APPENDIX E

DETECTING CYBER SECURITY EVENTS
The organisation monitors the security status of the networks and systems supporting the operation of essential functions in order to detect potential security problems and to track the ongoing effectiveness of protective security measures.

Not achieved - At least one of the following statements is true	Partially achieved - All of the following statements are true	Achieved - All the following statements are true	
Data relating to the security and operation of your essential functions is not collected.	Data relating to the security and operation of some areas of your essential functions is collected but coverage is not comprehensive.	Monitoring is based on an understanding of your networks, common cyber attack methods and what you need awareness of in order to detect potential security incidents that could affect the operation of your essential function (e.g. presence of malware, malicious emails, user policy violations).	
You do not confidently detect the presence or absence of Indicators of Compromise (IoCs) on your essential functions, such as known malicious command and control signatures (e.g. because applying the indicator is difficult or your logging data is not sufficiently detailed).	You easily detect the presence or absence of IoCs on your essential function, such as known malicious command and control signatures.	Your monitoring data provides enough detail to reliably detect security incidents that could affect the operation of your essential function.	
You are not able to audit the activities of users in relation to your essential function.	Some user monitoring is done, but not covering a fully agreed list of suspicious or undesirable behaviour.	You easily detect the presence or absence of IoCs on your essential functions, such as known malicious command and control signatures.	
You do not capture any traffic crossing your network boundary including as a minimum IP connections.	You monitor traffic crossing your network boundary (including IP address connections as a minimum).		

APPENDIX E

Not achieved - At least one of the following statements is true	Partially achieved - All of the following statements are true	Achieved - All the following statements are true
It is possible for logging data to be easily edited or deleted by unauthorised users or malicious attackers.	Only authorised staff can view logging data for investigations.	The integrity of logging data is protected, or any modification is detected and attributed.
There is no controlled list of who can view and query logging information.	Privileged users can view logging information.	The logging architecture has mechanisms, processes and procedures to ensure that it can protect itself from threats comparable to those it is trying to identify. This includes protecting the function itself, and the data within it.
There is no monitoring of the access to logging data.	There is some monitoring of access to logging data (e.g. copying, deleting or modification, or even viewing.)	Log data analysis and normalisation is only performed on copies of the data keeping the master copy unaltered.
There is no policy for accessing logging data.		Logging datasets are synchronised, using an accurate common time source, so separate datasets can be correlated in different ways.
Logging is not synchronised, using an accurate common time source.		Access to logging data is limited to those with business need and no others.
		All actions involving all logging data (e.g. copying, deleting or modification, or even viewing) can be traced back to a unique user.
		Legitimate reasons for accessing logging data are given in use policies.

APPENDIX E

Not achieved - At least one of the following statements is true	Partially achieved - All of the following statements are true	Achieved - All the following statements are true
Alerts from third party security software is not investigated e.g. Anti-Virus (AV) providers.	Alerts from third party security software are investigated, and action taken.	Logging data is enriched with other network knowledge and data when investigating certain suspicious activity or alerts.
Logs are distributed across devices with no easy way to access them other than manual login or physical action.	Some, but not all, logging datasets can be easily queried with search tools to aid investigations.	A wide range of signatures and indicators of compromise is used for investigations of suspicious activity and alerts.
The resolution of alerts to a network asset or system is not performed.	The resolution of alerts to a network asset or system is performed regularly.	Alerts can be easily resolved to network assets using knowledge of networks and systems. The resolution of these alerts is performed in almost real time.
Security alerts relating to essential functions are not prioritised.	Security alerts relating to some essential functions are prioritised.	Security alerts relating to all essential functions are prioritised and this information is used to support incident management.
Logs are reviewed infrequently.	Logs are reviewed at regular intervals.	Logs are reviewed almost continuously, in real time.
		Alerts are tested to ensure that they are generated reliably and that it is possible to distinguish genuine security incidents from false alarms.

Not achieved - At least one of the following statements is true	Partially achieved - All of the following statements are true	Achieved - All the following statements are true

