CompliVerse AI

Sample · fictional data

SECURITY ASSESSMENT REPORT

Example Bank

Vulnerability assessment and penetration test · Q4 2026

Engagements ENG-2026-014 (external and internal vulnerability assessment) and ENG-2026-015 (web application and API penetration test)

10	3	3	1
findings	critical on the asset	listed in CISA KEV	past its SLA

PREPARED FOR
Chief Information Security Officer, Example Bank

PREPARED BY
CompliVerse security team · engagement lead

ASSESSMENT PERIOD
2 – 13 November 2026

REPORT DATE
14 November 2026 · version 1.0

CLASSIFICATION
Confidential (sample)

DOMAIN
example-bank.sa

Sample · fictional data. Example Bank, example-bank.sa, every asset, address, finding, ticket, date and role in this report are fictional. CVE identifiers are real; the CVSS, EPSS and KEV values shown are illustrative and do not reflect current feeds.

1 · SCOPE AND AUTHORISATION

What was tested, under whose authority.

AUTHORISED BY
Chief Information Security Officer, Example Bank
Signed 30 October 2026 · authorisation ref. AUTH-2026-031

COUNTER-SIGNED
Engagement lead, CompliVerse
Signed 30 October 2026

SCOPE CHANGE
api.example-bank.sa /v2/* added
Written approval 2, 11 November 2026

In scope

ASSET	WHAT IT IS	HOW IT WAS ASSESSED
vpn.example-bank.sa	Remote access gateway · internet-facing	Hosted Nessus scan, external
www.example-bank.sa	Online banking web app · internet-facing	Nessus; manual web testing (ENG-2026-015)
api.example-bank.sa	Mobile banking API · internet-facing	Manual API testing (ENG-2026-015); external surface probe
rpt-app-03 · 10.20.6.14	Legacy reporting server · internal	Rapid7 InsightVM import
jump-host-01 · 10.20.1.5	Admin jump host · internal	Credentialed Nessus scan; CIS Ubuntu checks
core-bank-db-01 · 10.20.4.11	Core banking database · internal	Nessus, non-intrusive policy, agreed window
prod-payments	AWS account · cloud	AWS Inspector import; CIS AWS Foundations checks
Microsoft Entra ID	Directory · cloud	Access Reviews rules

Out of scope: the third-party payment gateway; denial-of-service testing; social engineering; physical testing. core-bank-db-01 was scanned with a non-intrusive policy only and was excluded from manual testing.

Rules of engagement

Signed authorisation	Signed by the client's accountable executive before any active test. No signature, no test.	Signed 30 Oct 2026
A written scope	Hosts, applications and APIs listed by name, address or path. Anything not on the list is out of scope.	3 hosts · 2 apps · 1 API
Agreed testing windows	Active testing runs only inside the windows agreed in writing.	Sun–Thu, 22:00–04:00 AST
Non-destructive by default	No denial of service, no data changes, proof-only checks. Anything intrusive needs its own written approval.	Intrusive tests approved: none
Rate limits	Request rates agreed per target, and set low for production.	At most 10 requests a second per host
A named stop contact and procedure	A named contact on each side can stop testing at any time. Testers halt on the call and confirm in writing.	Client: Head of IT Operations · Ours: engagement lead
Every action recorded	Testers log each action with its time, target and result. The platform's audit trail records every change to scope, findings and evidence.	Engagement log + platform audit trail

Who did what: scanner imports, enrichment, scoring, CIS checks and access rules ran in the CompliVerse platform. Manual web and API testing, validation and this report's narrative were done by the CompliVerse security team.

2 · EXECUTIVE SUMMARY

Three findings are critical where they sit. Fix the reporting server first.

3
critical on the asset, by the effective-risk formula

1
past its SLA: Log4Shell on the reporting server

1
fixed and verified by a re-run

1
proven by hand by our team

What matters

1. **Three findings are critical once the asset and threat data are counted.** The remote access gateway (CVE-2024-3400) and the legacy reporting server (Log4Shell) score critical outright; the web tier's HTTP/2 rapid-reset flaw is raised to critical because it is listed in CISA KEV on a customer-facing asset.
2. **The reporting server is two days past its 7-day SLA.** The fix (Log4j 2.17.1 or later) is approved and ticketed; until it lands, remove the JndiLookup class.
3. **The gateway fix is applied but not yet verified.** A re-scan is booked; the finding closes only when the scanner no longer detects it.
4. **Our team proved one serious API flaw.** One customer could read another customer's account through GET /v2/accounts/{id}. A fix is in progress and a retest is booked.
5. **Two high CVSS scores rank lower on their assets.** regreSSHion on the internal jump host scores medium and SWEET32 on the core banking database scores low: neither is known to be exploited, and both sit inside the network. The SWEET32 exception runs to 31 March 2027.

