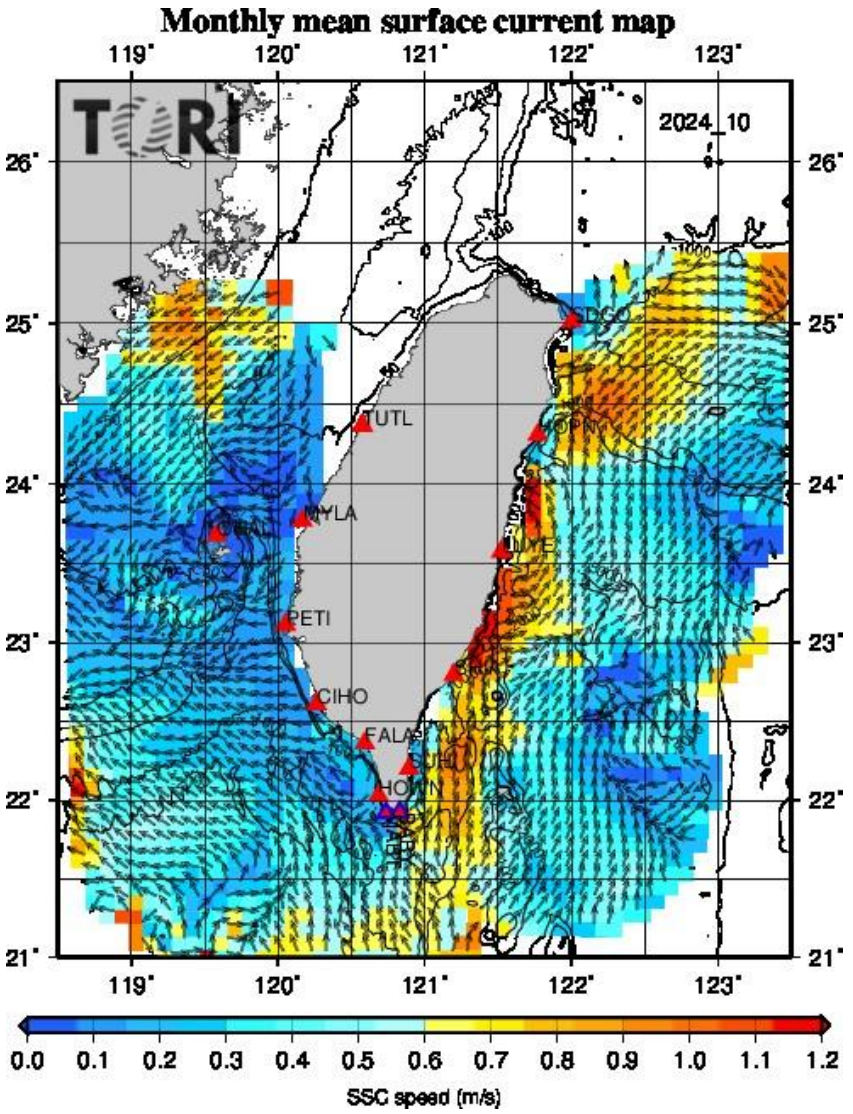
風速、溫度、壓力、
濕度、日照

海水溫度
鹽度



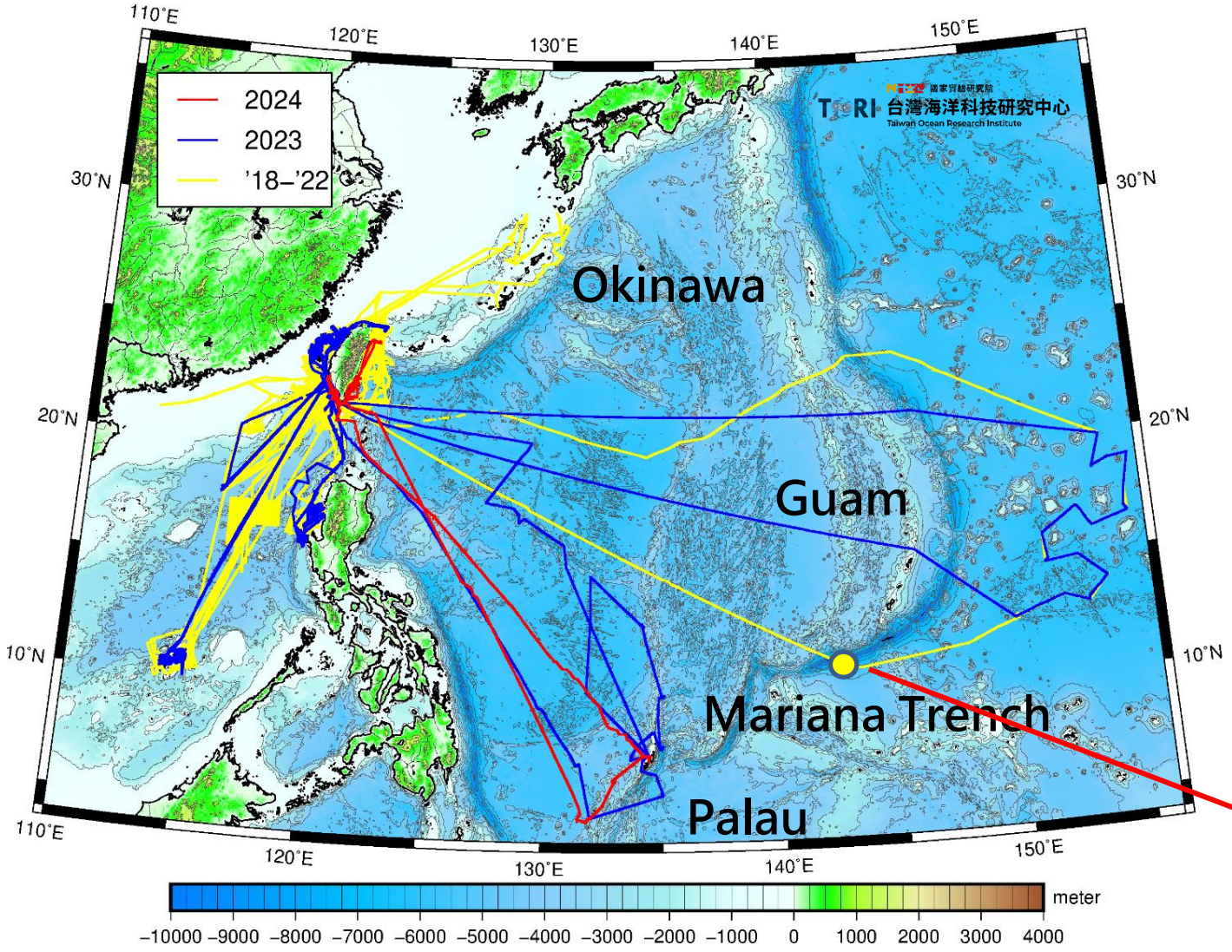
台灣海洋雷達觀測系統

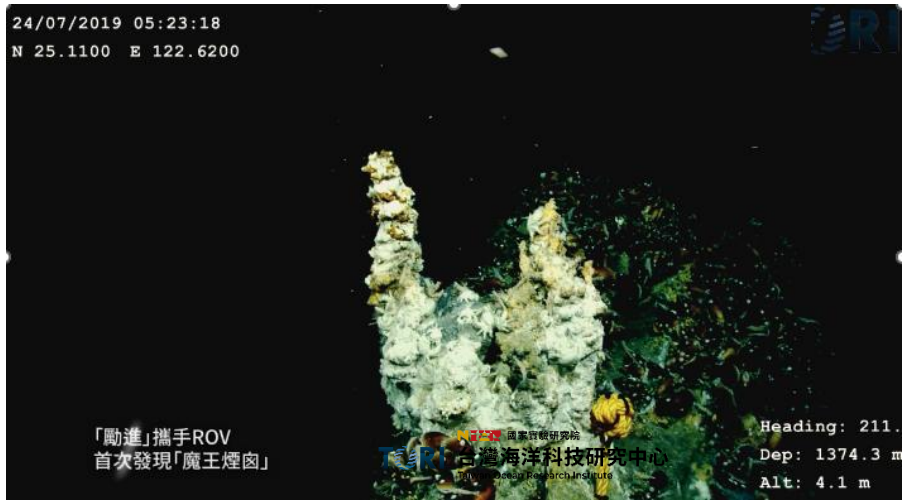
Taiwan Ocean Radar Observing System (TOROS)

