Clearlane CRA

Operational qualification (OQ) test script

Run in a test Jira project with at least two test users. Record the app version (Manage apps) and your site before starting. Attach a screenshot to each test. User A: Jira administrator (always in the security team). User B: second test user, not in the security team, who can browse and edit the test project. Clearlane CRA helps you meet the reporting requirements of the Cyber Resilience Act (Article 14, applying since 11 September 2026); it does not submit anything to ENISA's single reporting platform.

App version	
Site	
Executed by	
Date	
Approved by	

Test	Steps	Expected result	Result (pass / fail)	Tester, date
OQ-01 Settings and signing password	As User A (Jira administrator), open Apps > Clearlane CRA > "Settings". Under "Manufacturer", fill "Name", "Website (https)" and "Security contact"; keep the reminder box ("Send each case owner one reminder e-mail a day…") checked; under "Signing password policy", set "Attempts before lock" to 3 and "Lock (minutes)" to 5; press "Save". In "Signing password", type a 7-character password in "New password" and press "Save the password", then a password of 8 characters or more.	"Settings saved" appears. The 7-character password is refused with "The password is too short."; the longer one is accepted ("Saved") and "Change the password" is offered. User B (not a Jira administrator, not named in "Security team") has no "Settings" tab.		
OQ-02 Register a product and its support period	In "Products", press "Add a product": "Product name" = Gateway Console, "Type" = Software, "CRA class" = Default, no Member State selected; press "Save". Then press "All 27", add the test project in "Jira projects" and press "Save". In the product, press "Add a version": "Version" = 2.4.1, "On the market since" = one year ago, leave "Support until" as proposed, press "Save". Add version 2.4.0 with "Support until" two years after its market date and press "Save"; then fill "Why a shorter support period" and press "Save" again.	Without a Member State, saving is refused with "Some fields are missing or not valid. (Member States)". For 2.4.1, "Support until" is proposed five years after the market date ("Proposed: 5 years after it went on the market.") and the status is "Supported". Version 2.4.0 is refused until the reason is given ("reason for a shorter support"), then saved with it. Both versions show "No SBOM".		
OQ-03 Import an SBOM and search a component	On version 2.4.1, press "Import SBOM" and drop an SBOM exported as XML. Then use "choose a file" to select a CycloneDX (1.x) or SPDX (2.x or 3.0) JSON SBOM of that version that contains lodash 4.17.20, and press "Save this SBOM". Open the SBOM with "View" and type lodash in "Filter components…". In "Products", under "Which products contain…", type lodash < 4.17.21 and press "Search". Under "History of this product", press "Show".	The XML file is refused with "This is an XML file. Export the SBOM as JSON (CycloneDX or SPDX).". The JSON file is read as format, version and component count (for example "CycloneDX 1.5 · 312 components (25 direct)"), with file name, size and the product it describes (a warning if it describes another version); "SBOM saved: N components" appears. The SBOM view lists lodash with its version, type and "Direct", and shows the "SHA-256 of the file". The search returns "1 match in 1 version" (Gateway Console 2.4.1) marked "In		

