CCS ACCREDITATION

FOR

BravoSolution Enterprise Sourcing Platform (ESoP) & Commerce Decisions AWARD

This Certificate of Accreditation is a statement that the CCS Accreditor considers **BravoSolution Enterprise Sourcing Platform (ESoP) and Commerce Decisions AWARD** to have appropriate risk management measures in place to allow processing of OFFICIAL information and that the CCS SIRO accepts this assessment.

BravoSolution Enterprise Sourcing Platform (ESoP) and Commerce Decisions AWARD has undergone a risk assessment to identify, assess and articulate the risks to the data it will process. In addition, the treatment of these risks has been examined along with the remediation of vulnerabilities which have been assessed following annual IT Health checks. Evidence of the process is contained in: the Risk Management Accreditation Document Set (RMADS) produced in accordance with HMG IA Standard Numbers 1 & 2 – Supplement, Technical Risk Assessment and Risk Treatment, v1.0 April 2012.

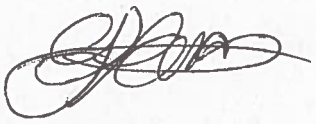
References:

eSourcing RMADS v2.0 dated 31/07/14

Responses to 2015 Pen Test – GPS - Aristi

The service described may therefore be operated in accordance with these measures and procedures for the purpose of conducting HMG business, and is accredited to store, forward and process information which is assessed as up to and including OFFICIAL.

This accreditation remains subject to the compliance checks and reaccreditation conditions described in the RMADS referenced above.



Gemma Sanders

CCS Accreditor

Date: 24 FEBRUARY 2015

This Certificate of Accreditation is valid for a period of 24 months from the date of the Accreditor's signature.

Crown Commercial Service

BACKGROUND

NOTE: The following is based on documents available from:

https://www.gov.uk/government/collections/government-security

Prior to April 2014 a security process called accreditation was mandated by the HMG Security Policy Framework (SPF) for all Government departments processing classified information. The process of accreditation provided for the assessment of a system against its security requirements, and approval was required from an accreditor as a prerequisite for operation. This was removed as a mandatory requirement from the April 2014 version of the SPF.

However, there is still a CCS requirement for a risk assessment to identify, assess and articulate the risks to organisations which may choose to use systems supplied by CCS or through a CCS Framework. This is done to provide confidence that the technology and information is secure enough to meet users' business needs.

All ICT systems that manage government information or that are interconnected to HMG systems and which are supplied by CCS, or through a CCS managed Framework, are assessed to identify technical risks. Proportionate assurance processes provide confidence that these identified risks are being properly managed.

Risks that result in the following outcomes are not accepted by CCS:

- Harm to the physical well-being of customers and employees
- Harm to the financial well-being of customers and employees
- Breaches of the organisation's legal or regulatory responsibilities
- Widespread damage to the reputation of HMG and departments.

Where a system relies on the security provided by a commercial product or service then there is no need to conduct customised technology and information risk assessments to help specify additional security controls. However, in this case CCS accepts that:

- It is completely reliant on the security claimed to be provided by commercial products and services, which can vary from 'very robust' to 'almost none at all'
- Security won't be tailored to any specific needs the user organisations might have

From a security perspective, if this approach is chosen it does not mean 'do nothing'. Where CCS chooses to take this approach there still needs to be evidence of:

- Organisational controls (for example personnel security, physical security and security training for users)
- Confidence and assurance that the commercial products and services they use are appropriate in the context of what they are doing and the threats they face
- Trusted 3rd party assessments of vulnerabilities and their remediation.