

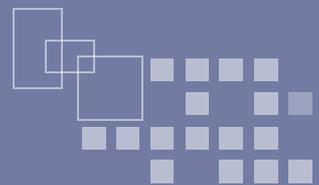


# 政府機關（構）資通安全責任等級分級 調整情形

行政院資通安全辦公室

吳啟文 副主任

中華民國104年7月14日

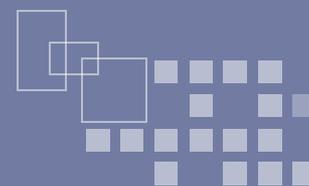


- ❖ **修訂及推動歷程**
- ❖ **本次修訂重點說明**
- ❖ **資安責任等級分級執行作業及彙整結果**
- ❖ **資安責任等級應辦事項管理分工及推動處理**

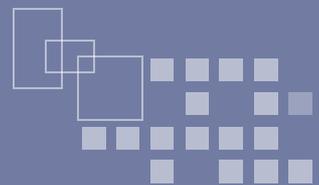


- ❖ **93年**：訂定「**政府機關(構)資訊安全責任等級分級作業施行計畫**」，針對重要政府機關(構)**建立資通安全整體防護體系**
- ❖ **94年**：增訂各政府機關(構)依資安責任等級**應執行工作事項**
- ❖ **98年**：精進各政府機關(構)依資安責任等級**應辦事項**
- ❖ **103年**：因應資通訊科技發展及資通安全威脅趨勢，進行資安責任等級檢討與修訂
  - 9月2日召開研修規劃討論會議
  - 12月1日辦理修訂說明會，與相關機關進行意見溝通與說明
- ❖ **104年**：1月20日核定修正之「**政府機關(構)資通安全責任等級分級作業規定**」分行各政府機關

# 推動歷程

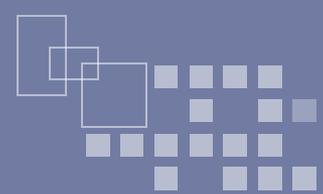


時間	說明
104年1月	<ol style="list-style-type: none"><li>1月20日分行修正之「政府機關(構)資通安全責任等級分級作業規定」</li><li>1月22日提報資安會報第27次委員會議，請主管機關儘速檢視調整各該機關及所屬機關(構)資安責任等級分級於3月底前彙送資安辦</li></ol>
104年2月	遴選2個主管機關(交通部、桃園市政府)試行資安責任等級分級作業，試行結果供其他主管機關參考
104年3月	<ol style="list-style-type: none"><li>3月上旬辦理北、中、南、東4區6場次說明會</li><li>少數主管機關彙送資安責任等級資料</li></ol>
104年4月	<ol style="list-style-type: none"><li>逾半數主管機關彙送資安責任等級資料</li></ol>
104年5月	<ol style="list-style-type: none"><li>5月18日提報行政院暨國安會資安辦104年5月份會議</li></ol>
104年6月	<ol style="list-style-type: none"><li>6月4日核定(備)政府機關(構)資安責任等級</li><li>各主管機關需於6月30日前彙送應辦事項規劃情形</li></ol>



- ❖ 修訂及推動歷程
- ❖ **本次修訂重點說明**
- ❖ 資安責任等級分級執行作業及彙整結果
- ❖ 資安責任等級應辦事項管理分工及推動處理

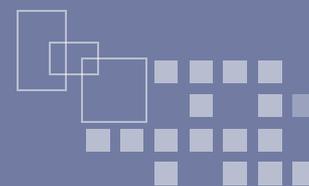
# 本次修訂重點說明(1/2)



