

Assurance Certificate



HM Prison &
Probation Service

HMPPS Information Security Team

System/Project Name:	Coracle
Environment:	HM Prisons
Date of Certificate:	12th May 2021
Version:	1.0

References:

1. High Level Design Document v3.0.
2. ITHC Penetration test by Fidus.
3. Risk Summary.

Assurance History

Coracle have been in prisons in a small capacity using their system having had a narrow assurance scope previously undertaken by MoJ. HMPPS Education have taken on this system oversight, and wanted to increase the scope. So that it could be used for a much wider range of deliverables, utilising their system that had been enhanced to provide this new level of service.

They have supplied a high level design (HLD), and have undergone an ITHC penetration test by a NCSC CHECK approved company. All recommended actions have been either completed, mitigated or accepted. There are no outstanding recommendations.

Business Context

Coracle is currently providing very limited education services in a small number of prisons. They are now approved to take more externally provided content from a range of providers. Including a direct input from Virtual Campus. To then reformat and put into their system (Osprey VLE). This will then be downloaded onto Chromebooks. These will connect in a secure sterile area via broadband to the Coracle cloud, to upload finished work, and download new work and any system updates. They are in cell approved for prisoner use.

Scope of Assurance

The scope of assurance is shown in the following diagrams (Figures 1 and 2):

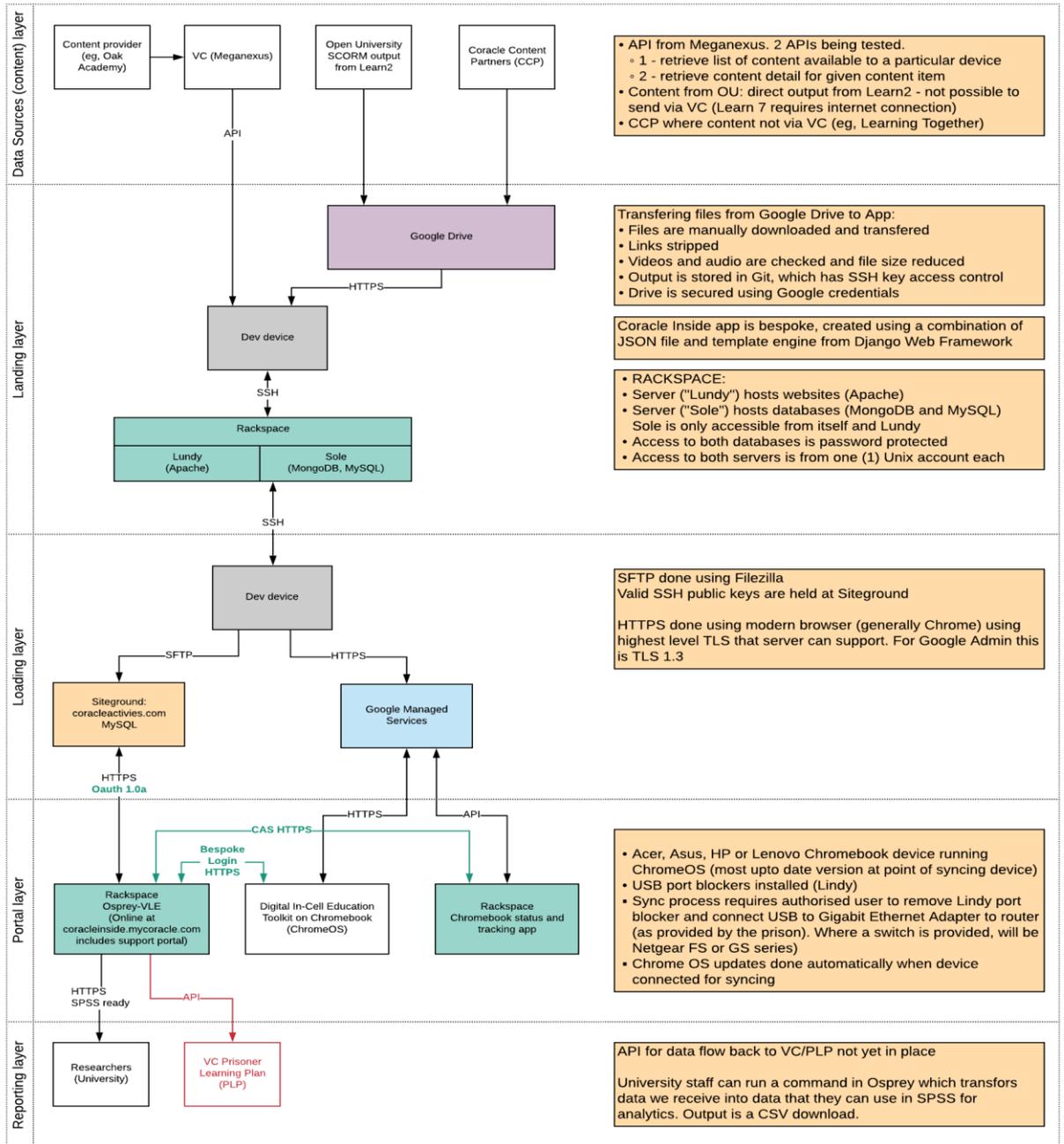
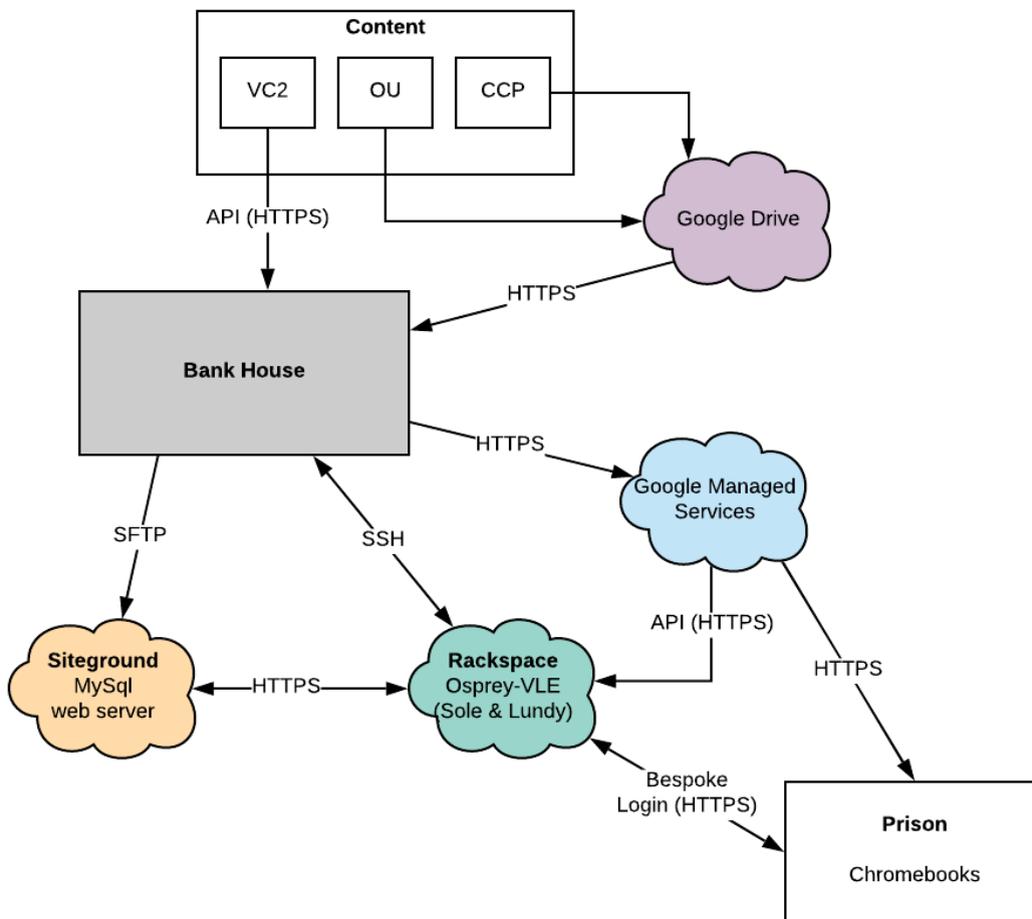