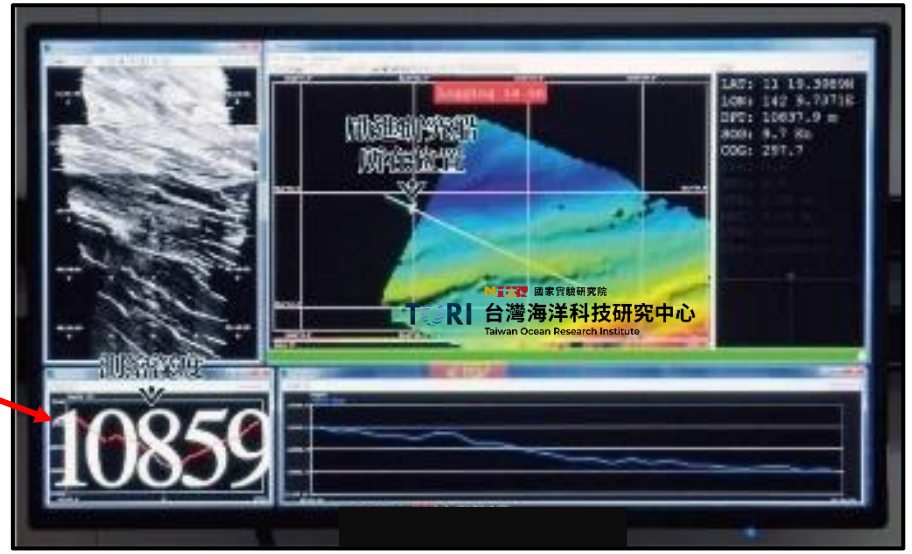


勵進研究船航次

Research Vessel Legend

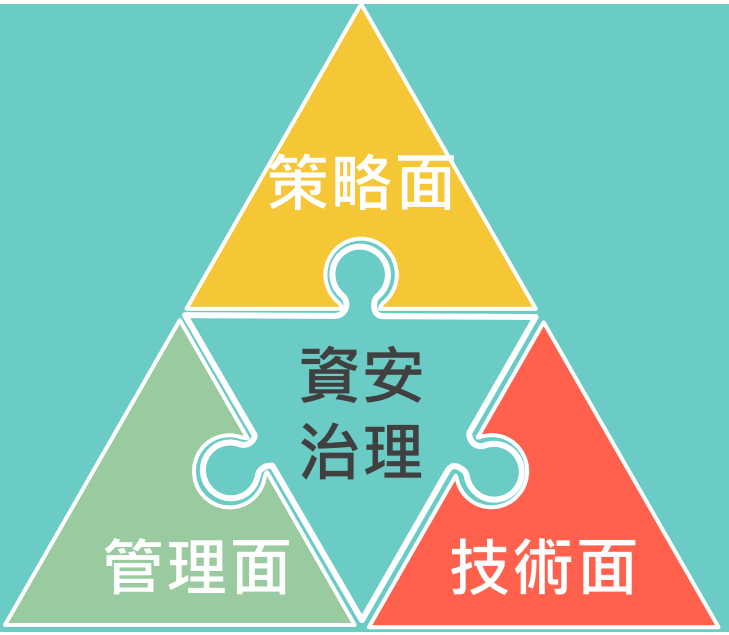






法規規範

主管機關	行政院	國科會	國家實驗研究院
母法	**資通安全管理法** **個人資料保護法** **人工智慧基本法草案**	依據資通安全管理法第十六條第六項及第十七條第四項規定訂定	
子法	資通安全情資分享辦法 資通安全事件通報及應變辦法 **特定非公務機關資通安全維護計畫實施情形稽核辦法** 公務機關所屬人員辦理資通安全業務獎懲辦法 **資通安全責任等級分級辦法** **資通安全管理法施行細則**	**國家科學及技術委員會所管特定非公務機關資通安全管理作業辦法** 辦法第六條：… 以**現場實地稽核**之方式，稽核其**資通安全維護計畫**實施情形	
作業規定	**特定非公務機關應辦事項**	**政府資助國家核心科技研究計畫安全管制作業手冊** 國家科學及技術委員會個人資料保護管理要點」	「**國家核心科技安全管制作業規定**」、「**國研院業務機密保護要點**」定期內稽並接受各級督導單位稽查。



資安治理初探

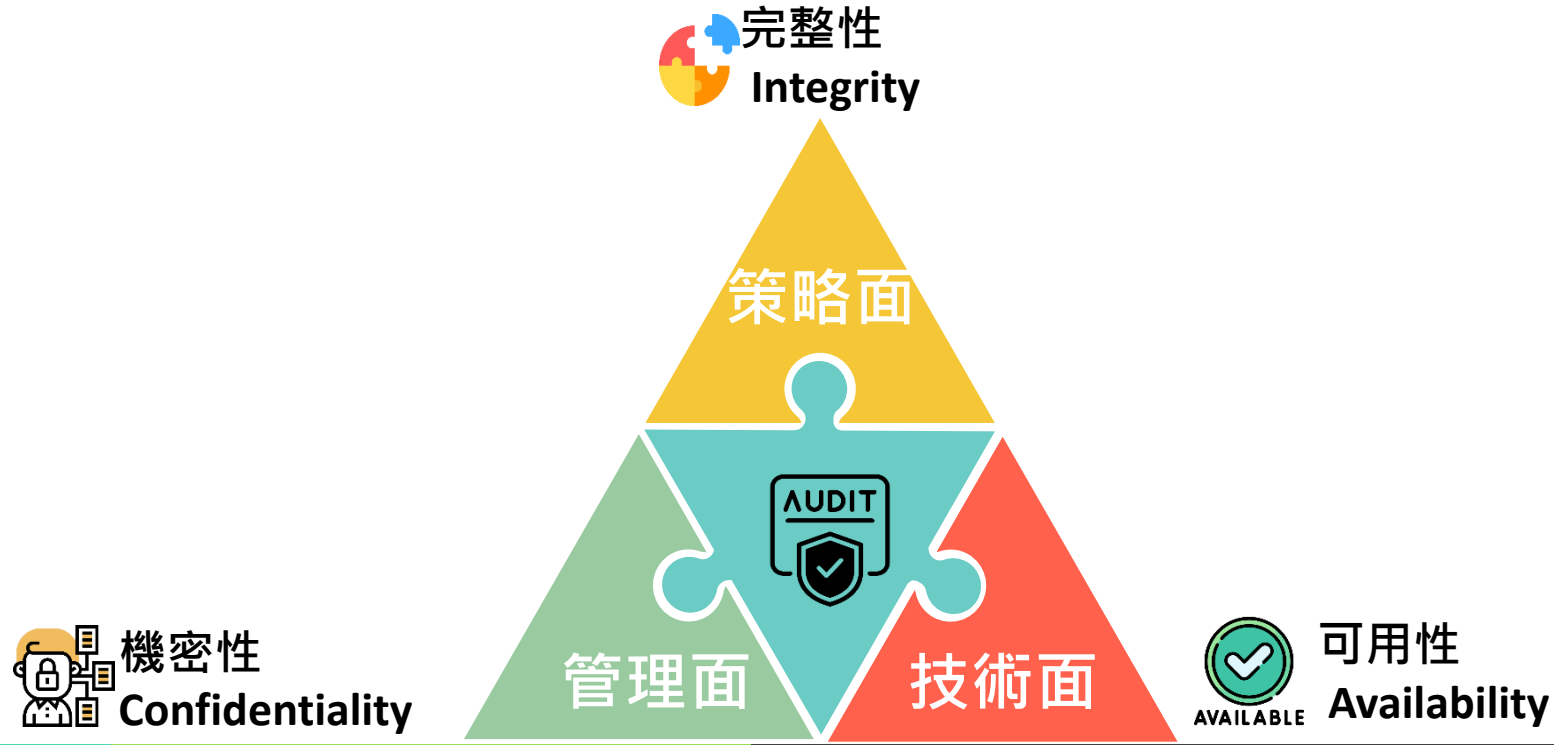
資訊資安工作任務、推動現況
基本防禦、SOC
資訊安全架構
資通安全教育訓練、社交工程演練

資訊資安工作任務

Missions

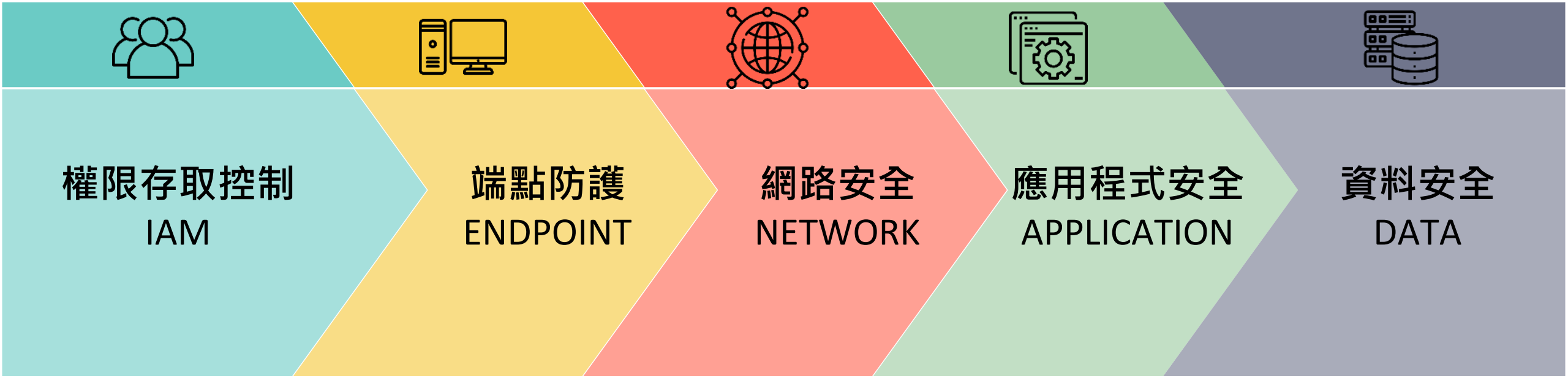
研究單位首重研究資料及研發成果，單位內部若沒有制定完善資訊安全管理策略及機制、落實執行、檢視、調整、改善及預防，網路攻防及資訊安全管理將陷入困境。

