SECAS Guidance Document: Director's Letter

Following a Security Assessment, a User may be asked to submit a Director's Letter, confirming that all outstanding observations have been remediated. There are two scenarios in which a User may be asked to submit a Director's Letter:

Following a Full User Security Assessment (FUSA)

If the Security Sub-Committee (SSC) sets your assurance status to '**Approved subject to Steps; Submitting a Directors Letter**', the User will be required to submit an Action Plan and Director's Letter to address the outstanding observations.

The action plan can be found in the Validation Workbook which is one of the document links at the bottom of the Security Assessments webpage. Users must submit a Director's Letter a **minimum of 8 weeks** in advance of their desired DCC Go-Live date.

Following a Verification User Security Assessment (VUSA) or a Security Self-Assessment (SSA)

If the SSC sets your compliance status to '**Compliant, subject to providing a remediation plan for the outstanding obligations, with a subsequent Director-signed cover letter once these obligations are remediated**', the User must submit the remediation plan to SECAS by the deadline given during the SSC meeting. The User will have **at least three weeks** to prepare the plan. Once this has been reviewed, this will be presented back to the SSC for information.

The remediation plan template can be found here. The subsequent Director-signed cover letter should be submitted once all remediations have been completed in accordance with the plan.

Content of Director's Letter

The Director's Letter should confirm that the steps set out in the User management response, together with any additional or alternative steps set out by the SSC, have been completed and signed off through internal governance. The Director's Letter should be accompanied by an **Action Plan** (when following a FUSA), or a **Remediation Plan** (when following a VUSA/SSA) which references the User Assessment CIO Report and should be updated with a detailed explanation of the steps taken and actions completed since the SSC review, along with details of any documentary evidence that has been updated.

In some cases, it may not be possible to complete all the actions prior to seeking SSC confirmation that the steps have been met (e.g. when a penetration test is scheduled to complete just before go-live or where destruction of data will not occur until after the start of live operations).

In these cases, the Director's letter should confirm that these steps will be completed with a **planned date**, together with explanatory details (e.g. the penetration test has been scheduled for 'x' date by 'y' CREST qualified Company and 'z' time has been allowed for any necessary remediation action).

The validation of the Director's Letter takes a **minimum of 10 working days** to complete. The validation may require back and forth engagement between Users and the Security Experts depending on the quality of the response, and the number of outstanding observations raised by the User CIO that have not been remediated as part of the Management Response.

Authorised Signatories

The Director should be either an Officer of the Company listed at Companies House; or an Authorised Director who has been given authority by the Company Board to commit the Company to completing the actions in the Management Response. If the latter, then this should be stated in the Director's Letter. The company letterhead should be as per gov.uk guidance found here.

Director's Letter Template

[Company Logo / Letter-headed paper]

[Company registered address]

[Company registration number]

[Date]

FAO: The Security Sub-Committee (SSC)

Dear Sir/Madam,

I write on behalf of <Your SEC Party Name> to confirm the observations from our Full/Verification User Security Assessment Report, dated XX/XX/XXXX, have been remedied as below:

GX.XX – *[A brief description on the action taken to remediate the observation and date on which this was completed]*

GX.XX – *[A brief description on the action taken to remediate the observation and date on which this was completed]*

GX.XX – *[A brief description on the action taken to remediate the observation and date on which this was completed]*

[Any other comments you wish to add regarding your Assessment and/or Remediation Plan]

Yours sincerely,

[Position in company and if applicable, that authority has been given by the Board to sign on their behalf]