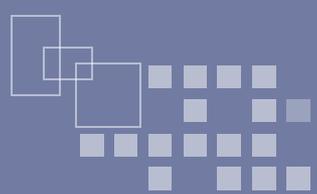
修訂說明 修訂項目	修訂重點說明
調整名稱	依行政規則名稱訂定原則，修訂為「 <b>政府機關（構）資通安全責任等級分級作業規定</b> 」
擴充適用對象	1.政府機關（構） 2.增加行政法人，及由政府委託民間興建營運後轉移(Build-Operate-Transfer, BOT)之 <b>關鍵資訊基礎設施營運單位</b> ，如遠通電收股份有限公司、台灣高速鐵路股份有限公司、高雄捷運股份有限公司等
簡化責任等級	因應資安威脅情勢， <b>簡化層級以加強資安防護</b> ，調整為 <b>A、B、C 3個等級</b>

備註：參照行政院國土辦公室於103年12月訂定之「國家關鍵基礎設施安全防護指導綱要」，關鍵資訊基礎設施(Critical Information Infrastructure, CII)係指涉及核心業務運作，為支持關鍵基礎設施持續營運所需之重要資訊系統或調度、控制系統(Supervisory Control and Data Acquisition, SCADA)，亦屬關鍵基礎設施之重要元件，應配合對應之關鍵基礎設施統一納管。

# 本次修訂重點說明(2/2)

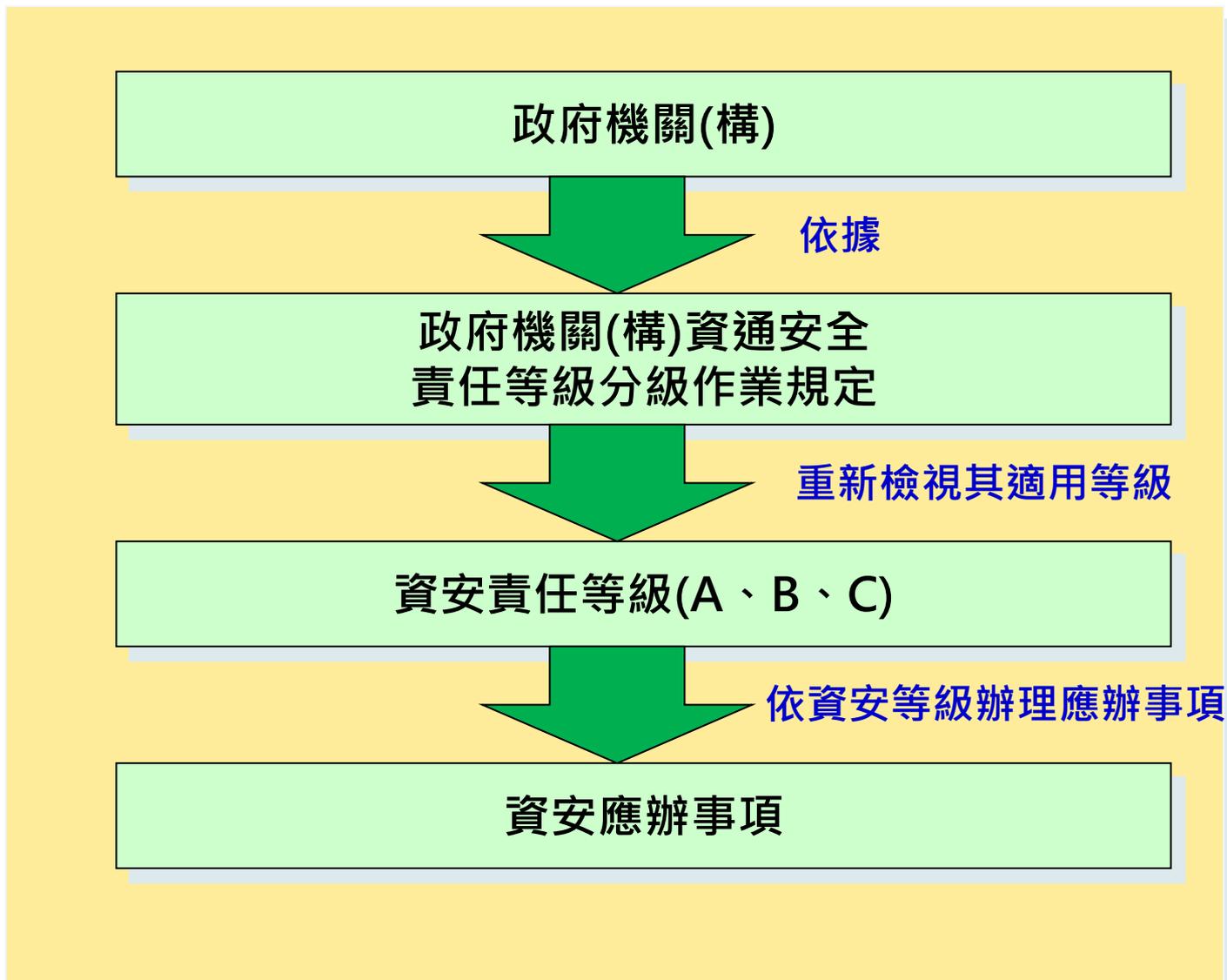
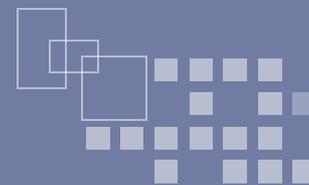