- **對外(縱向)**：存在遭受駭客入侵，導致資料外洩之風險
- **對內(橫向)**：個人資料外洩、當跳板，重者重要營業祕密、研發成果、機敏或核心資料遭竊。



基本防禦

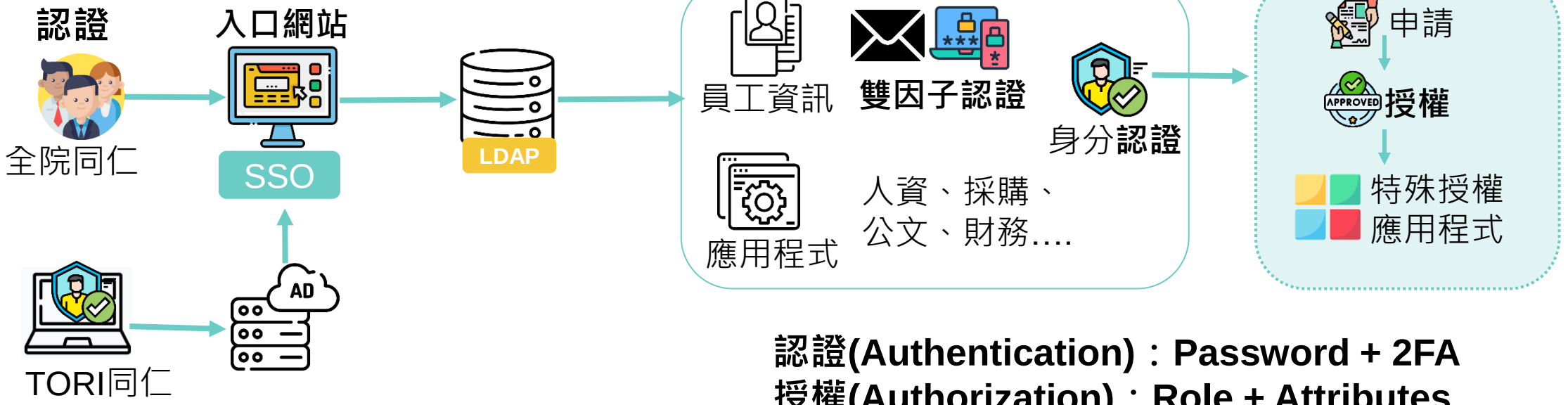
Fundamental Prevention Domains



Icon ref：https://www.flaticon.com/

權限存取控制

Identify and Access Management



認證(Authentication)：Password + 2FA
授權(Authorization)：Role + Attributes

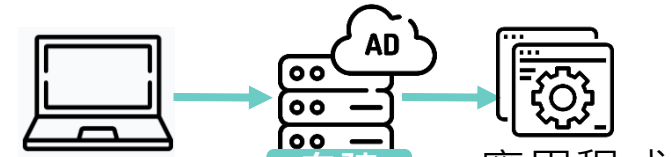
授權/特殊權限管理

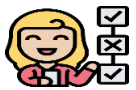
- ROOT
- 系統管理員
- 資料庫管理員
- 網路管理員
- 伺服器主機管理員

- 禁止共用帳號、特殊權限申請。
- 連線所在地限制(出國須先申請)
- 伺服器主機、資料庫系統**更新**原廠預設密碼、套用密碼原則。
- 符合密碼原則

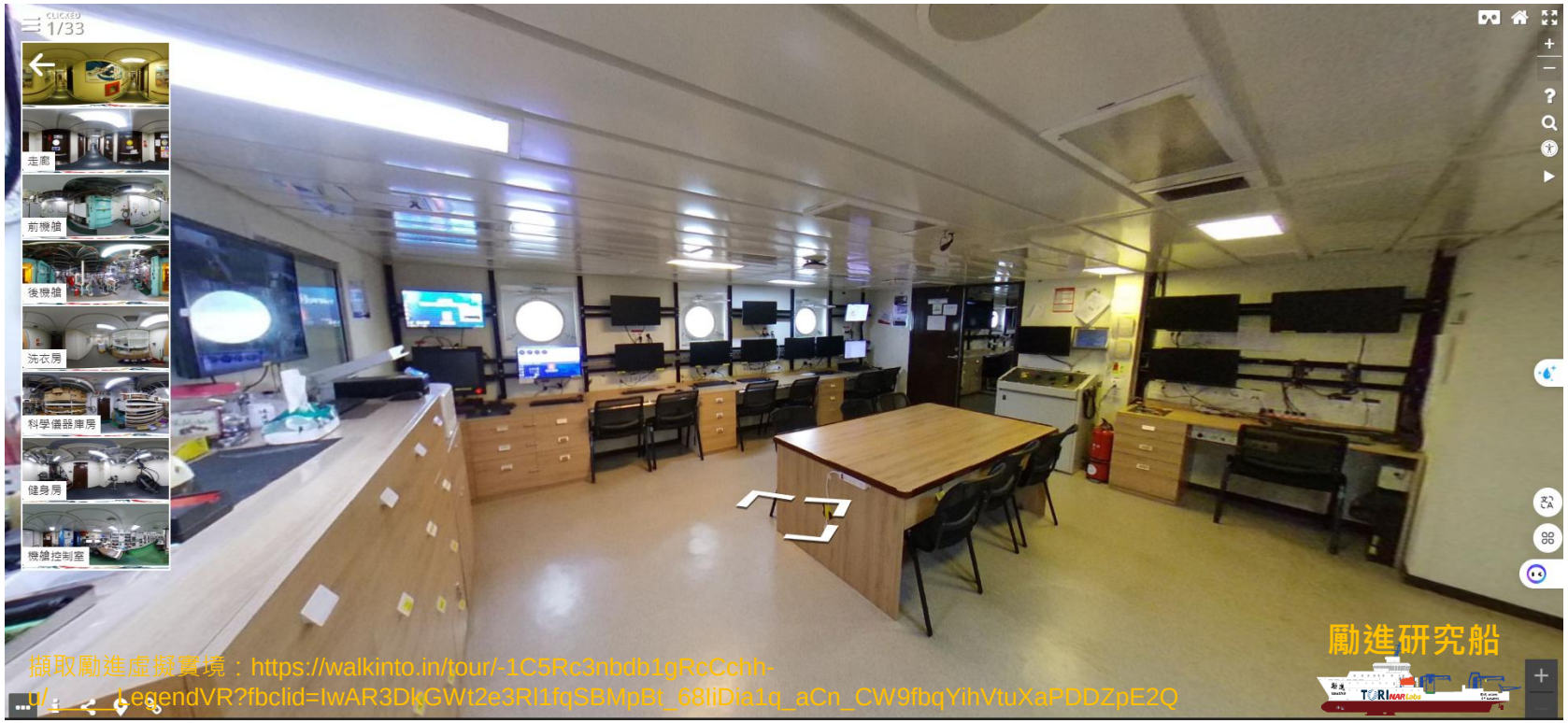
權限存取控制

Identify and Access Management





套用密碼原則(配合船期)