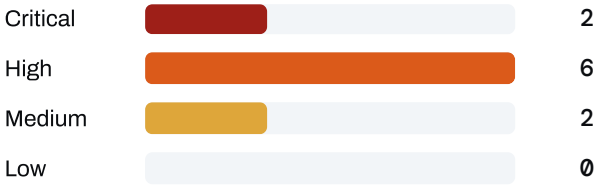
Do these first

#	FINDING	ACTION	OWNER	DUE
1	F-103 Log4j remote code execution (Log4Shell)	Upgrade Log4j to 2.17.1 or later on rpt-app-03	Applications manager	11 Nov · late
2	F-101 OS command injection in the remote access gateway	Apply the vendor hotfix for CVE-2024-3400 on the gateway, then rotate the credentials it holds.	Network security lead	11 Nov
3	F-102 HTTP/2 rapid reset denial of service on the web tier	Apply the web server vendor's HTTP/2 rapid-reset mitigations and cap concurrent streams per connection.	Web platform owner	4 Dec
4	F-109 Broken object-level authorisation on GET /v2/accounts/{id}	Check that the account belongs to the signed-in customer on every object lookup.	Mobile API owner	4 Dec
5	F-110 Privileged account without MFA (PRIV-05)	Register MFA for the account, or remove the privileged role.	Identity and access manager	4 Dec

3 · SEVERITY DASHBOARD

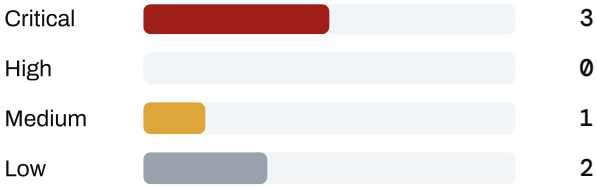
The same ten findings, two ways of ranking them.

BY SEVERITY · SCANNER OR TESTER



All 10 findings, as the scanner, the rule or the tester rated them.

BY EFFECTIVE RISK ON THE ASSET



The 6 findings with a CVE, scored by the fixed formula. The other 4 keep their severity.

STATUS



Open 4 · In progress 3 · Resolved 2 · Accepted 1

BY ASSET · HIGHEST EFFECTIVE RISK

ASSET	FINDINGS	HIGHEST
vpn.example-bank.sa	1	Critical 0.88
rpt-app-03 · 10.20.6.14	1	Critical 0.88
www.example-bank.sa	1	Critical 0.85
jump-host-01 · 10.20.1.5	2	Medium 0.45
core-bank-db-01 · 10.20.4.11	1	Low 0.39
api.example-bank.sa	2	No CVE
prod-payments	1	No CVE
Microsoft Entra ID	1	No CVE

THREAT SNAPSHOT

3 listed in CISA KEV

3 EPSS of 0.7 or more

5 with a public exploit (Exploit-DB or GitHub)

1 past its SLA

SLA by severity, set on import: critical 7 days, high 30, medium 90, low 180.

READING THE TWO RANKINGS

F-102 is rated high by its scanner but ranks critical on the asset: it is KEV-listed on a high-value, customer-facing system, so the formula's escalation floor applies. F-104 and F-105 carry high CVSS scores but rank medium and low: low exploit probability, not known to be exploited, reachable only inside the network.

4 · FINDINGS

Every finding, with CVSS, EPSS and KEV.

