

# UNCLASSIFIED

## **CESG Tailored Assurance Service Guidance Note 1- Transitions from Fast Track Assessments (FTA) and System Evaluations (SYSn) to CTAS**

### **Purpose**

This paper provides guidance on how to effect the transition of existing products and systems evaluated under certain Legacy Assurance Services (FTA and SYSn) onto CESG's Tailored Assurance Service (CTAS) whilst maintaining the assurance that has been previously established.

### **Principles**

Achieving the best value for money whilst still ensuring that the assurance is not compromised was the foremost consideration when preparing this Guidance; to that end appropriate re-use of evaluation material from any previous FASTRACK and SYSn evaluations is strongly encouraged.

### **Transition**

CTAS and the Legacy Services are different services with different evaluation methodologies and activities; hence before any product or system can enter CTAS it *must* go through a 'CTAS Gateway Review'. This Review will take account of as much material from the Legacy Services as appropriate (to ensure that legacy work is not nugatory) and map these to CTAS requirements.

It is expected that as a result of a Gateway Review the eventual CTAS Evaluation for the transferred system or product will require appreciably less time and effort than would a full new CTAS Evaluation (where information from the Legacy Services does not exist or is not available)<sup>1</sup>.

The Gateway Review shall be chaired by CESG.

During the Gateway Review the various stakeholders (the Accreditor, Sponsor, CESG, Developer and Customer) should identify any significant changes and consider their implications. Such changes can include:

- An alteration to the Impact Levels (C, I, A) arising from the current use of the system or product;
- Changes to system or product design or implementation;

---

<sup>1</sup> CESG does not currently have any data on how much information can typically be re-used in the Gateway Review; naturally, the actual amount will vary per evaluation.

## UNCLASSIFIED

- Modification to the legacy Security Target (ST) and Evaluation Work Programme (EWP) (to be updated with the changes and agreed by all parties);
- Modification to the legacy AMP (if available, otherwise it will need to be developed);
- Alterations to the security environment in which the product or system will be deployed;
- Changes in the level of threat to the product or system (driven by a changing threat environment);

The Sponsor is required to submit an SIA (Security Impact Analysis) detailing all the changes to the Target of Evaluation since completion of the original evaluation and the effects of these on security performance and assurance.

It is the Accreditor's prerogative to determine the admissibility of any information re-used from the Legacy Assurance work.

The three possible outcomes of the Gateway Review are:

- 1) A decision to allow a restricted scope CTAS Evaluation, re-using previous results as appropriate (such a decision requires the unanimous approval of all stakeholders);
- 2) A decision to require a full CTAS re-evaluation;
- 3) Exceptionally - a refusal to accept the system for CTAS Evaluation.

In the case of the first two outcomes the output of the Gateway Review shall include:

- An endorsed Security Target either as supplied or with specified modifications;
- An outline EWP for development by the Evaluation Companies;
- Recommendations on the production of an Assurance Maintenance Plan (AMP).

Ideally the Gateway Review will be completed before the Legacy Service Accreditation expires (with time to spare); this process is represented in Figure 1 below.

