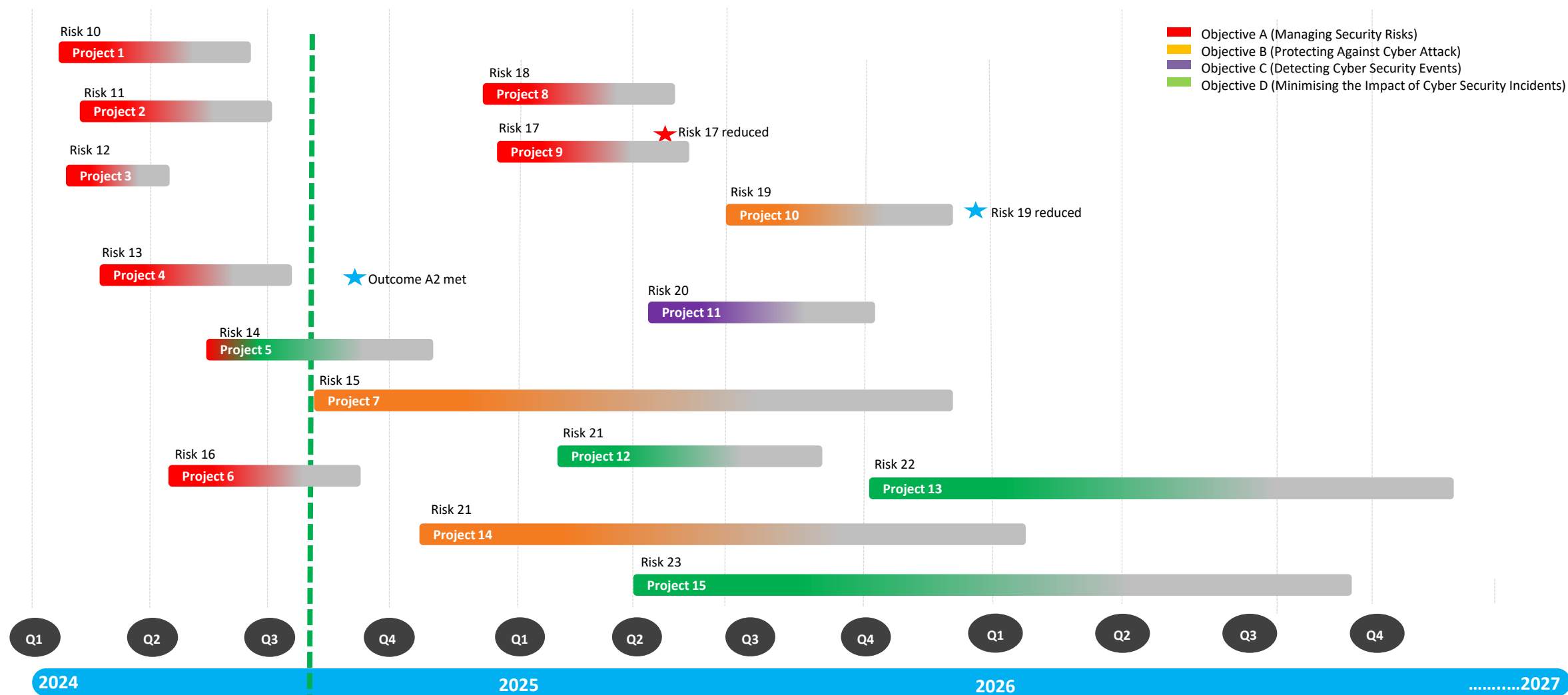


# Ofgem Competent Authority Advisory

## Example Improvement Plan





**Further Information:** This is a suggested format for a Gantt Chart. The OES can choose either Gantt format; they do not need to complete both.

CAF  
Objective

A  
Managing Security Risk



B  
Protecting Against Cyber Attack



**Further Information:** This is a suggested format for a Gantt Chart. The OES can choose either Gantt format; they do not need to complete both.



## CAF Objective

### C Detecting Cyber Security Events

(Risk No13)  
Security Monitoring  
Q1 2020



(Risk No22)  
Security Event Discovery  
Q3 2020



### D Minimising Impact Cyber Incidents

(Risk No14)  
BCM/DR/Crisis Management Plans  
Q1 2020



(Risk No17)  
Lessons Learnt  
Q1 2020



(Risk No17)  
Incident Management  
Q1 2020



Initiative (Risk No32)  
Threat Intelligence  
Q1 2021



Initiative (Risk No23)  
Proactive Monitoring Review  
Q1 2021



**Further Information:** This is a suggested format for a Gantt Chart. The OES can choose either Gantt format; they do not need to complete both.



Improve ment Plan ID	Initiative / Project Name	Initiative / Project Description	Applicable Scope / Improvement Area	Risk Ref No	Risk Criticality	Other Industry Framework Control reference	CAF Mapping –  Related CAF outcomes	Basic Profile and/or Enhanced Profile Maturity alignment	Start Date	Finish Date	Risk Tolerance
<i>The reference ID</i>	<i>Name of initiative</i>	<i>Describe the initiative and include Project Control area (primary)</i>	<i>What scope does this apply to? And exclusions NIS Scope (site, system, geography etc.)</i>	<i>Any relevant risk reference ID (Should align with the ID from the RA)</i>	<i>Is the Improvement Plan mapped to a HIGH risk etc.?</i>	<i>Related control outcomes including <b>compensating controls</b> such as Physical security controls. (If applicable)</i>		<i>Which Profile is the initiative looking to meet or exceed?</i>			<i>Is the risk now within risk appetite? Yes, No</i>  <i>If Yes, then revised risk criticality should be stated e.g. Medium or Low for a High risk If No, then current risk criticality should be stated.</i>
<i>[Example ] PRO 15a</i>	<i>Phase 1 -OT incident management use cases.</i>	<i>Description: Create fully test and implement incident management use cases for top 10 cyber OT incident scenarios. Control: NIST RE. 1</i>	<i>Only Non production environment within the same network boundaries</i>	<i>Risk 23</i>	<i>High</i>	<i>e.g. PE-3 Physical Access Control</i>	<i>D1.a, D1.b, D1.c</i>	<i>BP</i>	<i>31 Oct 21</i>	<i>20 Dec 22</i>	<i>Yes, Low</i>
<i>[Example ] PRO 15b</i>	<i>Phase 2 - OT incident management use cases.</i>	<i>Description: Create fully test and implement incident management use cases for top 10 cyber OT incident scenarios. Control: NIST RE. 1</i>	<i>All NIS scope – Production systems</i>	<i>Risk 24</i>	<i>High</i>	<i>e.g. PE-3 Physical Access Control</i>	<i>C1.a, C1.b, C1.c</i>	<i>EP</i>	<i>31 Oct 21</i>	<i>20 October 23</i>	<i>No, High</i>

Statement which summarises OES Risk Appetite and Risk response should be noted here. This can be a summary statement from NIS Self Assessment Part B. For e.g. Risk response is 'Mitigate' for all Medium and High risk criticality etc.