修訂說明 修訂項目	修訂重點說明
明定CII 責任等級	凡涉及 <b>關鍵資訊基礎設施(Critical Information Infrastructure, CII)</b> 之營運機關(單位)，其資安責任等級列為 <b>A級</b>
核定各機關責任 等級	<ol style="list-style-type: none"> <li>1. 行政院所屬二級機關、各直轄市政府及縣(市)政府應檢視其所屬機關(構)(含行政法人)資安責任等級之分級及其妥適性，並<b>彙送行政院資安辦</b></li> <li>2. 經行政院資安辦複核後，提請資安會報核定資通安全責任等級</li> <li>3. 總統府、立法院、司法院、考試院、監察院所屬機關(構)之資安責任等級，<b>比照第1點規定辦理，並提請資安會報備查</b></li> </ol>
擴增應辦事項	<ol style="list-style-type: none"> <li>1. 參考網路攻防演練及政府機關(構)資安健診、稽核結果，進行資安責任等級應辦事項檢討</li> <li>2. 分<b>政策、管理、技術及認知與訓練</b>等<b>4個面向、10個類別</b>強化應辦事項內容</li> </ol>

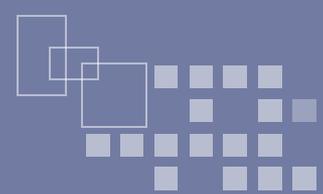


- ❖ 修訂及推動歷程
- ❖ 本次修訂重點說明
- ❖ 資安責任等級分級執行作業及彙整結果
- ❖ 資安責任等級應辦事項管理分工及推動處理

# 資安責任等級分級執行作業



# 資安責任等級分級準則(1/4)



## 政府機關層級

涉及外交、國防、國土安全、財政、經濟、警政等重要業務

涉及能源、水資源、通訊傳播、交通、金融、緊急救援與醫院、高科技園區等關鍵資訊基礎設施業務或營運

保有全國、區域性或地區性個人資料檔案

A級

B級

C級

資安責任等級

# 資安責任等級分級準則(2/4)



## 政府機關部分

### 政府機關層級

A級：總統府、五院及直轄市政府、五院所屬二級機關及相當二級機關之獨立機關  
B級：縣(市)政府

涉及外交、國防、國土安全、財政、經濟、警政業務

A級：凡涉及外交、國防、國土安全，及掌理全國財政、經濟、警政等重要業務之機關  
B級：凡涉及社會秩序及人民財產業務之機關

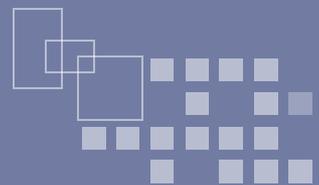
涉及關鍵資訊基礎設施業務或營運

A級：負責關鍵資訊基礎設施之營運機關

保有全國、區域性或地區性個人資料檔案

A級：保有全國性個人資料檔案之機關  
B級：保有區域性或地區性個人資料檔案之機關

# 政府機關資安責任等級區分



屬性 等級	政府機關屬性