APPENDIX E

Your organisation has no sources of threat intelligence.	Your organisation uses some threat intelligence services, but you don't necessarily choose sources or providers specifically because of your business needs, or specific threats in your sector (e.g. sector-based infoshare, ICS software vendors, anti-virus providers, specialist threat intel firms, special interest groups).	You have selected threat intelligence feeds using risk-based and threat-informed decisions based on your business needs and sector (e.g. vendor reporting and patching, strong anti-virus providers, sector and community-based infoshare, special interest groups).	
You do not apply updates in a timely way, after receiving them. (e.g. AV signature updates, other threat signatures or Indicators of Compromise (IoCs).	You receive updates for all your signature based protective technologies (e.g. AV, IDS).	You apply all new signatures and IoCs within a reasonable (risk-based) time of receiving them.	
You do not receive signature updates for all protective technologies such as AV and IDS or other software in use.	You apply some updates, signatures and IoCs in a timely way.	You receive signature updates for all your protective technologies (e.g. AV, IDS).	
You do not evaluate the usefulness of your threat intelligence or share feedback with providers or other users.	You know how effective your threat intelligence is (e.g. by tracking how threat intelligence helps you identify security problems).	You track the effectiveness of your intelligence feeds and actively share feedback on the usefulness of IoCs and any other indicators with the threat community (e.g. sector partners, threat intelligence providers, government agencies).	
Not achieved - At least one of the following statements is true	**Partially achieved - All of the following statements are true**	**Achieved - All the following statements are true**	
There are no staff who perform a monitoring function.	Monitoring staff have some investigative skills and a basic understanding of the data they need to work with.	You have monitoring staff, who are responsible for the analysis, investigation and reporting of monitoring alerts covering both security and performance.	

APPENDIX E

Monitoring staff do not have the correct specialist skills.	Monitoring staff can report to other parts of the organisation (e.g. security directors, resilience managers).	Monitoring staff have defined roles and skills that cover all parts of the monitoring and investigation process.	
Monitoring staff are not capable of reporting against governance requirements.	Monitoring staff are capable of following most of the required workflows.	Monitoring staff follow process and procedures that address all governance reporting requirements, internal and external.	
Monitoring staff lack the skills to successfully perform some significant parts of the defined workflow.	Your monitoring tools can make use of logging that would capture most unsophisticated and untargeted attack types.	Monitoring staff are empowered to look beyond the fixed process to investigate and understand non-standard threats, by developing their own investigative techniques and making new use of data.	
Monitoring tools are only able to make use of a fraction of logging data being collected.	Your monitoring tools work with most logging data, with some configuration.	Your monitoring tools make use of all logging data collected to pinpoint activity within an incident.	
Monitoring tools cannot be configured to make use of new logging streams, as they come online.	Monitoring staff are aware of some essential functions and can manage alerts relating to them.	Monitoring staff and tools drive and shape new log data collection and can make wide use of it.	
Monitoring staff have a lack of awareness of the essential functions the organisation provides, what assets relate to those functions and hence the importance of the logging data and security events.		Monitoring staff are aware of the operation of essential functions and related assets and can identify and prioritise alerts or investigations that relate to them.	

The organisation detects, within networks and information systems, malicious activity affecting, or with the potential to affect, the operation of essential functions even when the activity evades standard signature based security prevent/detect solutions (or when standard solutions are not deployable).

APPENDIX E

Not achieved - At least one of the following statements is true	Achieved - All the following statements are true	Comments
Normal system behaviour is insufficiently understood to be able to use system abnormalities to detect malicious activity.	Normal system behaviour is fully understood to such an extent that searching for system abnormalities is a potentially effective way of detecting malicious activity (e.g. you fully understand which systems should and should not communicate and when).	
You have no established understanding of what abnormalities to look for that might signify malicious activities.	System abnormality descriptions from past attacks and threat intelligence, on yours and other networks, are used to signify malicious activity.	SOCOS
	The system abnormalities you search for consider the nature of attacks likely to impact on the networks and information systems supporting the operation of essential functions.	We prioritise (DLUHC?
	The system abnormality descriptions you use are updated to reflect changes in your networks and information systems and current threat intelligence.	No clearly defined feedback loop

Not achieved - At least one of the following statements is true	Achieved - All the following statements are true	Comments

You do not routinely search for system abnormalities indicative of malicious activity.	You routinely search for system abnormalities indicative of malicious activity on the networks and information systems supporting the operation of your essential function, generating alerts based on the results of such searches.	3rd party Intergence contract plus in-house CISM expertise. However due to **resourcing/ recruitment** in-house expertise resource is sporadic
	You have justified confidence in the effectiveness of your searches for system abnormalities indicative of malicious activity.	3rd party Intergence contract plus in-house CISM expertise. However due to **resourcing/ recruitment** in-house expertise resource is sporadic

CAF Objective D - Minimising the impact of cyber security incidents

Capabilities exist to minimise the adverse impact of a cyber security incident on the operation of essential functions, including the restoration of those functions where necessary.

Principle: D1 Respons	There are well-defined and tested incident management processes in place, that aim to ensure continuity of essential functions in the event of system or

e and Recovery Planning	service failure. Mitigation activities designed to contain or limit the impact of compromise are also in place.

