GovAssure: The new cyber security regime

WHITE PAPER

DATE: October 2023

AUTHOR: Tom Miller

VERSION: 1.0

TABLE OF CONTENTS

Introduction 3

What does this mean? 3

What is GovAssure? 3

Stage 1: Organisational context, essential services, and mission 4

Stage 2: In-scope systems and assignment of the Government CAF profile 4

Stage 3: CAF self-assessment 4

Stage 4: Independent assurance review 4

Stage 5: Final assessment and targeted improvement plan 5

How AMR CyberSecurity can help 5

Introduction

With an ever-growing threat facing HM Government (HMG), cyber security capability has become ever more important and critical to ensuring the UK remains safe and secure. GovAssure is an enhanced cyber security programme that has been implemented by HMG to ensure HMT IT systems are protected from this growing threat. GovAssure is run by the Cabinet Office's Government Security Group (GSG), with input from the National Cyber Security Centre (NCSC).

This whitepaper aims to explain and provide an overview of the history of GovAssure, what it means for government departments and how AMR Cyber security can assist in delivering the key aims of the programme and HMG's Cyber Security Strategy.

What does this mean?

The Chancellor of the Duchy of Lancaster announced GovAssure in his speech to CyberUK in April 2023. He said: "*Cyber threats are growing, which is why we are committed to overhauling our defences to better protect government from attacks. Today's cyber assurance will strengthen government systems, which run vital services for the public, from attacks. It will also improve the country's resilience, a key part of our recent Integrated Review Refresh.*"

The GovAssure programme has been established to review government departments and select arm's length bodies, approach to cyber security. It is currently only designated for OFFICIAL systems and does not apply to SECRET systems or higher. (Government Security Classifications - GOV.UK (www.gov.uk)).

It will enhance HMG's understanding of the cyber security posture and capability of government departments, and arm's length bodies. Through robust and thorough annual security audits, departments will attest to their cyber security assurance measures as set out in the NCSC's Cyber Assessment Framework (CAF) (NCSC CAF guidance - NCSC.GOV.UK).

The CAF was originally designed by the NCSC to be used by operators within Critical National Infrastructure (CNI) in relation to the Network & Information Systems (NIS) Regulations, which aimed to raise cyber security levels and the resilience of key systems across the EU. NIS came into force in the UK in May 2018.

What is GovAssure?

GovAssure will replace the existing 'Departmental Security Health Checks' that departments must currently fill out and provide to Cabinet Office for review. This is a key part of the Governments Cyber Security Strategy (Government Cyber Security Strategy: 2022 to 2030 - GOV.UK (www.gov.uk)) to improve cyber resilience and help government organisations protect themselves from growing hostile cyber threats.

GovAssure is a five-stage process:

1. Organisational contact and services
2. In-scope systems and assignment to the Government CAF profile

3. CAF self-assessment
4. Independent assurance review
5. Final assessment and targeted improvement plan

Stage 1: Organisational context, essential services, and mission

The first stage of GovAssure is a scoping exercise. This requires organisations to develop a complete understanding of their strategic context and establish an understanding of the cyber security threat landscape in which it operates.

The scope will be defined by the essential services that the department provides: either in relation to CNI, or Operators of Essential Services (OES).

Stage 2: In-scope systems and assignment of the Government Cyber Asessment Frameworkprofile

Once essential services are identified, critical systems are then identified. Critical systems may be a mix of operational and support systems in relation to the identified essential services.

There are two Government Cyber Assessment Framework (CAF) profiles: Baseline and Enhanced. These profiles will be assigned through discussion with GSG, the NCSC and the Cabinet Office. However, the enhanced profile will be automatically applied to government CNI.

Stage 3: CAF self-assessment

The CAF has four objectives:

1. Managing security risk
2. Protecting against cyber attack
3. Detecting cyber security events
4. Minimising the impact of cyber security incidents

Departments should complete the self-assessment with input from relevant key stakeholders within the organisation. The CAF has been mapped to several industry standard frameworks, including ISO 27001 and NIST SP 800-53. (https://www.security.gov.uk/guidance/govassure/downloads/GovAssure_CAF-Mapping-Document.xlsx)

Stage 4: Independent assurance review

Accredited third parties will perform independent reviews to verify the organisations self-assessment. This review will assess the level of attainment to the relevant CAF profile, validate the results of the self-assessed findings, and determine the effectiveness of the current cyber security controls.

This assessment will evaluate the level of attainment of the relevant Government CAF

profilevia:

- A review of the customer completed WebCAF submissions provided for the system in scope.
- A review of the supporting documentation referenced within the customer WebCAF submissions provided for the system in scope.
- Interviews with key stakeholders to review responses on a per objective basis.

Reviews will consider the extent to which supporting indicators of good practice have been achieved, partially achieved, or not achieved.

Stage 5: Final assessment and targeted improvement plan

Once the independent review has been completed, a final assessment report is generated and provided to the organisation by the Independent Assurance provider. GSG will then work with the organisation to develop a Targeted Improvement Plan, outlining a prioritised list of areas for improvement.

How AMR CyberSecurity can help

AMR CyberSecurity is a GovAssure Independent Assurance Reviewer and can provide the stage 4 aspect of GovAssure to relevant organisations. We can provide several highly skilled and qualified assurance consultants to assist organisations in carrying out the Independent Assurance Review, as well as other assurance activities in relation to cyber security.