<b>A級</b>	<ol style="list-style-type: none"> <li>1. 總統府、國安會、立法院、司法院、考試院、監察院、行政院及直轄市政府。</li> <li>2. 立法院、司法院、考試院、監察院及行政院等所屬二級機關、相當二級機關之獨立機關。但其業務或組織單純者，得報經其上級機關核准，調整為B級或C級</li> <li>3. 凡涉及外交、國防、國土安全，及掌理全國財政、經濟、警政等重要業務之機關，如外交部領事事務局、內政部警政署刑事警察局等</li> <li>4. 負責能源、水資源、通訊傳播、交通、金融、緊急救援、高科技園區等關鍵資訊基礎設施之營運機關，如交通部民用航空局飛航服務總臺、臺北市自來水事業處等</li> <li>5. 保有全國性個人資料檔案之機關，如勞動部勞工保險局、衛生福利部中央健康保險署等</li> </ol>
<b>B級</b>	<ol style="list-style-type: none"> <li>1. 縣（市）政府</li> <li>2. 凡涉及社會秩序及人民財產業務之機關，如地方政府警察局、地方政府地政事務所等</li> <li>3. 保有區域性或地區性個人資料檔案之機關，如財政部各區國稅局、地方政府戶政事務所等</li> </ol>
<b>C級</b>	其他政府機關及地方政府民意機關

# 資安責任等級分級準則(3/4)



## 學術機構部分

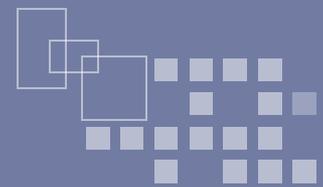
### 各級學校

- A級：凡涉及各相關機關委託研究具國家安全機密性或敏感性之學校
- B級：各大學
- C級：各學院、專科學校及各高中職（含）以下學校

### 學術研究機構 與 網路中心

- B級：臺灣學術網路各區域網路中心暨各直轄市、縣（市）教育網路中心
- C級：教育部所屬研究機構

# 學術機構資安責任等級區分



屬性 等級	學術機構屬性
A	凡涉及各相關機關委託研究具國家安全機密性或敏感性之學校。
B	<ol style="list-style-type: none"><li>1. 各大學。</li><li>2. 臺灣學術網路各區域網路中心暨各直轄市、縣（市）教育網路中心。</li></ol>
C	<ol style="list-style-type: none"><li>1. 各學院、專科學校及各高中職（含）以下學校。</li><li>2. 教育部所屬研究機構。</li></ol>

# 資安責任等級分級準則(4/4)



## 國(公)營事業、醫療機構及其他部分

涉及外交、國防、  
國土安全、財政、  
經濟、警政業務

B級：國（公）營事業涉及**全國或地方民生資源**  
等業務

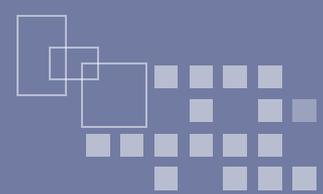
涉及**關鍵資訊基礎設施業務**或營運

A級：國（公）營事業與特許機構，處理涉及**能源、水資源、通訊傳播、交通、金融**等**關鍵資訊基礎設施業務者**；由政府委託民間興建營運後轉移(BOT)之**關鍵資訊基礎設施營運單位**；  
**醫學中心**  
B級：**區域醫院**  
C級：**地區醫院**