D1.a Response Plan	**Not achieved - At least one of the following statements is true**	**Partially achieved - All of the following statements are true**	**Achieved - All the following statements are true**
You have an up-to-date incident response plan that is grounded in a thorough risk assessment that takes account of your essential function and covers a range of incident scenarios.	Your incident response plan is not documented.	Your response plan covers your essential functions.	Your incident response plan is based on a clear understanding of the security risks to the networks and information systems supporting your essential function.
	Your incident response plan does not include your organisation's identified essential function.	Your response plan comprehensively covers scenarios that are focused on likely impacts of known and well-understood attacks only.	Your incident response plan is based on a clear understanding of the security risks to the networks and information systems supporting your essential function.
	Your incident response plan is not well understood by relevant staff.	Your response plan is understood by all staff who are involved with your organisation's response function.	Your incident response plan is based on a clear understanding of the security risks to the networks and information systems supporting your essential function.
	DRAFT to be discussed/ recommended for adoption by Cyber T&F group.	Your response plan is documented and shared with all relevant stakeholders.	

D1.b Response and Recovery Capability	**Not achieved - At least one of the following statements is true**	**Achieved - All the following statements are true**

You have the capability to enact your incident response plan, including effective limitation of impact on the operation of your essential function. During an incident, you have access to timely information on which to base your response decisions.	Inadequate arrangements have been made to make the right resources available to implement your response plan.	You understand the resources that will likely be needed to carry out any required response activities, and arrangements are in place to make these resources available.
	Your response team members are not equipped to make good response decisions and put them into effect.	You understand the types of information that will likely be needed to inform response decisions and arrangements are in place to make this information available.
	Inadequate back-up mechanisms exist to allow the continued operation of your essential function during an incident.	Your response team members have the skills and knowledge required to decide on the response actions necessary to limit harm, and the authority to carry them out.
		Key roles are duplicated, and operational delivery knowledge is shared with all individuals involved in the operations and recovery of the essential function.
		Back-up mechanisms are available that can be readily activated to allow continued operation of your essential function (although possibly at a reduced level) if primary networks and information systems fail or are unavailable.

		Arrangements exist to augment your organisation's incident response capabilities with external support if necessary (e.g. specialist cyber incident responders).	

D1.c Testing and Exercising	Not achieved - At least one of the following statements is true	Achieved - All the following statements are true	
Your organisation carries out exercises to test response plans, using past incidents that affected your (and other) organisation, and scenarios that draw on threat intelligence and your risk assessment.	Exercises test only a discrete part of the process (e.g. that backups are working), but do not consider all areas.	Exercise scenarios are based on incidents experienced by your and other organisations or are composed using experience or threat intelligence.	
	Incident response exercises are not routinely carried out or are carried out in an ad-hoc way.	Exercise scenarios are documented, regularly reviewed, and validated.	
	Outputs from exercises are not fed into the organisation's lessons learned process.	Exercises are routinely run, with the findings documented and used to refine incident response plans and protective security, in line with the lessons learned.	
	Exercises do not test all parts of the response cycle.	Exercises test all parts of your response cycle relating to your essential functions (e.g. restoration of normal function levels).	

Principle: D2 Lessons Learned	When an incident occurs, steps are taken to understand its root causes and to ensure appropriate remediating action is taken to protect against future incidents.	

APPENDIX E

D2.a Incident Root Cause Analysis	Not achieved - At least one of the following statements is true	Achieved - All the following statements are true	
When an incident occurs, steps must be taken to understand its root causes and ensure appropriate remediating action is taken.	You are not usually able to resolve incidents to a root cause.	Root cause analysis is conducted routinely as a key part of your lessons learned activities following an incident.	
	You do not have a formal process for investigating causes.	Your root cause analysis is comprehensive, covering organisational process issues, as well as vulnerabilities in your networks, systems or software.	
		All relevant incident data is made available to the analysis team to perform root cause analysis.	

D2.b Using Incidents to Drive Improvements	Not achieved - At least one of the following statements is true	Achieved - All the following statements are true	
Your organisation uses lessons learned from incidents to improve your security measures.	Following incidents, lessons learned are not captured or are limited in scope.	You have a documented incident review process/policy which ensures that lessons learned from each incident are identified, captured, and acted upon.	
	Improvements arising from lessons learned following an incident are not implemented or not given sufficient organisational priority.	Lessons learned cover issues with reporting, roles, governance, skills and organisational processes as well as technical aspects of networks and information systems.	

		You use lessons learned to improve security measures, including updating and retesting response plans when necessary.	
		Security improvements identified as a result of lessons learned are prioritised, with the highest priority improvements completed quickly.	
		Analysis is fed to senior management and incorporated into risk management and continuous improvement.	

Principles & Related Guidance
https://www.ncsc.gov.uk/collection/caf/table-view-principles-and-related-guidance