Test	Steps	Expected result	Result (pass / fail)	Tester, date
		range", with "Open a case for 1 version". The history shows "SBOM imported" with version, format and count.		
OQ-04 Open a case from a work item	In the test project, create a work item with summary "[Snyk] High severity - Prototype Pollution in lodash" and description "CVE-2020-8203. Vulnerable versions: < 4.17.21". Open its "CRA" panel and press "Open a case". Under "Products and versions affected", press "Add them" (or pick 2.4.1 by hand); keep "Owner" = User A; press "Open the case". Reload the work item.	The panel offers "Open a CRA case on [key]" and the form shows "Read from the Snyk work item: check before saving.", with "Title", "Identifiers" (CVE-2020-8203), "Severity" High, "Component" lodash and "Vulnerable versions" < 4.17.21 prefilled, "1 version contains this component: Gateway Console 2.4.1", and a "Fix target date" with "Proposed: 30 days for this severity.". "CRA-0001 opened" appears; the panel now shows the case at step "Qualification" with "Qualify it", and no longer offers to open another case. "Vulnerabilities" lists CRA-0001.		
OQ-05 Qualify, sign and start the clocks	As User A, on CRA-0001 under "Qualification": "Are the products listed affected?" = "Affected"; "Is it actively exploited?" = "Yes"; in "When did you become aware of it?", enter a date and time 30 hours before now; fill "Why"; press "Qualify and sign". Read the statement, type the correct password in "Signing password" and press "Sign".	Before signing, "Reportable under Article 14: the clocks start." appears and the hint shows Early warning = awareness + 24 h and Notification = awareness + 72 h. After signing, the qualification shows the signature: User A's name, "Qualification", date and time, the statement "I qualify CRA-0001 as an actively exploited vulnerability in the products listed. It is reported under Article 14 of the Cyber Resilience Act." and the SHA-256 fingerprint. Three clocks appear: "Early warning" "Late" (due awareness + 24 h, with UTC time), "Notification" "Open" (due awareness + 72 h, about 42 h left), "Final report" "Not started" ("Starts when the fix or mitigation is available."). "History" shows "Qualified (signed) · Art. 14".		
OQ-06 Wrong signing password and lock-out	On CRA-0001, press "Qualify again", keep the answers, write a new "Why" and press "Qualify and sign". Press "Sign" with a wrong password twice, then a third time; then with the correct password. Wait 5 minutes (the lock set in test 1) and sign again with the correct password.	The first two attempts show "Wrong signing password." and nothing is recorded. The third shows "Signing is locked for a few minutes after too many attempts.", and the correct password is refused with the same message while the lock lasts. After 5 minutes the signature is accepted: "History" shows "Qualified again (signed) · Art. 14", the qualification shows "1 earlier qualification", and the three due times are unchanged.		
OQ-07 ENISA fields and reports recorded as submitted	On CRA-0001, under "Reporting to ENISA", open the "Notification" tab, then the "Early warning" tab. Check the required fields, open "+ … optional fields", edit "Summary" and press "Save the text". Press "Copy" on one field and "Copy all fields", and paste into a text editor. Set "Submitted on the platform at" to now, fill "Platform reference" and press "Record as submitted". Record the "Notification" the same way. Press "Show the text sent".	Before the early warning is recorded, the Notification tab shows "Record the early warning first.". Required fields carry ENISA's labels and are prefilled from the case and the product: "Notification type" (Vulnerability), "Title", "Summary", "Member States where the product is available", "Product name", "Product version" (2.4.1) and "Date and time when you become aware (UTC)"; each shows characters used / limit. "Text saved" appears; the pasted text holds each label and value. After recording: "Submitted [date time] ([UTC]) · recorded by User A · [reference]" with "… late" for the early warning and "on time" for the notification, and a SHA-256; the clocks show "Submitted late" and "Submitted". "History" shows "Report submitted · Early warning (submitted late)" and "Report submitted · Notification"; "Show the text sent" shows exactly the recorded fields.		
OQ-08 Fix, final report and users informed	On CRA-0001, open the "Final report" tab. Under "Fix or mitigation", press "Record the fix": "What is available" = "Security update", "Fixed version" = 2.4.2, "Available to users since" = now, fill "What it changes" and "Link for users", press "Record the fix". Without leaving the "Final report" tab, look at "Date when corrective or mitigating measure has been available" and	Before the fix, the Final report tab shows "Record the fix first: the final report describes it.". After it: "Fix recorded", step "Disclosure", and the "Final report" clock due exactly 14 days after "Available to users since"; in the open tab, the fields taken from the fix are filled in at once (the date in UTC, "Version 2.4.2. …"). While a required field is empty, "1 required field is empty or too long." is		