ID	FINDING · ASSET	SOURCE	CVSS	EPSS	KEV	EFFECTIVE RISK	SEVERITY	STATUS	DUE
F-101	**OS command injection in the remote access gateway** vpn.example-bank.sa · CVE-2024-3400	Tenable Nessus	10.0	0.94	Yes	Critical 0.88	Critical	Resolved	11 Nov
F-102	**HTTP/2 rapid reset denial of service on the web tier** www.example-bank.sa · CVE-2023-44487	Tenable Nessus	7.5	0.82	Yes	Critical 0.85	High	In progress	4 Dec
F-103	**Log4j remote code execution (Log4Shell)** rpt-app-03 · 10.20.6.14 · CVE-2021-44228	Rapid7 InsightVM	10.0	0.94	Yes	Critical 0.88	Critical	In progress	11 Nov late
F-104	**OpenSSH signal handler race (regreSSHion)** jump-host-01 · 10.20.1.5 · CVE-2024-6387	Tenable Nessus	8.1	0.38	No	Medium 0.45	High	Open	4 Dec
F-105	**SWEET32: 64-bit block ciphers offered on TLS** core-bank-db-01 · 10.20.4.11 · CVE-2016-2183	Tenable Nessus	7.5	0.02	No	Low 0.39	High	Accepted	31 Mar 2027
F-106	**SSH prefix truncation (Terrapin)** jump-host-01 · 10.20.1.5 · CVE-2023-48795	Tenable Nessus	5.9	0.05	No	Low 0.30	Medium	Open	2 Feb 2027
F-107	**TLS 1.0 and 1.1 still enabled** api.example-bank.sa	External surface probe	–	–	No	No CVE	Medium	Open	2 Feb 2027
F-108	**AWS root user has no MFA (CIS AWS 1.5)** prod-payments	CIS AWS Foundations v3.0	–	–	No	No CVE	High	Resolved	4 Dec
F-109	**Broken object-level authorisation on GET /v2/accounts/{id}** api.example-bank.sa	Our team · manual test	–	–	No	No CVE	High	In progress	4 Dec
F-110	**Privileged account without MFA (PRIV-05)** Microsoft Entra ID	Access Reviews	–	–	No	No CVE	High	Open	4 Dec

CVSS is the scanner's score, kept beside NVD's; EPSS is FIRST.org's exploit probability; KEV means listed in CISA's Known Exploited Vulnerabilities catalogue. Effective risk applies to findings with a CVE; the formula is in the appendix. Values are illustrative.

4 · FINDINGS IN DETAIL

The three critical findings.

F-101 **OS command injection in the remote access gateway** — EFFECTIVE RISK Critical 0.88 — SEVERITY Critical

ASSET	CVE · CWE	CVSS
vpn.example-bank.sa · Remote access gateway	CVE-2024-3400 · CWE-77	10.0 scanner · 10.0 NVD
EPSS · KEV	**PUBLIC EXPLOIT**	**FOUND BY**
0.94 · Listed	Exploit-DB · GitHub PoC	Tenable Nessus

OS command injection in the gateway's VPN portal lets an unauthenticated attacker run commands with root privileges.

Why it ranks here. Critical: maximum CVSS, very likely to be exploited, listed in CISA KEV, on an internet-facing gateway.

`0.30 × 1.00 + 0.25 × 0.94 + 0.20 × 1.00 + 0.10 × 1.00 + 0.15 × 0.30 = 0.880`

Evidence. Version banner and plugin output from the hosted Nessus scan; vendor advisory reference.

Recommendation. Apply the vendor hotfix for CVE-2024-3400 on the gateway, then rotate the credentials it holds.

Owner: Network security lead · Status: Resolved · Plan: Applied · Due: 11 Nov · ServiceNow INC0048202

F-103 **Log4j remote code execution (Log4Shell)** — EFFECTIVE RISK Critical 0.88 — SEVERITY Critical

ASSET	CVE · CWE	CVSS
rpt-app-03 · 10.20.6.14 · Legacy reporting server	CVE-2021-44228 · CWE-502	10.0 scanner · 10.0 NVD
EPSS · KEV	**PUBLIC EXPLOIT**	**FOUND BY**
0.94 · Listed	Exploit-DB · GitHub PoC	Rapid7 InsightVM

JNDI lookups in Log4j 2 let anyone who controls a logged string load and run remote code on the reporting server.

Why it ranks here. Critical: maximum CVSS, very likely to be exploited, listed in CISA KEV, on a server holding regulated data.

`0.30 × 1.00 + 0.25 × 0.94 + 0.20 × 1.00 + 0.10 × 0.80 + 0.15 × 0.40 = 0.875`

Evidence. Vulnerable library version found by Rapid7 InsightVM; path to the JAR file.

Recommendation. Upgrade Log4j to 2.17.1 or later on rpt-app-03; until then, remove the JndiLookup class.

Owner: Applications manager · Status: In progress · Plan: Approved · Due: 11 Nov · ServiceNow INC0048207

F-102 **HTTP/2 rapid reset denial of service on the web tier** — EFFECTIVE RISK Critical 0.85 — SEVERITY High

ASSET	CVE · CWE	CVSS
www.example-bank.sa · Online banking web app	CVE-2023-44487 · CWE-400	7.5 scanner · 7.5 NVD
EPSS · KEV	**PUBLIC EXPLOIT**	**FOUND BY**
0.82 · Listed	GitHub PoC	Tenable Nessus

Rapid stream resets over HTTP/2 let an attacker exhaust the web tier's resources: a denial of service against online banking.