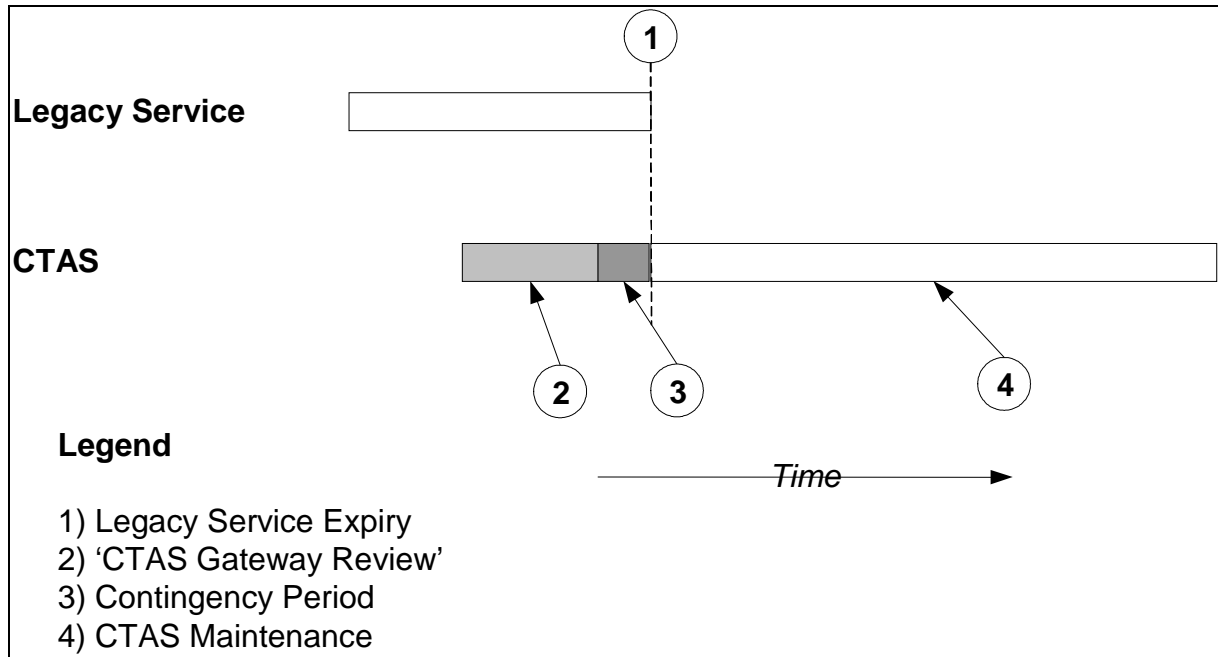


Figure 1: Normal Transition from Legacy Services to CTAS

### Maintenance

Part of the 'CTAS Gateway Review' (as with New CTAS Evaluations) will be agreeing an Assurance Maintenance Plan (AMP). Once the Review is completed and the AMP is agreed the product or system will be considered to be in CTAS Maintenance.

### Interim Arrangements

It is recognised that, in some cases, the situation where the Legacy Service expires before a CTAS Gateway Review has taken place is unavoidable and an Interim Arrangement is necessary.

Ultimately the assurance of the system is the responsibility of the Accreditor and they have two choices:

- 1) Agree a 'Grace Period' during which the system continues to operate temporarily even after the accreditation has expired (and arrange a 'CTAS Gateway Review' for the earliest possible date);
- 2) Suspend operation of the system until a 'CTAS Gateway Review' has been completed.

It is expected that the Accreditor's decision will be made in consultation with the SIRO, Customer, Sponsor, and CESG.

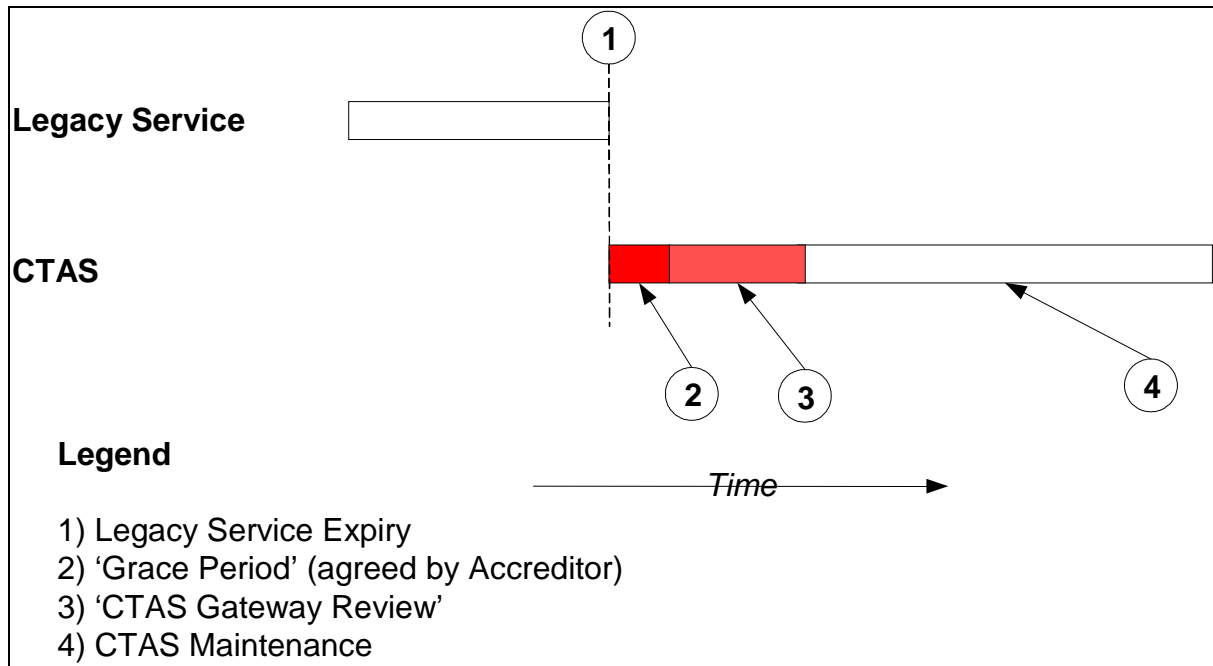


Figure 2: Transition where an interim arrangement is required

It is important to emphasise that the situation represented in Figure 2 is far from ideal and every effort should be made to proactively engage the CTAS Service as soon as possible.

### Intellectual Property Issues

The re-use of the information from the Legacy Services is highly dependent on which organisation owns the Intellectual Property (specifically the copyright). It is imperative that the customer and sponsor re-assure themselves that the information is releasable to the Evaluation Companies in advance of the CTAS Gateway Review taking place.

In the case of FASTRACK there is a generic contract that ensures that the intellectual property of evaluation reporting belongs to the Crown; hence is reusable.

In the case of SYSn there is no contract with CESG and which organisation owns the intellectual property will depend on the specific contract. The status of the title in the intellectual property needs to be ascertained for each situation.

For further details on intellectual property issues please contact CESG ([iacs@cesg.gsi.gov.uk](mailto:iacs@cesg.gsi.gov.uk)).