端點防護
ENDPOINT

公務Business

值得信賴的端點設備

資訊設備

TORI

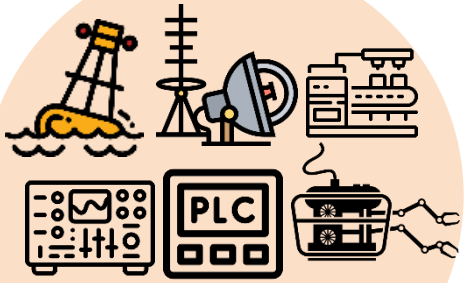
個人Personal

個人設備

BYOD

特殊

IoT設備

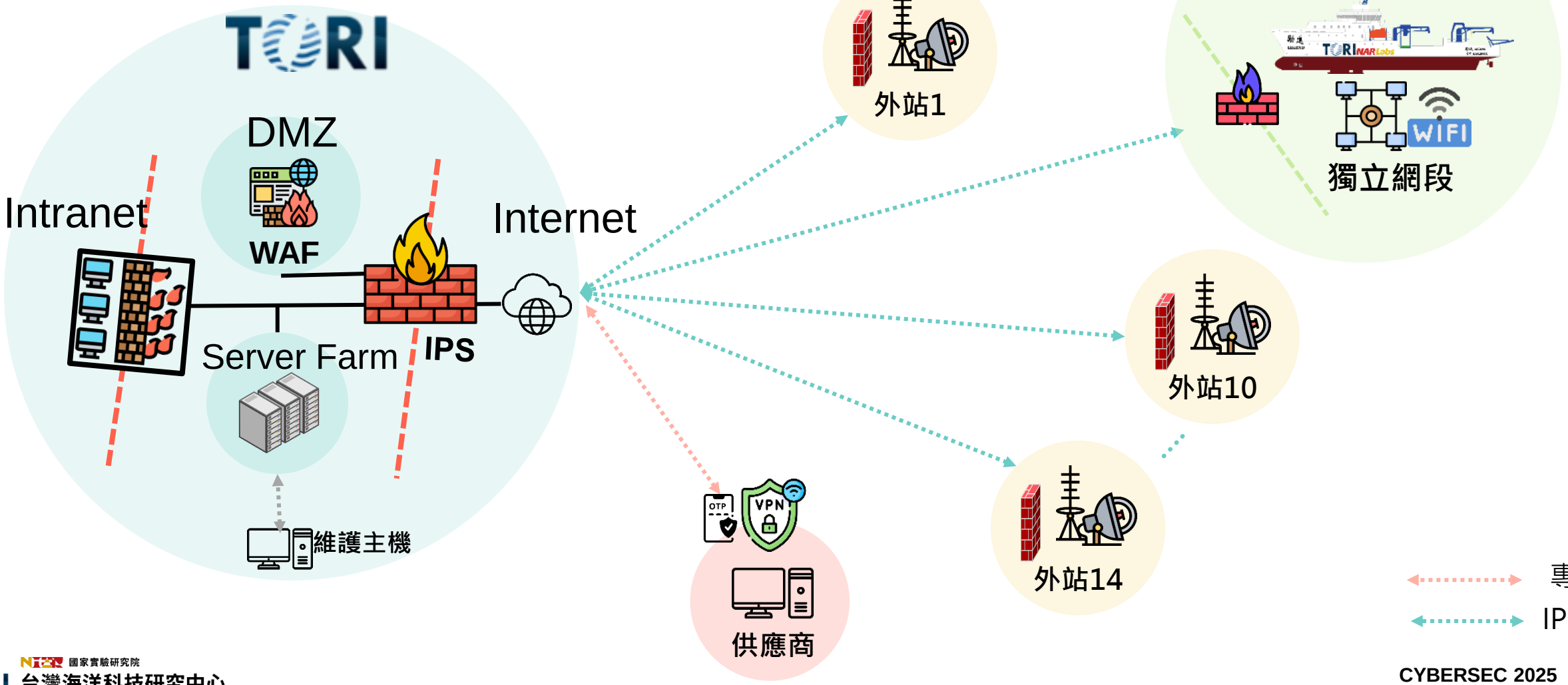


OT/CT設備

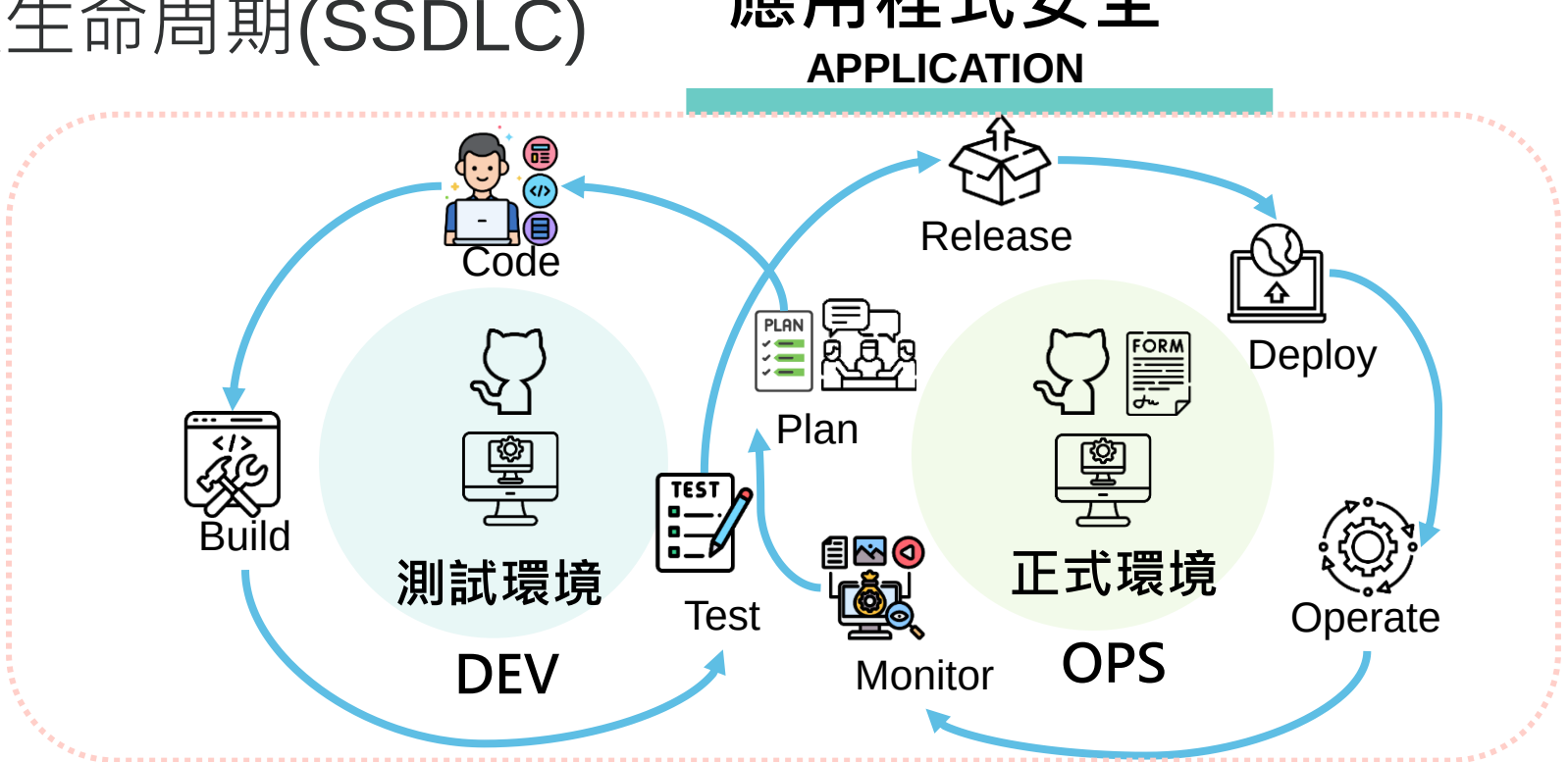
勵進研究船

軟體 Software
作業系統更新
漏洞修補
軟體/韌體更新
防毒
端點防護(EDR)
資產管理軟體

網路安全
NETWORK



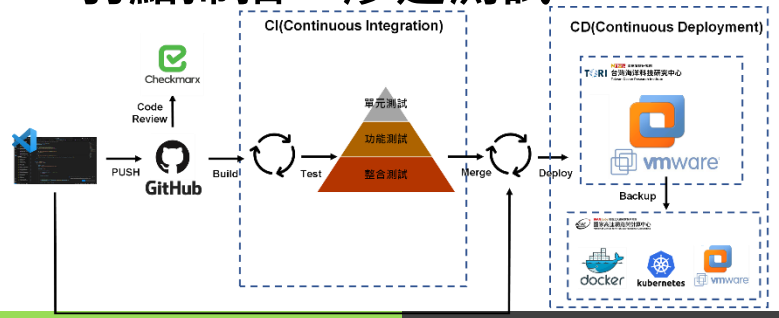
系統發展生命周期(SSDLC)



+

SEC (Secure)

- 系統防護需求分級(高、中、低)
- 進行安全性與隱私風險評鑑
- 導入軟體開發生命週期(SDLC)
- 使用信任開源(避免Log4j)
- OWASP TOP 10
- **源碼檢測**
- 持續性整合/部署(**CI/CD**)機制
- **弱點掃描、滲透測試**



資料安全
DATA

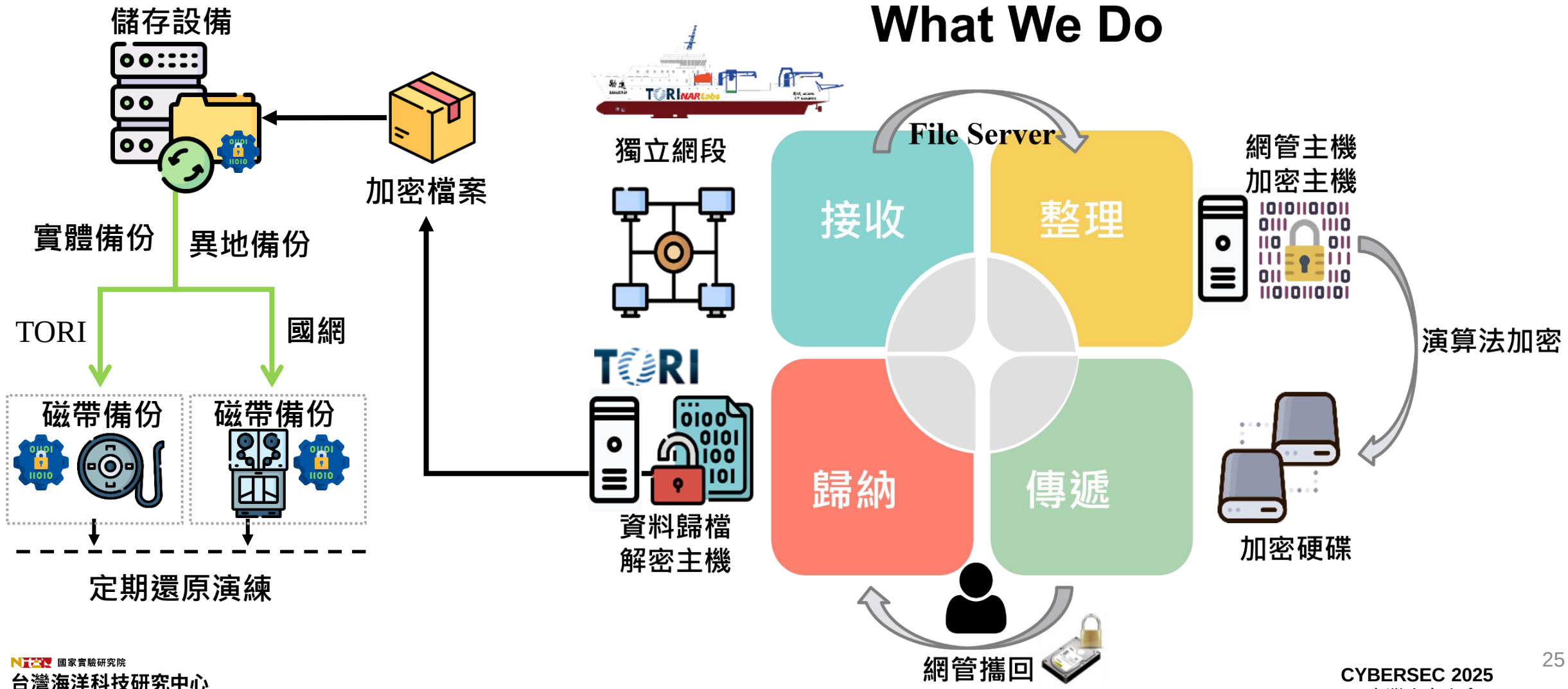
- 資料存取權限控管
- 備份、備援
  「**3-2-1 備份原則**」
- 定期執行資料備份還原測試