Test	Steps	Expected result	Result (pass / fail)	Tester, date
	"Details about the security update or corrective measure available". Fill "Date and time when it occurred (UTC)" only, leaving "Full description of the impact" empty, and look at "Record as submitted"; then fill "Full description of the impact" and press "Record as submitted". Under "Users and advisory" › "Users informed", press "Record", fill "Informed at" and "How", read "What they were told", press "Record".	shown and "Record as submitted" is greyed out (a report with an empty required field is also refused by the app's server). Once recorded, the clock shows "Submitted" and the fix shows "The final report was submitted with this fix: it can no longer change." (no "Edit"). "What they were told" is prefilled with the product, version, "Update to version 2.4.2 or later." and the security contact; the record shows date, channel and "recorded by User A". "History" shows "Fix available", "Report submitted · Final report" and "Users informed".		
OQ-09 Severe incident clocks and owner reminder	As User A, press "New case": "Kind" = "Incident", "Work item" = "Create one" (test project, any "Work item type"), fill "Title" and "What is known", pick Gateway Console 2.4.1, "Owner" = User B; press "Open the case". Qualify: "Affected", "Is the incident severe?" = "Yes", "Is it suspected to come from unlawful or malicious acts?" = "Unknown", awareness 30 hours ago, "Why"; sign. Record no report. The next day after 09:00 UTC, check User B's mailbox and the case "History". Then, as User B, record the "Early warning" and the "Notification" as submitted now.	Before the notification is recorded, the "Final report" clock shows "Not started" ("Starts when the notification is submitted."); the early warning fields include "Incident is suspected of unlawful or malicious acts" = Unknown. User B receives one e-mail from Jira, "Clearlane CRA: 1 case needs you", naming the case with "Early warning late since [date] UTC" and a link; nothing is posted on the work item, and no second reminder arrives that day. "History" shows "Reminder e-mail sent · early warning late". After the notification is recorded, the final report is due exactly one calendar month after the notification's submission time.		
OQ-10 CSAF advisory	On CRA-0001, under "Users and advisory" › "Security advisory", pick "EN" as "Advisory language" and press "Preview". Press "Record a publication", fill "What changed" and "Where it is published", press "Record the publication", then "Download the CSAF file". Open the work item's attachments and the downloaded file (optionally in a CSAF 2.0 validator).	The preview shows the affected product and versions, fixed version, severity, identifiers, "This vulnerability is actively exploited.", what to do and the contact. "Revision 1 published on [date] · Attached to [key]" appears; the work item has cra-0001.json; the revision line shows the summary, URL, User A and a SHA-256. The file is a CSAF 2.0 security advisory ("csaf_version": "2.0", tracking id CRA-0001, publisher = the manufacturer's name and website) listing 2.4.1 as known affected and 2.4.2 as fixed, a vendor fix and the exploit status. "History" shows "Advisory published".		
OQ-11 Permissions	As User A, press "New case", choose "Use an existing one", pick a work item of a project User B cannot browse and press "Open the case". As User B (not in the security team), open Apps › Clearlane CRA › "Vulnerabilities", choose "All" and type that case number in the search field. As User B, open CRA-0001 and then "Products".	User B does not see the case on the hidden work item: it is not listed and the search shows "No case matches these filters.". On CRA-0001, User B sees "Read only: the owner and the security team change this case.", with no "Qualify again", no "Close and sign" and no field to edit. In "Products", User B has no "Add a product" and sees "SBOMs are only visible to the security team.".		

Test	Steps	Expected result	Result (pass / fail)	Tester, date
OQ-12 Closure, evidence file and audit trail	As User A, on CRA-0001 check the “Closure” list, press “Close and sign”, fill “Note” and sign with the correct password. Press “Evidence file (PDF)” and open the file. Press “Attach PDF to the work item”. In “History”, press “Show all”.	Every item of the list is ticked (“Fix or mitigation”, “Early warning”, “Notification”, “Final report”, “Users informed”, “Advisory published (or delay recorded)”). After signing: “Fixed · closed on [date]”, and the closure signature shows name, “Closure”, date and time, the statement “I confirm that the handling of CRA-0001 is complete as recorded: corrective or mitigating measure, reports, information of users and advisory. I close this case.” and its SHA-256; nothing can be edited any more. The PDF “CRA case evidence file” holds the case data, products and versions with market date, support end and Member States, the qualification, each report (due and submitted in UTC, reference, timeliness, SHA-256, text submitted), fix, users informed, advisory revisions, electronic signatures, work item attachments and audit trail, with “Generated … by … · Clearlane CRA” and page numbers. “Attached to [key]” appears. “History” lists every step recorded on CRA-0001 (tests 4 to 8, 10 and 12) with date, time and person; no entry can be edited or deleted.		

Template provided by Clearlane to support your validation. Adapt it to your intended use and procedures. clearlaneapps.com/validation/