Figure 1 - Scope of Assurance Diagram



Locations are colour coded to match the layer levels in figure 1.

Figure 2 - Network Architecture Diagram

Assurance Decision

This assurance certificate covers the operation of the Coracle Chromebooks in HM Prisons, including In Cell prisoner use and the transfer of information via broadband. There is a separate SyOps for local prison use in the operation and requirements.

Risks identified within the Penetration Test Treatment Plan not mitigated are accepted on the basis of the evidence presented in the current operating environment and the residual risk assessment.

Operation of the system outside the parameters laid down in the HLD, or a serious security incident, or a cluster of minor security incidents that involves the applications, data or infrastructure may invalidate the assurance.

Any changes to the system that impacts on the risk assessment or risk treatment, or changes to the threat landscape during the period of assurance must be submitted for review by HMPPS Information Security Team with a view to re-assurance.

Continued Assurance will be dependent on a robust annual ITHC conducted as per the current HMG requirements found here: <https://www.gov.uk/government/publications/it-health-check-ithc-supporting-guidance>

Note: Security Assurance provides no guarantee that security incidents will not occur but is an indication that a risk management process has been followed based on assurances provided by the education provider and the penetration test company.

Risk Summary

The risks identified by the Penetration test process for this system have been suitably mitigated or accepted.

HMPPS Assurer

Name	Patrick Clarke
Post	HMPPS Deputy head of Information Security
Signature	Patrick Clarke (email confirmation)
Date	12/05/2021
Assurance Date	13/05/2021
Assurance Expiry Date & Notes	Because the assurance is being undertaken by continuous assurance in the standard of ISO 27001 risk audit and treatment, and under the security working group compliance. There is no expiry of the assurance.

Information Asset Owner/ System Owner

Name	Sarah McKnight
Post	Deputy Director Of Reducing Reoffending
Signature	Sarah.McKnight@justice.gov.uk
Date	13/05/2021
Note	-