- 資料盤點
- 資料分類、分級管理
- 建立目錄、存放位置
- 定期盤點核心機敏資料

- 「資通安全管理法」
- 「國家機密保護法
- 「個人資料保護法」
- 「國家科學及技術委員會個人資料保護管理要點」
- 「國研院業務機密保護要點」

- ISO 27001:2022 控制措施
  8.12 **資料外洩防護**（DLP, Data Leakage Prevention）
  針對敏感資訊的傳輸

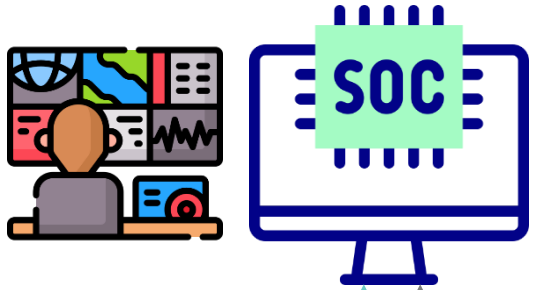
資料安全
DATA

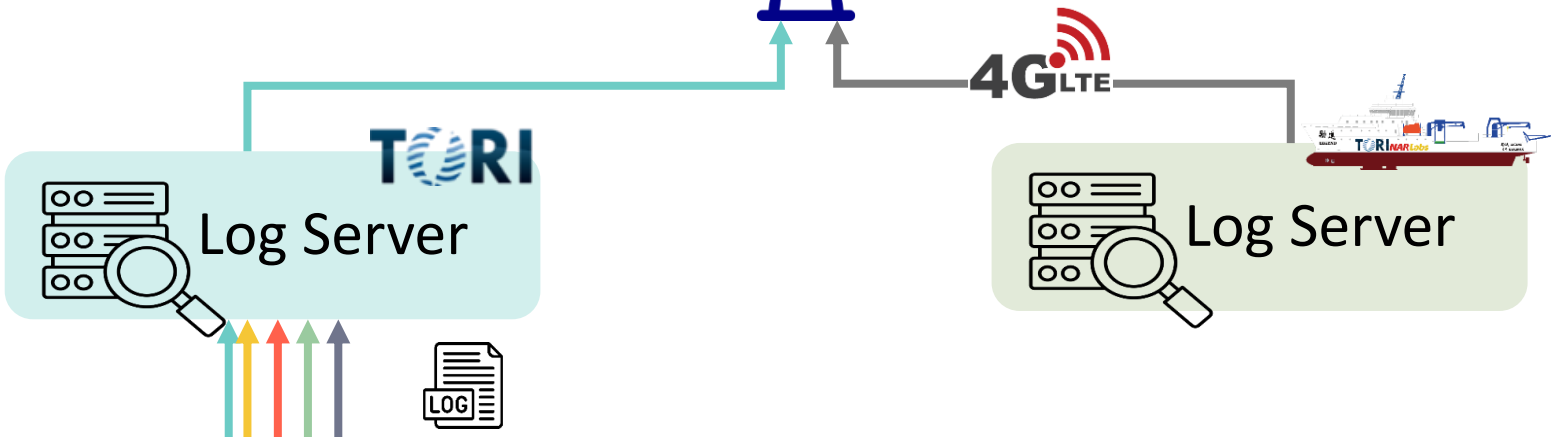

What We Do
儲存設備
加密檔案
實體備份
異地備份
TORI
國網
磁帶備份
磁帶備份
定期還原演練
獨立網段
TORI
資料歸檔
解密主機
File Server
接收
整理
歸納
傳遞
網管主機
加密主機
演算法加密
加密硬碟
網管攜回