Why it ranks here. Escalated to critical: listed in CISA KEV and likely to be exploited, on a high-value customer-facing asset.

`0.30 × 0.75 + 0.25 × 0.82 + 0.20 × 1.00 + 0.10 × 1.00 + 0.15 × 0.40 = 0.790 → escalation floor 0.850`

Evidence. HTTP/2 enabled on the web tier; server version from the Nessus scan.

Recommendation. Apply the web server vendor's HTTP/2 rapid-reset mitigations and cap concurrent streams per connection.

Owner: Web platform owner · Status: In progress · Plan: Approved · Due: 4 Dec · ServiceNow INC0048213

4 · FINDINGS IN DETAIL

The API flaw, and two high CVSS scores that rank lower.

F-109 Broken object-level authorisation on GET /v2/accounts/{id}

EFFECTIVE RISK No CVE · SEVERITY High

ASSET	CVE · CWE	CVSS
api.example-bank.sa · Mobile banking API	— · CWE-639	Tester: 8.1
EPSS · KEV	**PUBLIC EXPLOIT**	**FOUND BY**
— · Not listed	Proven by our team	Our team · manual test

The API returns any account whose number is supplied, without checking that it belongs to the signed-in customer.

Why it ranks here. Found by hand, so no effective-risk score: severity set by the tester (CVSS 8.1).

Evidence. Request and response pair: test customer A's token read test customer B's account.

Recommendation. Check that the account belongs to the signed-in customer on every object lookup.

Owner: Mobile API owner · Status: In progress · Plan: Approved · Due: 4 Dec · ServiceNow INC0048215

F-104 OpenSSH signal handler race (regreSSHion)

EFFECTIVE RISK Medium 0.45 · SEVERITY High

ASSET	CVE · CWE	CVSS
jump-host-01 · 10.20.1.5 · Admin jump host	CVE-2024-6387 · CWE-364	8.1 scanner · 8.1 NVD
EPSS · KEV	**PUBLIC EXPLOIT**	**FOUND BY**
0.38 · Not listed	GitHub PoC	Tenable Nessus

A signal-handler race in the OpenSSH server can allow unauthenticated remote code execution as root on glibc-based Linux.

Why it ranks here. Medium: a high CVSS, but a moderate chance of exploitation, not known exploited, on an internal admin host.

0.30 × 0.81 + 0.25 × 0.38 + 0.20 × 0.00 + 0.10 × 0.80 + 0.15 × 0.20 = 0.448

Evidence. OpenSSH version banner from the credentialed Nessus scan.

Recommendation. Upgrade OpenSSH to 9.8p1 or later on jump-host-01.

Owner: Infrastructure lead · Status: Open · Plan: Recommended · Due: 4 Dec

F-105 SWEET32: 64-bit block ciphers offered on TLS

EFFECTIVE RISK Low 0.39 · SEVERITY High

ASSET	CVE · CWE	CVSS
core-bank-db-01 · 10.20.4.11 · Core banking database	CVE-2016-2183 · CWE-200	7.5 scanner · 7.5 NVD
EPSS · KEV	**PUBLIC EXPLOIT**	**FOUND BY**
0.02 · Not listed	None found	Tenable Nessus

64-bit block ciphers such as 3DES let an attacker on the network path recover plaintext from long-lived encrypted sessions.

Why it ranks here. Low: a high CVSS, but very unlikely to be exploited and reachable only inside the network.

0.30 × 0.75 + 0.25 × 0.02 + 0.20 × 0.00 + 0.10 × 1.00 + 0.15 × 0.40 = 0.390

Evidence. Cipher suites offered by the database listener.

Recommendation. Remove 3DES cipher suites once the legacy client is retired; exception approved until then.

Owner: Database administrator · Status: Accepted · Plan: Exception · Due: 31 Mar 2027

F-106 SSH prefix truncation (Terrapin) · **F-107** TLS 1.0 and 1.1 still enabled · **F-108** AWS root user has no MFA (CIS AWS 1.5) · **F-110** Privileged account without MFA (PRIV-05): see the findings table and the remediation plan.

5 · REMEDIATION PLAN

Who fixes what, by when, and how we know it worked.