保有**全國、區域性或地區性個人資料檔案**

A級：保有**全國性個人資料檔案**之機構  
B級：保有**區域性或地區性個人資料檔案**之機構

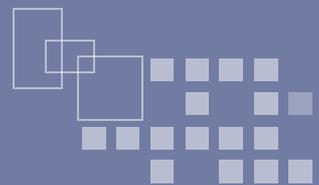
# 國(公)營事業、醫療機構及其他 資安責任等級區分



屬性 等級	國(公)營事業、醫療機構及其他單位屬性
A	<ol style="list-style-type: none"> <li>1. 國(公)營事業與特許機構，處理涉及能源、水資源、通訊傳播、交通、金融等關鍵資訊基礎設施業務者，如臺灣港務股份有限公司、臺灣證券交易所、台灣電力公司等。</li> <li>2. 由政府委託民間興建營運後轉移(BOT)之關鍵資訊基礎設施營運單位，如遠通電收股份有限公司、台灣高速鐵路股份有限公司、高雄捷運股份有限公司等。</li> <li>3. 醫學中心，如國立臺灣大學醫學院附設醫院、臺北榮民總醫院等。</li> <li>4. 保有全國性個人資料檔案之機構，如中華郵政股份有限公司等。</li> </ol>
B	<ol style="list-style-type: none"> <li>1. 國(公)營事業涉及全國或地方民生資源等業務，如台灣糖業股份有限公司等。</li> <li>2. 區域醫院，如臺北市立聯合醫院、衛生福利部桃園醫院、國立臺灣大學醫學院附設醫院雲林分院等。</li> <li>3. 保有區域性或地區性個人資料檔案之機構。</li> </ol>
C	<ol style="list-style-type: none"> <li>1. 其他國(公)營事業機構，如金門酒廠實業股份有限公司、福建省連江縣馬祖日報社等。</li> <li>2. 地區醫院，如臺北市立關渡醫院、國立成功大學醫學院附設醫院斗六分院、臺北榮民總醫院新竹分院等。</li> </ol>

備註：原為國(公)營已民營化之事業、公辦民營事業、民營公用事業及政府捐助之財團法人，得由其主管(監督)機關參照本規定，自行訂定資通安全責任等級，並依其訂定之應辦事項監督管理

# 資安責任等級分級彙整總表



等級	依原規定	依修正後規定			
		合計	政府機關	事業機構(單位)	學術機構
A級	57	127	83	25	19
B級	306	569	381	19	169
C級	6,434	6,591	2,573	94	3,924
合計	6,797	7,287	3,037	138	4,112

363

696

C+D

# 資安責任等級分級彙整結果 - 政府機關



機關	合計	A級	B級	C級
總統府+國安會	6	3	1	2
立法院	1	1	0	0
司法院及所屬	37	1	0	36
考試院及所屬	8	3	1	4
監察院及所屬	25	2	0	23
行政院及所屬	570	65	170	335
新北市及所屬	165	2	15	148
臺北市及所屬	144	2	12	130
桃園市及所屬	109	1	11	97
臺中市及所屬	200	1	16	183
臺南市及所屬	179	1	16	162
高雄市及所屬	222	1	20	201
臺灣省各縣(市)及所屬	1,294	0	110	1,184
福建省金門縣、連江縣及所屬	77	0	9	68
<b>合計</b>	<b>3,037</b>	<b>83</b>	<b>381</b>	<b>2,573</b>

# 資安責任等級分級彙整結果 - 事業機構

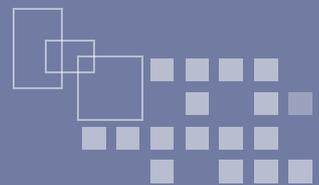


機關	合計	A級	B級	C級
總統府+國安會	0	0	0	0
立法院	0	0	0	0
司法院及所屬	0	0	0	0
考試院及所屬	0	0	0	0
監察院及所屬	0	0	0	0
行政院及所屬	116	21	18	77
新北市及所屬	0	0	0	0
臺北市及所屬	4	2	1	1
桃園市及所屬	1	0	0	1
臺中市及所屬	1	1	0	0
臺南市及所屬	0	0	0	0
高雄市及所屬	2	1	0	1
臺灣省各縣(市)及所屬	3	0	0	3
福建省金門縣、連江縣及所屬	11	0	0	11
合計	138	25	19	94