SOC監控

Security Operation Center

7*24 小時不間斷監控





- 有限頻寬符合資安法規需求
  - **離岸不監控**、**靠岸監控**，若有異常立即告警。
  - **靠岸回傳**離岸期間收集之日誌給SOC監控中心分析。

權限存取控制 IAM

端點防護 ENDPOINT

網路安全 NETWORK

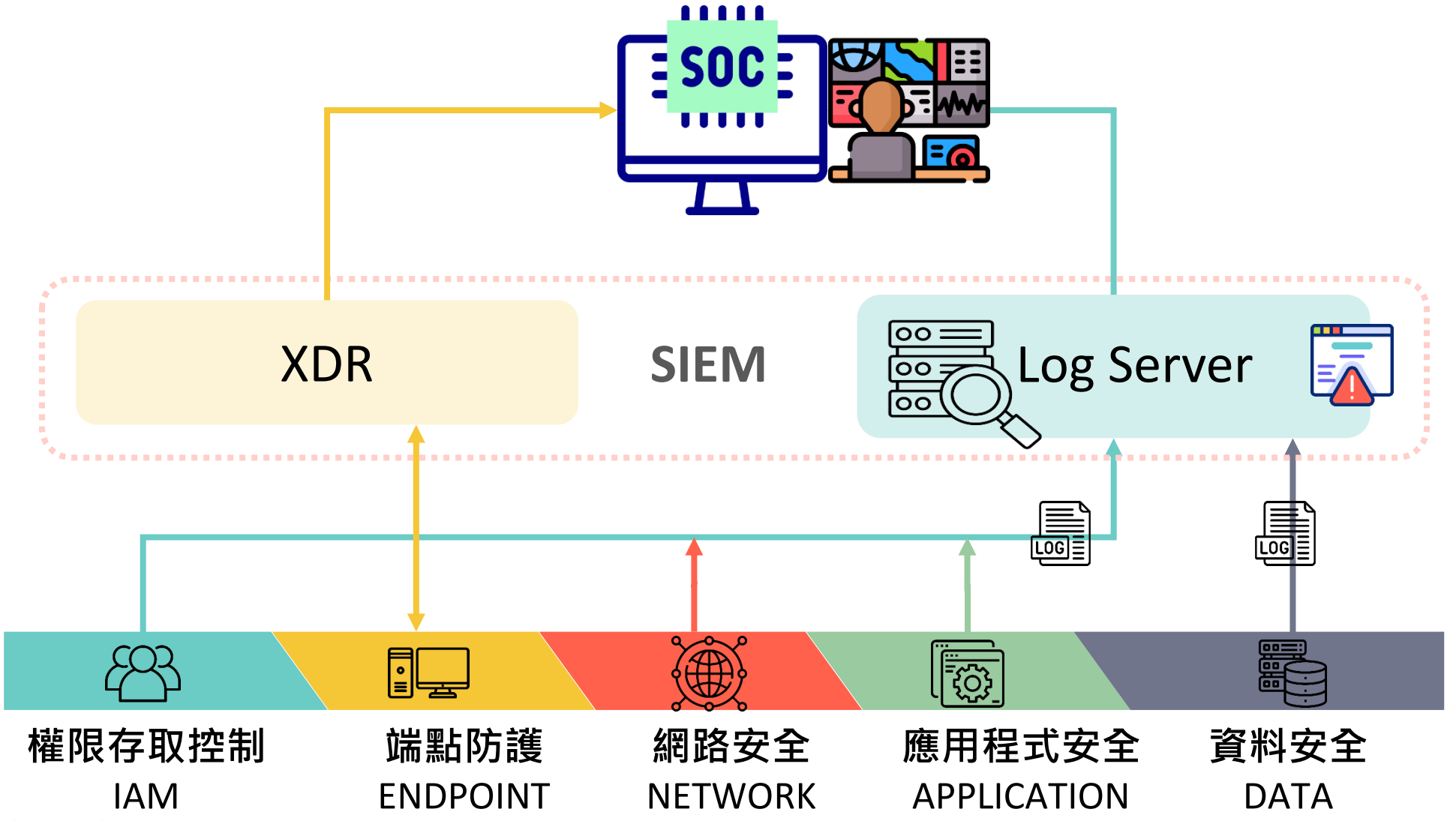
應用程式安全 APPLICATION

資料安全 DATA

Icon ref：https://www.flaticon.com/

資訊安全架構

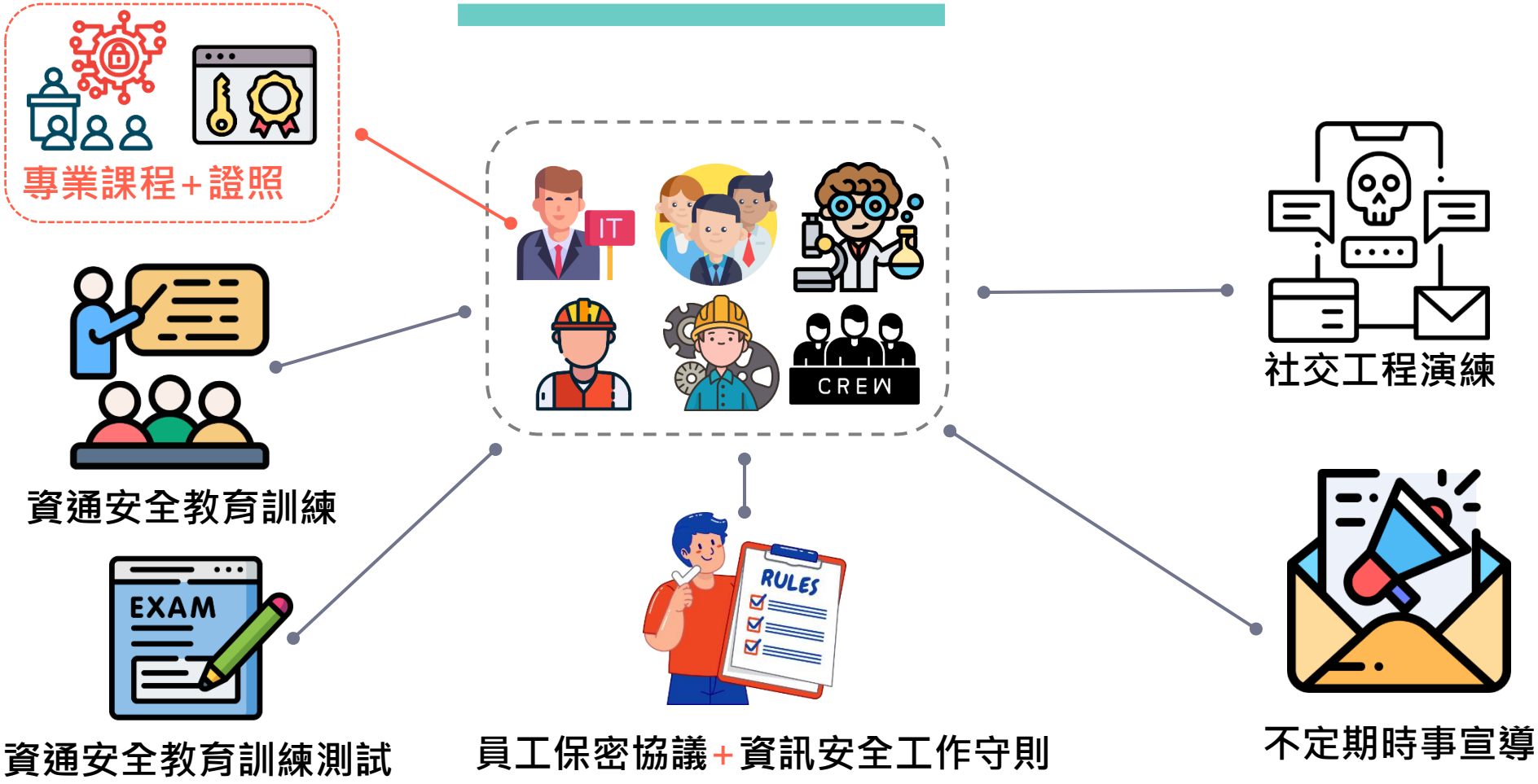
Security=Prevention+Detection+Response



Icon ref：https://www.flaticon.com/

資通安全教育訓練

Awareness and Training Courses



- 一般使用者及主管，每人每年至少接受之**一般資通安全教育訓練3小時**。
- 資通安全專責人員以外之**資訊人員每人每年至少12小時**。

Icon ref：https://www.flaticon.com/

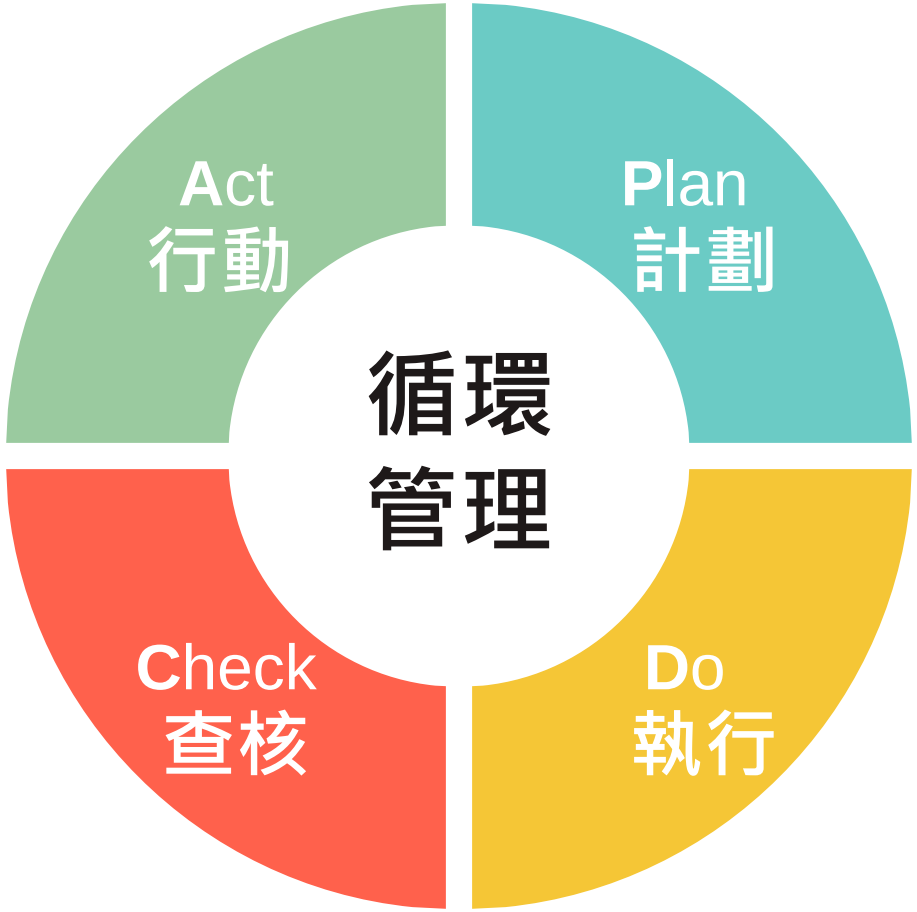
稽核作業

稽核循環管理
法規規範、資通安全法遵事項
國科會稽核項目
國際海事組織規章
資訊資安管理推動

稽核循環管理

Audits

- 矯正措施
- 持續改善



- 法規
- 上級單位要求及期望
- 資訊安全政策
- 資訊安全目標

- 內部稽核計畫
- 管理審查

- 風險評鑑與處理

Icon ref：https://www.flaticon.com/

法規規範

2019

2018/11/21頒布
2019/1/1 施行
資通安全責任等級分級辦法

2019

2019/2/23 施行
科技部所管**特定非公務機關**資通安全管理作業辦法

2022

2022/7/27
科技部改制為**國家科學及技術委員會**
2022/8/27
數位發展部成立

2023

2023/5/31修訂
個人資料保護法
生效日期：未定
施行日期，由行政院定之。
2023/10/23
人工智慧基本法草案

2019

2018/6/6頒布
2019/1/1 施行
資通安全管理法
(簡稱：資安法)

資安法納管對象包含公務機關及**特定非公務機關**。
特定非公務機關：指關鍵基礎設施提供者、 公營事業及**政府捐助之財團法人**。 相關定義可參考資安法第 3 條第 5 至 9 款條文。

2021

2019名稱調整為
「政府機關（構）資通安全責任等級分級作業規定」
2021/08/23修正

2022

2022/12/1修訂
國家科學及技術委員會所管**特定非公務機關**資通安全管理作業辦法

2024

2024/7/15修訂
人工智慧基本法草案總說明及條文
施行日期，由行政院定之。

資通安全法遵事項

制度面向	辦理項目	辦理內容
管理面	資通系統分級及防護基準	完成**資通系統分級**，並完成防護基準；每年至少檢視一次妥適性。
	資訊安全管理系統之導入及**通過公正第三方之驗證**	全部核心資通系統導入資訊安全管理系統，並於三年內完成第三方驗證；並持續維持其驗證有效性。
	業務持續運作演練	全部核心資通系統辦理業務持續運作演練
	辦理內部資通安全稽核*	
	資通安全專責人員	