PRIORITY	FINDING	ACTION	OWNER	DUE	PLAN	TICKET
P1	F-103 Log4j remote code execution (Log4Shell)	Upgrade Log4j to 2.17.1 or later on rpt-app-03; until then, remove the JndiLookup class.	Applications manager	11 Nov late	Approved	INC0048207
P1	F-101 OS command injection in the remote access gateway	Apply the vendor hotfix for CVE-2024-3400 on the gateway, then rotate the credentials it holds.	Network security lead	11 Nov	Applied	INC0048202
P1	F-102 HTTP/2 rapid reset denial of service on the web tier	Apply the web server vendor's HTTP/2 rapid-reset mitigations and cap concurrent streams per connection.	Web platform owner	4 Dec	Approved	INC0048213
P1	F-109 Broken object-level authorisation on GET /v2/accounts/{id}	Check that the account belongs to the signed-in customer on every object lookup.	Mobile API owner	4 Dec	Approved	INC0048215
P2	F-110 Privileged account without MFA (PRIV-05)	Register MFA for the account, or remove the privileged role.	Identity and access manager	4 Dec	Recommended	–
P2	F-104 OpenSSH signal handler race (regreSSHion)	Upgrade OpenSSH to 9.8p1 or later on jump-host-01.	Infrastructure lead	4 Dec	Recommended	–
P2	F-106 SSH prefix truncation (Terrapin)	Covered by the OpenSSH upgrade in F-104.	Infrastructure lead	2 Feb 2027	Recommended	–
P3	F-107 TLS 1.0 and 1.1 still enabled	Allow TLS 1.2 and 1.3 only on the API gateway.	Mobile API owner	2 Feb 2027	Recommended	–
Done	F-108 AWS root user has no MFA (CIS AWS 1.5)	Enable a hardware MFA device on the root user; re-run the check.	Cloud platform lead	4 Dec	Verified	INC0048198
Exception	F-105 SWEET32: 64-bit block ciphers offered on TLS	Remove 3DES cipher suites once the legacy client is retired; exception approved until then.	Database administrator	31 Mar 2027	Exception	–

HOW A FIX IS VERIFIED

1. The owner approves the fix plan; your team applies it.
2. A resolved ServiceNow ticket marks the plan **applied**, never verified.
3. A re-scan, or a re-run of the check, that no longer detects the issue marks it **verified**.
4. Our team retests manual findings (F-109) and signs off the retest.

EXCEPTION ON RECORD

F-105 · SWEET32 on core-bank-db-01. Approved by the Chief Information Security Officer until 31 March 2027. Compensating control: the listener is reachable only inside the network. Revisit when the legacy client is retired.

APPENDIX

Method, formula and definitions.

Sources and enrichment

Findings were imported from Tenable Nessus (including a hosted scan), Rapid7 InsightVM and AWS Inspector, and from CIS AWS Foundations and CIS Ubuntu checks and Access Reviews rules. Each CVE was enriched with NVD, FIRST.org EPSS and CISA KEV (refreshed daily), Exploit-DB (weekly) and GitHub proof-of-concept counts.

Effective risk

```
0.30 × CVSS/10 + 0.25 × EPSS + 0.20 × KEV +
0.10 × asset value + 0.15 × (business impact −
1)
```

Asset value is the asset's CIA rating out of 5. Business impact is the worst that applies: customer-facing 1.2, internet-facing 1.3, regulated data 1.4, operational dependency 0.8 to 1.5. **Escalation:** an EPSS of 0.7 or more, or a KEV listing, on a high-value asset floors the score at 0.85. **Bands:** low below 0.40, medium below 0.70, high below 0.85, critical from 0.85. It is a fixed formula, not AI.

Severity and SLA

Severity is the scanner's, the rule's or the tester's rating. SLA due dates are set on import by severity: critical 7 days, high 30, medium 90, low 180.

Who did what

Platform: imports, enrichment, scoring, CIS checks, access rules, findings register, fix plans, tickets and this report's data. **Our team:** scoping and rules of engagement, manual web and API testing, validation, the narrative and the recommendations.

Use of AI

No AI produced a score in this report. AI mapped findings to the bank's controls (automatic above the confidence floor; weaker suggestions reviewed by a person) and drafted fix plans that owners approved. AI prompts pass through the platform's data-protection gateway.

Glossary

CVSS	Common Vulnerability Scoring System, 0 to 10.
EPSS	Exploit Prediction Scoring System: the probability of exploitation in the next 30 days.
KEV	CISA's catalogue of vulnerabilities known to be exploited.
CWE	Common Weakness Enumeration: the kind of flaw.
BOLA	Broken object-level authorisation: reading or changing another user's object.

Sample · fictional data. This sample shows the shape of a CompliVerse assessment report. The bank, domain, assets, addresses, findings, tickets, dates and roles are invented; the CVE identifiers are real but their CVSS, EPSS and KEV values here are illustrative.