# 資安責任等級分級彙整結果 - 學術機構

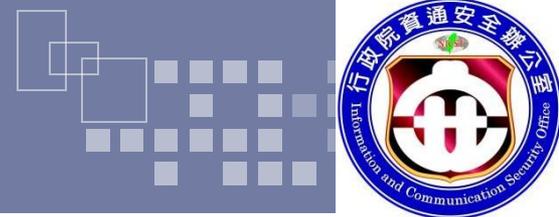


機關	合計	A級	B級	C級
公私立大專院校	161	0	126	35
公私立中等學校	1,241	0	0	1,241
公私立小學	2,644	0	0	2,644
公私立大學附設醫院	13	2	7	4
教育網路中心	35	0	35	0
試務機構	18	17	1	0
合計	4,112	19	169	3,924



- ❖ 修訂及推動歷程
- ❖ 本次修訂重點說明
- ❖ 資安責任等級分級執行作業及彙整結果
- ❖ 資安責任等級應辦事項管理分工及推動處理

# 資安責任等級應辦事項(1/3)



等級	面向 作業 名稱	政策面	管理面			
		資訊系統分級	ISMS推動作業	資安 專責人力	稽核方式	業務持續 運作演練
<b>A級</b>		<ul style="list-style-type: none"> <li>一、完成資訊系統分級(104年底前)</li> <li>二、完成資訊系統資安防護基準要求(105年底前)</li> </ul>	<ul style="list-style-type: none"> <li>一、全部核心資訊系統完成ISMS導入(105年底前)</li> <li>二、全部核心資訊系統通過第三方驗證(106年底前)</li> </ul>	指派資安專責人力2人	每年至少2次內稽	每年至少辦理1次核心資訊系統持續運作演練
<b>B級</b>		<ul style="list-style-type: none"> <li>一、完成資訊系統分級(104年底前)</li> <li>二、完成資訊系統資安防護基準要求(105年底前)</li> </ul>	<ul style="list-style-type: none"> <li>一、至少2項核心資訊系統完成ISMS導入(106年底前)</li> <li>二、至少2項核心資訊系統通過第三方驗證(107年底前)</li> </ul>	指派資安專責人力1人	每年至少1次內稽	每2年至少辦理1次核心資訊系統持續運作演練
<b>C級</b>		依各主管機關規定	自行成立推動小組規劃作業	依各主管機關規定	依各主管機關規定	依各主管機關規定

備註：增修項目：以紅色字體顯示

核心資訊系統：係指經資訊系統分級後，等級為「高」者

# 資安責任等級應辦事項(2/3)



等級	面向 作業 名稱	技術面		
		防護縱深	監控管理	安全性檢測
<b>A級</b>	<ul style="list-style-type: none"> <li>一、防毒、防火牆、郵件過濾裝置</li> <li>二、IDS/IPS、Web應用程式防火牆</li> <li>三、APT攻擊防禦</li> </ul>	SOC監控 (104年底前)	<ul style="list-style-type: none"> <li>一、每年至少辦理2次網站安全弱點檢測</li> <li>二、每年至少辦理1次系統滲透測試</li> <li>三、每年至少辦理1次資安健診</li> </ul>	
<b>B級</b>	<ul style="list-style-type: none"> <li>一、防毒、防火牆、郵件過濾裝置</li> <li>二、IDS/IPS</li> <li>三、Web應用程式防火牆(機關具有對外服務之核心資訊系統)</li> </ul>	SOC監控 (105年底前)	<ul style="list-style-type: none"> <li>一、每年至少辦理1次網站安全弱點檢測</li> <li>二、每2年至少辦理1次系統滲透測試</li> <li>三、每2年至少辦理1次資安健診</li> </ul>	
<b>C級</b>	<ul style="list-style-type: none"> <li>一、防毒</li> <li>二、防火牆</li> <li>三、郵件過濾裝置(機關具有郵件伺服器)</li> </ul>	依各主管機關規定	依各主管機關規定	