*註：國研院現有稽核含**院級稽核、內控稽核及中心內部稽核**。

資通安全責任等級分級辦法

資通安全法遵事項

制度面向	辦理項目	辦理項目細項	辦理內容
技術面	安全性檢測	**弱點掃描**	全部核心資通系統辦理弱點掃描
		滲透測試	全部核心資通系統辦理滲透測試
	資通安全健診		網路架構檢視、網路惡意活動檢視、使用者端電腦惡意活動檢視、伺服器主機惡意活動檢視、目錄伺服器設定及防火牆連線設定檢視
	資通安全威脅偵測管理機制		完成**威脅偵測機制建置**，並持續維運
	資通安全防護 (啟用，並持續使用及適時進行軟、硬體之必要更新或升級)		防毒軟體、網路防火牆、具有郵件伺服器者，應備電子郵件過濾機制
			IDS/IPS、具有對外服務之核心資通系統者，應備應用程式防火牆(**WAF**)
			APT攻擊防禦

資通安全責任等級分級辦法

資通安全法遵事項

制度面向	辦理項目	辦理內容
認知與訓練	資通安全教育訓練	資通安全專責人員（資通安全專業課程訓練或資通安全職能訓練）
		資通安全專責人員以外之資訊人員（資通安全專業課程訓練或資通安全職能訓練）
		一般使用者及主管，每人每年至少接受之一般資通安全教育訓練
	資通安全專業證照及職能訓練證書	初次受核定或等級變更後之一年內，資通安全專職(責)人員總計應持有之資通安全專業證照 ，並持續維持證照之有效性

資通安全責任等級分級辦法

國科會稽核項目

數位發展部資通安全署
Administration for Cyber Security, moda

實地稽核，由**行政院國家資通安全會報組成稽核小組**，至受稽機關進行實地訪視及審查，實地稽核分策略面、管理面及技術面等3個構面，共9個稽核項目。

構面	稽核項目
策略面	一、核心業務及其重要性
	二、資通安全政策及推動組織
	三、專責人力及經費配置
管理面	四、資訊及資通系統盤點及風險評估
	五、資通系統或服務委外辦理之管理措施
	六、資通安全維護計畫與實施情形之持續精進及績效管理機制
技術面	七、資通安全防護及控制措施
	八、資通系統發展及維護安全
	九、資通安全事件通報應變及情資評估因應

https://moda.gov.tw/ACS/operations/drill-and-audit/652

國際海事組織規章

GUIDELINES ON MARITIME CYBER RISK MANAGEMENT

國際海事組織(International Maritime Organization；IMO)

INTERNATIONAL MARITIME ORGANIZATION

E

4 ALBERT EMBANKMENT
LONDON SE1 7SR
Telephone: +44 (0)20 7735 7611 Fax: +44 (0)20 7587 3210

2022

MSC-FAL.1/Circ.3/Rev.2
7 June 2022

GUIDELINES ON MARITIME CYBER RISK MANAGEMENT

1 The Facilitation Committee, at its forty-first session (4 to 7 April 2017), and the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), having considered the urgent need to raise awareness on cyber risk threats and vulnerabilities, approved the *Guidelines on maritime cyber risk management*, as set out in the annex.

2 The Guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyberthreats and vulnerabilities. The Guidelines also include functional elements that support effective cyber risk management.

3 The Maritime Safety Committee, at its 104th session (4 to 8 October 2021), and the Facilitation Committee, at its forty-sixth session (9 to 13 May 2022), approved an update to the additional guidance and standards included in paragraph 4.2 of the Guidelines.

4 Member Governments are invited to bring the contents of this circular to the attention of all stakeholders concerned.

5 This circular and any revisions supersede the interim guidelines contained in MSC.1/Circ.1526.

3.6 These functional elements encompass the activities and desired outcomes of effective cyber risk management across critical systems affecting maritime operations and information exchange, and constitute an ongoing process with effective feedback mechanisms.

3.7 Effective cyber risk management should ensure an appropriate level of awareness of cyber risks at all levels of an organization. The level of awareness and preparedness should be appropriate to roles and responsibilities in the cyber risk management system.

4 BEST PRACTICES FOR IMPLEMENTATION OF CYBER RISK MANAGEMENT

4.1 The approach to cyber risk management described herein provides a foundation for better understanding and managing cyber risks, thus enabling a risk management approach to address cyberthreats and vulnerabilities. For detailed guidance on cyber risk management, users of these Guidelines should also refer to Member Governments' and Flag Administrations' requirements, as well as relevant international and industry standards and best practices.

4.2 Additional guidance and standards may include, but are not limited to:*

.1 The Guidelines on Cyber Security Onboard Ships produced and supported by ICS, IUMI, BIMCO, OCIMF, INTERTANKO, INTERCARGO, InterManager, WSC and SYBAss.

.2 Consolidated IACS *Recommendation on cyber resilience* (Rec 166).

.3 ISO/IEC 27001 standard on Information technology – Security techniques – Information security management systems – Requirements. Published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

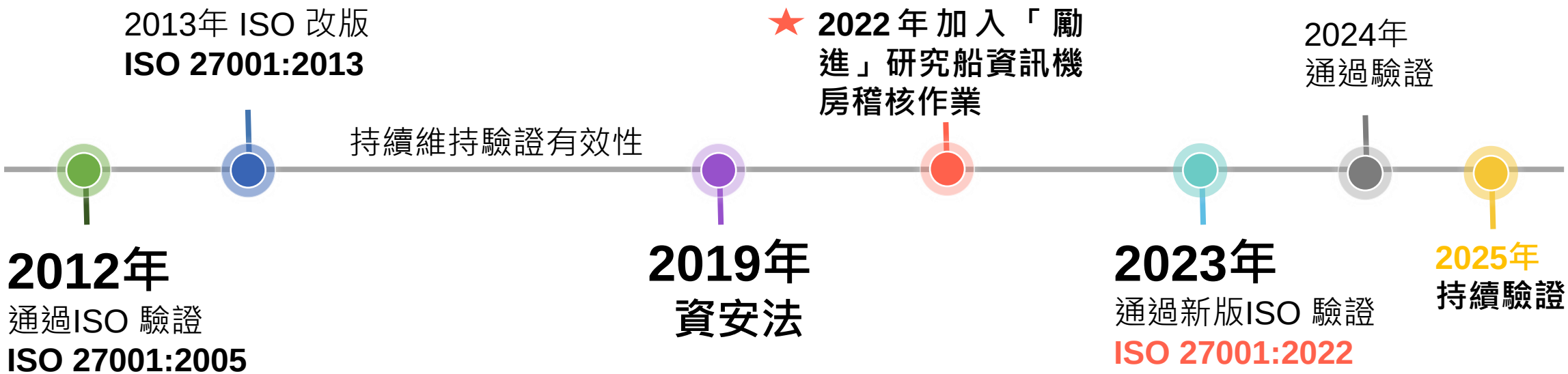
.4 United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework).

ISO/IEC 27001 資訊安全管理標準

IMO has issued MSC-FAL.1-Circ.3-Rev.2 Guidelines on maritime cyber risk management.

資訊資安管理推動

- 根據國際標準之**資訊安全管理系統(ISMS)**，建立本中心資訊安全管理機制，以保護本中心資訊資產之機密性、完整性與可用性，進而提供高品質之服務。
- 本中心於 2012 年取得 ISO27001 資訊安全認證，在相關控制措施的規範下，建立起資訊安全標準的通用防護基準，並強化資訊安全的管理，以增進組織內部運作的資通安全防護。



稽核
Audits

2012

ISO 驗證/實施範圍

全機關資安法實施範圍

2019

ISO 驗證/實施範圍

ISO/IEC 27001 驗證/實施範圍

全機關資安法實施範圍

ISO/IEC 27001 實施範圍

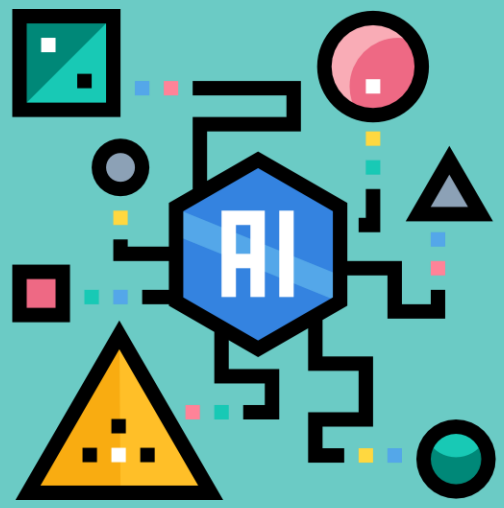
2022

ISO 驗證範圍

- 內部資通安全稽核含**院級稽核、內控稽核及中心內部稽核。**

- **公正第三方之驗證**
- **國科會實體稽核**
- 其他(**審計部稽核、會計師稽核**)

