Annex A. Key Actions and Timelines – Summary

Key action no.	Action required of:	Requirements	Deadline	Page no. action plan
Preparatory	All Scottish public bodies	• Provide contact details for (i) Board/Senior Management, (ii) working-level, and (iii) incident response to SG Cyber Resilience Unit.	End November 2017	N/A
1	Scottish Government, NCRLB, NCSC, Cyber Catalysts Scottish Government	• Finalise **Scottish Public Sector Cyber Resilience Framework**, taking account of developments with NIS Directive and Security Policy Framework. • Update **Scottish Public Finance Manual** to reflect Framework requirements.	End June 2018 End June 2018	16-18
2	All Scottish public bodies	• Ensure **minimum cyber risk governance arrangements** in place.	End June 2018	19-20
3	All Scottish public bodies managing networks	• Ensure **membership of Cybersecurity Information Sharing Partnership**.	End June 2018	20
4	All Scottish public bodies	• Undergo **Cyber Essentials "pre-assessment"** funded (to defined limits) by Scottish Government. • Take **Board/Senior Management level decision** on whether to pursue Cyber Essentials or Cyber Essentials Plus Certification. • Achieve **Cyber Essentials** or **Cyber Essentials Plus** certification.[29]	End March 2018 End April 2018 End October 2018	21-24

29 As noted in the action plan, it is possible that, in exceptional cases and for some particularly complex public bodies, the pre-assessment will make clear that Cyber Essentials or Cyber Essentials Plus is not an appropriate standard to work towards. It is also possible that, as the process of undergoing Cyber Essentials/Plus pre-assessments or certification for public bodies proceeds, wider issues or challenges in the operation of the scheme will be identified. Where this is the case, public bodies will be encouraged to raise this with the Scottish Government Cyber Resilience Unit who will draw these issues to the attention of the NCSC, and alternatives to Cyber Essentials may be considered.

5	All Scottish public bodies	• Ensure **appropriate implementation of Active Cyber Defence measures**	End June 2018	25-26
6	All Scottish public bodies	• Ensure **initial arrangements for appropriate training and awareness raising** in place.	End June 2018	26-27
	Scottish Government	• Develop and disseminate **core training and awareness raising approach, materials, etc.** for use by public sector, as part of wider security training and awareness raising package.	From March 2018-2020	
	All Scottish public bodies	• **Adapt and implement core training and awareness raising approach, materials, etc.** as it becomes available.	From March 2018-2020	
7	Scottish Government, NCSC, Police Scotland	• Finalise and disseminate **central cyber incident reporting and coordination protocols** and **template cyber incident response plans**.	End 2017	27-28
	All Scottish public bodies	• Ensure **cyber incident response plans in place** and **aligned with central protocols**.	End June 2018	
8	Scottish Government	• Seek views of Scottish business organisations on **draft supply chain cyber security policy on procurement**.	Early 2018	29-30
	Scottish Government	• Publish **Scottish Procurement Policy Note** as part of Scottish Public Sector Cyber Resilience Framework.	End May 2018	
	Scottish Government	• **Align grant funding guidance** and **SPFM**.	End May 2018	
	All Scottish public bodies	• **Implement Scottish Procurement Policy Note** and **grant funding guidance** as part of Scottish Public Sector Cyber Resilience Framework.	From June 2018	

9	Scottish Government	• Put in place **Dynamic Purchasing System** for **Digital services** (including **cyber security**) for Scottish public sector.	End October 2017	30-31
10	Public Sector Cyber Catalysts	• Work with Scottish Government, NCSC and NCRLB to **finalise Scottish Public Sector Cyber Resilience Framework**, and **identify key challenges** facing Scottish public sector.	By end June 2018	31-32
	All Scottish public bodies, inc. Cyber Catalysts	• Begin **implementation of**, and (in line with final arrangements) **reporting against**, Framework.	From end June 2018	
	Public Sector Cyber Catalysts	• **Share learning and knowledge** with wider public sector.	In line with progress	
11	All Scottish public bodies	• **Informal, working-level responses** to enquiries on progress from Scottish Government Cyber Resilience Unit.	Ongoing	33
		• Provide **one-off written assurance at Board/Senior Management level** on the following: ○ confirmation of (i) having undergone a Cyber Essentials pre-assessment, (ii) having taken a decision on whether to seek Cyber Essentials or Cyber Essentials Plus, and (iii) the expected timelines for achieving this. ○ Board/Senior Management level commitment and basic governance arrangements. ○ CiSP membership. ○ Appropriate use of Active Cyber Defence measures. ○ Appropriate training and awareness raising processes. ○ Cyber incident response protocols, aligned with central mechanisms.	End June 2018	
		• Provide **one-off written confirmation** that Cyber Essentials or Cyber Essentials Plus certification (or, exceptionally, alternative independent assurance) has been achieved.	End October 2018	
	Scottish Government	• Develop and implement appropriate **monitoring and evaluation arrangements** as part of **Scottish Public Sector Cyber Resilience Framework**, and communicate these to public bodies.	End June 2018	

Annex A – Key milestones