備註：增修項目：以紅色字體顯示

核心資訊系統：係指經資訊系統分級後，等級為「高」者

# 資安責任等級應辦事項(3/3)



等級	面向 作業 名稱	認知與訓練	
		資安教育訓練(一般主管、資訊人員/資安人員、 一般使用者)	專業證照
A級		<ul style="list-style-type: none"> <li>一、每年資安人員(資訊人員)至少2人次須接受12小時以上資安專業課程訓練或資安職能訓練</li> <li>二、每年一般使用者與主管至少須接受3小時資安宣導課程並通過課程評量</li> </ul>	每年維持至少2張國際資安專業證照與2張資安職能訓練證書之有效性
B級		<ul style="list-style-type: none"> <li>一、每年資安人員(資訊人員)至少1人次須接受12小時以上資安專業課程訓練或資安職能訓練</li> <li>二、每年一般使用者與主管至少須接受3小時資安宣導課程並通過課程評量</li> </ul>	每年維持至少1張國際資安專業證照與1張資安職能訓練證書之有效性
C級		<ul style="list-style-type: none"> <li>一、依各主管機關規定資安人員(資訊人員) 資安專業課程訓練或資安職能訓練要求</li> <li>二、每年一般使用者與主管至少須接受3小時資安宣導課程並通過課程評量</li> </ul>	依各主管機關規定

備註：增修項目：以紅色字體顯示

核心資訊系統：係指經資訊系統分級後，等級為「高」者

# 資安責任等級應辦事項管理分工(1/2)



機關	合計	A級	B級	C級
總統府+國安會	6	3	1	2
立法院	1	1	0	0
司法院及所屬	37	1	0	36
考試院及所屬	8	3	1	4
監察院及所屬	25	2	0	23
國防部及所屬	32	18	5	9
學術機構	4,112	19	169	3,924
行政院及所屬(不含國防部及所屬)	654	68	183	403
新北市及所屬	165	2	15	148
臺北市及所屬	148	4	13	131
桃園市及所屬	110	1	11	98
臺中市及所屬	201	2	16	183
臺南市及所屬	179	1	16	162
高雄市及所屬	224	2	20	202
臺灣省各縣(市)及所屬	1,297	0	110	1,187
福建省金門縣、連江縣及所屬	88	0	9	79
其他體系(機關)列管	4,221	47	176	3,998
行政院列管	3,066	80	393	2,593

# 資安責任等級應辦事項管理分工(2/2)



- ❖ 各機關（構）資安責任等級檢討完成後，後續應辦事項之推動，**總統府、國安會、立法院、司法院、考試院、監察院暨其所屬機關(構)**，**由各該體系自行推動及管考**
- ❖ 另**國防部及所屬、學術機構**援例分由**國防部、教育部**負責**推動及管考**
- ❖ 其餘本院及所屬機關(構)，以及省政府、直轄市政府、各縣(市)政府暨其所屬機關(構)，將由資安辦**透過資安會報資安作業管考網站**，督促落實執行
- ❖ 總計其他體系(機關)**列管者計4,221個機關**(構、單位)，由資安辦**列管者計3,066個機關**(構、單位)

# 資安責任等級應辦事項推動處理



- ❖ 為順利推動相關作業，於**本年3月上旬**分北、中、南、東4區**辦理6場次資安責任等級分級說明會**
- ❖ 各主管機關依核定(備)之資安責任等級規劃推動應辦事項，所需經費原則由**本年度相關預算勻支或納編105年度預算**，並**協調處理所屬機關(構)經費與人力困難**，屬本院列管者規劃結果需於**本年6月30日前彙送資安辦**
- ❖ 資安辦將彙整各機關推動辦理情形，據以**通盤檢討應辦事項及規劃權宜措施**，並針對各機關**資安經費及人力不足**等問題，持續了解與協處後，綜整相關資料，**送請行政院主計總處及人事行政總處**整體考量及協助因應



報告完畢 敬請指正