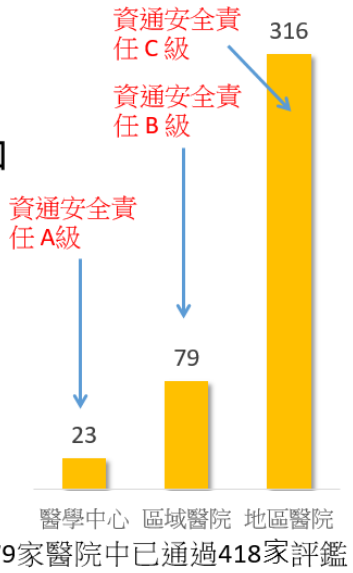
附件 ：

客戶端(醫院)面臨的合規壓力

法規合規評估階段

- 衛福部以資安法、醫院評鑑與醫材上市合規審查三支箭強化醫療體系落實資安作為(個資隱私、網路安全)
  - 以通過醫院醫院評鑑之479 家醫院為母體，皆已落入資安法ABC級管理範圍
  - 其中 64家CI指定醫院(公立醫院)，需逐步加入衛福部HISAC資安聯防機制

衛生福利部政策作為	強度要求	基層診所(約2萬餘)	非CI醫院(約420多)	CI醫院(46家)
訂定各級醫療院所資訊安全防護基準參考原則	普	V	V	V
以醫院評鑑基準引導提高資安防護水準(評鑑辦法)	中		V	V
資安聯防機制強化關鍵基礎設施防護能力(資安法)	高			V



479家醫院中已通過418家評鑑

資料來源：衛生福利部關鍵基礎設施資安工作推動專案辦公室(2020)，資安所整理

醫材業者視醫院要求配合資安需求確認

企業需求確認階段

	醫院資安要求	A 級	B 級	C級
流程安全	檢視系統分級	每年		
	ISO 27001	需 (第三方公正驗證)		
	資安專職人員	4 名	2 名	1名
	內部資安稽核	每年 2 次	每年 1 次	每兩年 1 次
	業務持續運作演練	每年 1 次	每兩年 1 次	每兩年 1 次
	資安治理成熟度	每年1次		每兩年 1 次
產品安全	弱點掃描	每年 2 次	每年 1 次	每兩年 1 次
	滲透測試	每年 1 次	每兩年 1 次	每兩年 1 次
	資通安全健診	每年 1 次	每兩年 1 次	每兩年 1 次
	威脅偵測、端點偵測、組態管理	建立並維運		X
	資通安全防護、弱點通報	建立並維運		
人員合規	認知訓練	資安專職人員每年 12 小時專職訓練 非專職資訊人員每兩年3小時專職訓練 一般人員每年3小時通識訓練		
	專責人員資安證書	4人員各有一張證書與證照	2人員各有一張證書與證照	1人員有一張證照

資料來源：全國法規資料庫附件