CYBER ESSENTIALS READINESS REPORT

Example GmbH

PERIOD	DOMAINS	HOSTS	CREATED ON
23/06/2026 – 21/09/2026	1	8	14/10/2026

This report maps the externally visible findings of Example GmbH to the five technical controls of Cyber Essentials, the certification scheme of the UK NCSC (requirements v3.3, “Danzell” question set, valid since 27 April 2026). It shows where action is already visible from outside and what you still need to evidence internally. veyrisk does not certify.

1. Overview

4 open findings would likely lead to a fail. Fix them before you submit your self-assessment.

CONTROL	STATUS	OPEN FINDINGS	LIKELY FAIL
Firewalls	FINDINGS OPEN	3	2
Secure configuration	FINDINGS OPEN	5	0
Security update management	FINDINGS OPEN	1	1
User access control	FINDINGS OPEN	1	1
Malware protection	CANNOT BE ASSESSED FROM OUTSIDE	0	0

2. Firewalls

FINDINGS OPEN

What veyrisk checks from outside

Only the services you need may be reachable from the internet. veyrisk checks open ports (only with ownership proof), publicly reachable admin interfaces, and development and test systems.

SEVERITY	FINDING	OPEN FOR (DAYS)	NOTE

HIGH	vpn.example.com RDP reachable from the internet (port 3389)	38	HIGH OR CRITICAL AND OPEN FOR MORE THAN 14 DAYS
HIGH	shop.example.com Admin interface publicly reachable (phpMyAdmin)	61	HIGH OR CRITICAL AND OPEN FOR MORE THAN 14 DAYS
MEDIUM	dev.example.com Development or test system publicly reachable	61	

To evidence internally

- A firewall at every internet boundary, with its default password changed
- Every inbound rule documented and justified, rules no longer needed removed
- A software firewall on devices used on untrusted networks such as public Wi-Fi

3. Secure configuration

FINDINGS OPEN

What veyrisk checks from outside

Devices and services are hardened: no unnecessary software, no default accounts, secure settings. veyrisk checks certificates, TLS, HTTPS, security headers and version disclosure, plus configuration findings from web app and cloud checks.

SEVERITY	FINDING	OPEN FOR (DAYS)	NOTE
MEDIUM	mail.example.com TLS certificate expires in 9 days	3	
MEDIUM	shop.example.com Missing Strict-Transport-Security header	90	
LOW	www.example.com Software version disclosed in Server header (Apache/2.4.49)	45	
LOW	www.example.com Missing Content-Security-Policy header	90	
LOW	portal.example.com Missing X-Content-Type-Options header	90	

To evidence internally

- Unneeded software, services and user accounts removed or disabled

- Default passwords changed, auto-run disabled
- Device locking with a PIN, password or biometrics on every device

4. Security update management

FINDINGS OPEN

What veyrisk checks from outside

All software is licensed and still supported by the vendor. Critical and high-risk updates must be installed within 14 days of release. veyrisk uses Advanced Vulnerability Detection findings and web app findings with a CVE for this.

SEVERITY	FINDING	OPEN FOR (DAYS)	NOTE
HIGH	vpn.example.com OpenSSH 'regreSSHion' Remote Code Execution Vulnerability (22/tcp)	26	HIGH OR CRITICAL AND OPEN FOR MORE THAN 14 DAYS

To evidence internally

- An inventory of all in-scope devices with operating system and version
- Only supported operating systems and applications in use, unsupported ones removed or segregated
- Automatic updates turned on where possible, otherwise proof of installation within 14 days

5. User access control

FINDINGS OPEN

What veyrisk checks from outside

Accounts are only created when needed, and admin rights are used through separate accounts. MFA is mandatory on every cloud service that offers it; without it the assessment fails automatically. Passkeys count as passwordless sign-in. veyrisk only sees this in connected cloud and Microsoft 365 accounts.

SEVERITY	FINDING	OPEN FOR (DAYS)	NOTE
HIGH	Microsoft 365 (example.com) Ensure multifactor authentication is enabled for all users	9	MFA MISSING: AUTOMATIC FAIL

To evidence internally

- MFA for all users on every cloud service that offers it
- Separate admin accounts that are not used for email or web browsing

- A defined process for creating and removing accounts, with regular reviews of access rights
- Password rules or passwordless sign-in with passkeys, protection against brute-force attacks

6. Malware protection

CANNOT BE ASSESSED FROM OUTSIDE

What veyrisk checks from outside

Malware protection runs on every in-scope device. This cannot be checked from outside.

Malware protection cannot be checked from outside.

To evidence internally

- Anti-malware software with current signatures on every device, or application allow-listing
- Files scanned on access and protection against malicious websites

7. Notes and limitations

This report is a readiness check from the outside and not a certification. veyrisk does not certify. Cyber Essentials and Cyber Essentials Plus are awarded only by IASME-licensed certification bodies; Cyber Essentials Plus adds technical testing. The certificate is valid for 12 months.

The scope covers all internet-connected devices and all cloud services. veyrisk only sees the publicly reachable systems of your domains and connected cloud accounts. Malware protection and most of access control cannot be checked from outside.

The mapping of findings to controls is veyrisk's assessment. Findings on email authentication (SPF, DMARC, MTA-STS) belong to none of the five controls and are not shown here. The NCSC requirements and your certification body's assessment are what count.

VEYRISK · NEONOTU GMBH

Edelsbergstraße 8, 80686 München · +49 89 2000 7975 0 · contact@veyrisk.com