Icon ref：https://www.flaticon.com/



未來挑戰與展望

強化防禦
未來展望與潛在風險

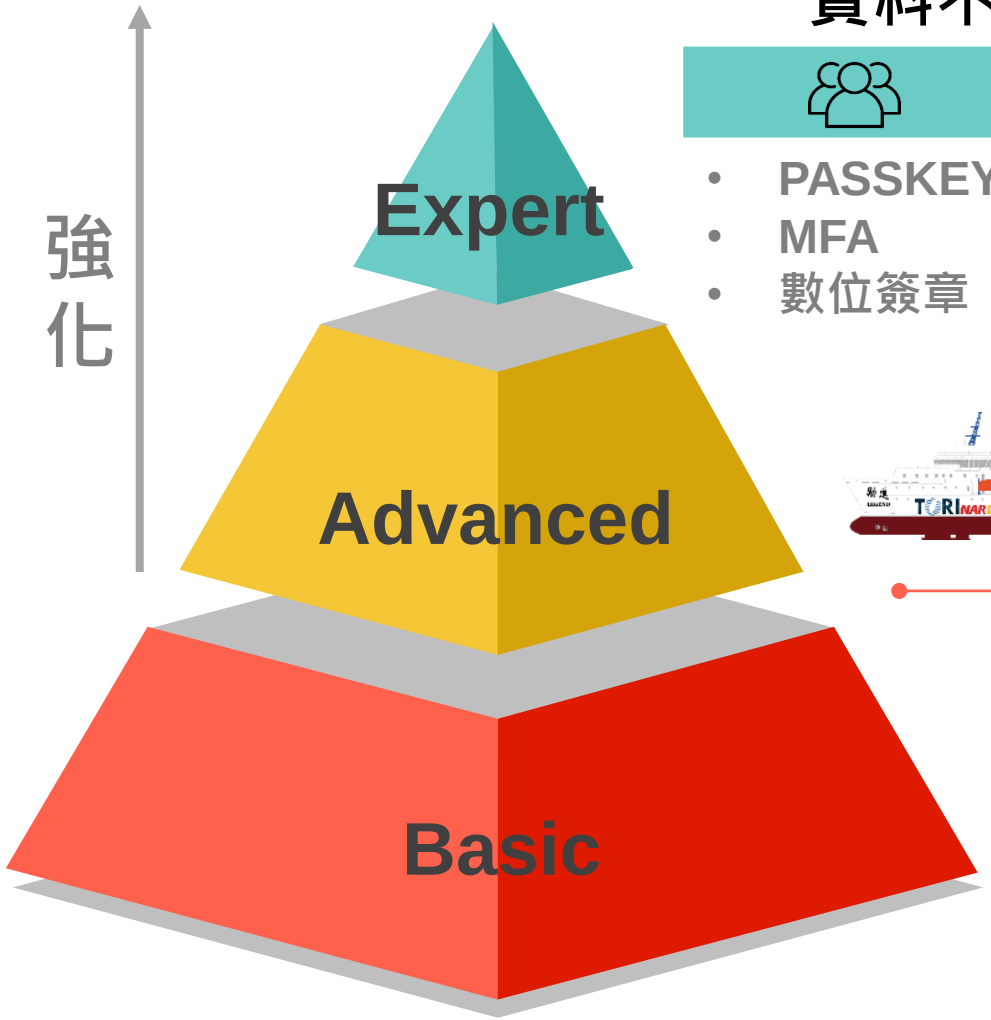
海事領域資訊安全挑戰
勵進研究船資訊安全挑戰

強化防禦

Strengthening prevention and detection

資料不外洩 + 資安事件不影響營運

強化



• PASSKEY • MFA • 數位簽章	• OT、IT、CT • 全面導入EDR • ISA/IEC 62443	• APT • DLP	• 資產管理 • CA	• 端點DLP • 資料加密 • ISO/IEC 27701之認證

海事資通風險+研究船資訊安全挑戰

Baseline

70分 滿足法規

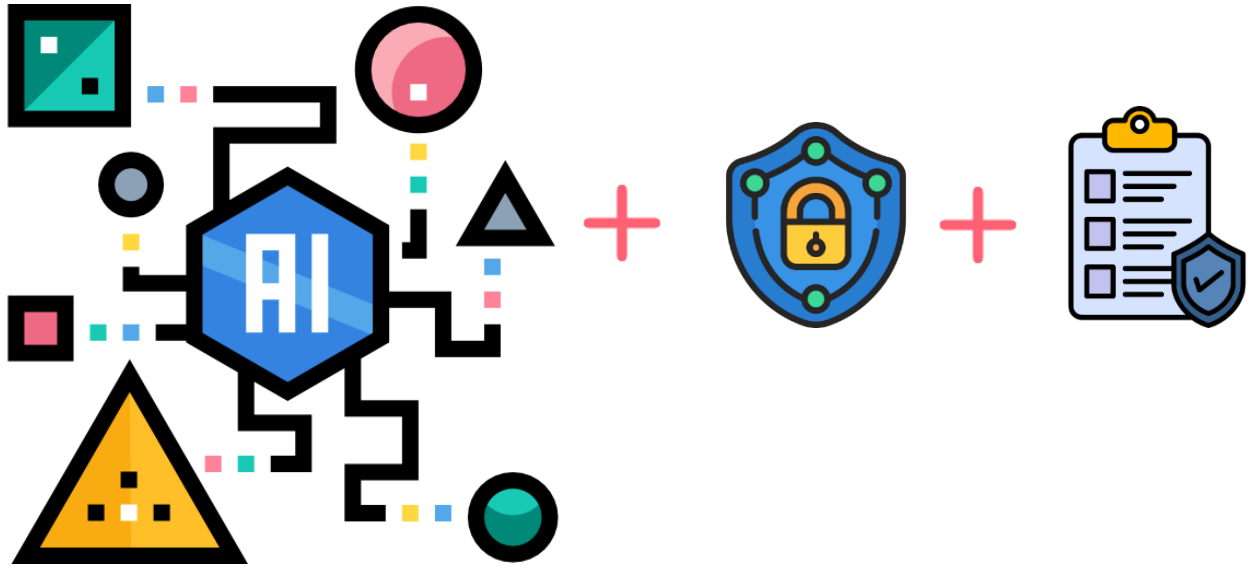
資安法 +個資法 +ISO 27001

Awareness

Icon ref：https://www.flaticon.com/

未來展望與潛在風險

Future and Risk



- 人工智慧基本法草案總說明及條文
- 數位發展部公部門人工智慧應用參考手冊草案

實體➔私有雲

- ISO/IEC 27017、 ISO/IEC 27018 雲端服務安全管理
- ISO/IEC 42001:2023人工智慧管理系統

生成式人工智慧風險

人工幻覺 Hallucination

影子AI Shadow AI

釣魚 Phishing

Icon ref：https://www.flaticon.com/

海事領域資訊安全挑戰

Cybersecurity Challenges in Maritime Operations

缺乏對電腦和網路的存取控制

攻擊者竊取敏感資料、安裝惡意軟體，甚至控制船舶系統。

過時/未修補的軟體

過時的作業系統

船舶過時的作業系統、軟體未安裝最新的安全性修補程式。

網路未隔離

缺乏入侵偵測

低品質網路硬體

船舶網路未劃分不同的網段，惡意軟體更容易在整個網路中傳播。沒有任何系統來偵測攻擊。

源碼檢測

弱點掃描

滲透測試

船舶使用應用系統缺乏DevSecOps概念

CREW

缺乏網路安全和安全政策

沒有適宜政策來指導員工如何安全地使用電腦和網路。

https://www.slideshare.net/valentinbanaco/maritime-cyber-security-education

勵進研究船資訊安全挑戰

Cybersecurity Challenges in Maritime Operations on R/V *LEGEND*

CT IT OT

控制與導航 Control & Navigation

雷達 Radar

電子海圖顯示與信息系統 ECDIS

全球海上遇險及安全系統 GMDSS

應差分定位系統/動態定位系統DGPS / DP System

自動識別系統 AIS

測深儀/船速器Echo Sounder / Speed Log

電羅經 Gyro Compass

急指位無線電示標/雷達詢答機 EPIRB / SART

氣象傳真系統 Weather Facsimile

航行警告電傳 NAVTEX

科儀設備 Scientific Equipment

機械及動力裝置 MACHINERY & Propulsion

通訊系統 Communication

中/高頻無線電 MF/HF Radiotelephone

超高頻無線電 VHF Radiotelephone

國際海事衛星通訊 INMARSAT-C / SSAS

網路衛星通訊系統 VSAT / INMARSAT FBB

勵進研究船資訊安全挑戰

Cybersecurity Challenges in Maritime Operations on R/V *LEGEND*

雷達

工業控制系統 (ICS)

自動辨識系統(AIS)

全球海上遇險系統 (GMDSS)

全球導航衛星系統與全球定位系統

電子海圖顯示和資訊系統（ECDIS）

訊號干擾、假訊息分享、未加密、欺騙攻擊、惡意軟體、DoS/DDoS 攻擊、封包修改、缺乏加密、遠端存取策略薄弱、缺乏SOS培訓

RISK

竊取有價值的數據、 GPS 訊號虛假資訊、擾亂船舶運作、失去通訊、電腦和作業系統受損

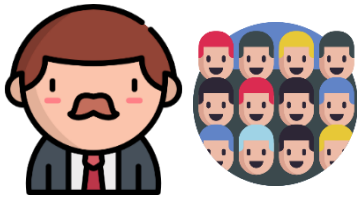
Never-ending studying

+0

冰山下

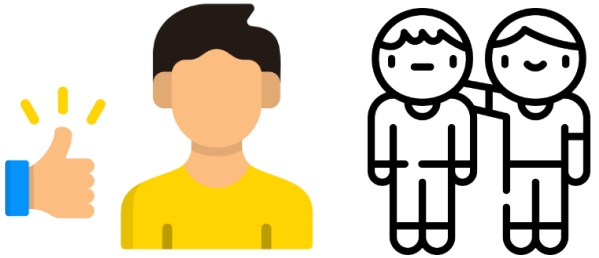
專業的工作事項

冰山一角
資訊服務



期許

投資專業
提升技能



鼓勵與關懷

謝謝聆聽

TEAM
CYBERSECURITY