Torchsec Technologies
Revolutionary Managed Services

TRUST CENTER · PUBLIC ARTIFACT

NIST CSF 2.0 Shared Responsibility Matrix

Who owns which cybersecurity outcomes across the Torchsec-managed environment — mapped to the six functions of the NIST Cybersecurity Framework 2.0.

GV GOVERN | ID IDENTIFY | PR PROTECT | DE DETECT | RS RESPOND | RC RECOVER

Prepared for: **Prospective clients & security reviewers**

Revolutionary Managed Services

Torchsec.com
(380) 900-7099
info@torchsec.com
Centerburg, OH

HOW TO READ THIS DOCUMENT

The shared responsibility model

Security in a managed environment is a partnership. Torchsec operates, monitors, and maintains a broad security stack on your behalf — but certain decisions and actions remain with your organization. This matrix makes that split explicit for every function of NIST CSF 2.0, so your auditors, insurers, and leadership can see exactly where accountability sits.

- **Torchsec-led** — we own and operate this control
- **Shared** — joint responsibility; roles defined below
- **Client-owned** — your organization is accountable

> **Scope.** Responsibility splits reflect Torchsec's standard managed-services engagement. Coverage varies by service tier and by the controls in your executed service agreement. Where a client uses their own tooling (e.g., a pre-existing SIEM or backup platform), the corresponding row shifts toward **Client-owned** or **Shared**.

Govern GV — Organizational context, strategy & oversight

Establishing and monitoring the organization's cybersecurity risk-management strategy, expectations, and policy.

CONTROL AREA	OWNER	RESPONSIBILITY SPLIT	TORCHSEC TOOLING
Risk-management strategy GV.RM / GV.RR	SHARED	Torchsec advises on risk posture and control roadmap via vCIO/vSO reviews; client leadership sets risk appetite and approves the strategy.	myITprocess (vCIO findings, QBRs); Compliance Manager
Security policies & standards GV.PO	SHARED	Torchsec provides policy templates and maintains the technical control baseline; client formally adopts and enforces organizational policy.	IT Glue / MyGlue; Compliance Manager
Roles, responsibilities & authorities GV.RR	SHARED	Torchsec staffs the security operations roles (SOC, service delivery, vSO); client designates internal points of contact and approvers.	Autotask PSA (ownership + workflow)
Cybersecurity in supply chain (vendor risk) GV.SC	SHARED	Torchsec manages risk of the tools it operates and its own sub-processors; client owns risk decisions for their other third-party vendors.	Vendor review process; Dark Web ID (exposure)
Security awareness & training GV.RR-04 / PR.AT	TORCHSEC	Torchsec delivers ongoing awareness training and phishing simulation; client ensures staff participation.	BullPhish ID (training + phishing sim)
SaaS & AI acceptable-use governance GV.PO / GV.OC	SHARED	Torchsec provides AI/SaaS acceptable-use guidance and monitors sanctioned cloud identity activity; client approves which SaaS/AI tools are permitted.	SaaS Alerts; DNS Filter (shadow-IT visibility)

Identify ID — Asset management & risk assessment

Understanding assets, suppliers, and related cybersecurity risks to prioritize efforts.

CONTROL AREA	OWNER	RESPONSIBILITY SPLIT	TORCHSEC TOOLING
Asset inventory & discovery ID.AM	TORCHSEC	Continuous discovery and inventory of endpoints, network devices, and cloud identities in the managed estate; client informs us of new sites/systems.	Datto RMM; Auvik + Network Glue; SaaS Alerts
Data identification & classification ID.AM-07	SHARED	Torchsec discovers and locates sensitive/PII data; client defines what is sensitive and its handling requirements.	Actifile; Compliance Manager Discovery Agent (PII)
Risk assessment ID.RA	TORCHSEC	Torchsec conducts recurring security and network assessments and reports findings; client reviews and authorizes remediation.	Network Detective; RoboShadow; Compliance Manager
Vulnerability management lifecycle ID.RA-01 / -06	TORCHSEC	Torchsec scans, scores, prioritizes, and schedules remediation; client approves change windows for disruptive fixes.	Vulscan; RoboShadow; Datto RMM patching
Penetration testing ID.RA / PR validation	TORCHSEC	Torchsec runs managed internal/external testing on an agreed cadence; client authorizes scope and testing windows.	vPenTest (managed penetration testing)
Credential exposure monitoring ID.RA-02	TORCHSEC	Torchsec monitors the dark web for leaked client credentials and initiates response; client enforces resets when notified.	Dark Web ID

Protect

PR — Safeguards to manage risk

Using safeguards to prevent or reduce cybersecurity risk across identity, data, and platforms.

CONTROL AREA	OWNER	RESPONSIBILITY SPLIT	TORCHSEC TOOLING
Identity & access management PR.AA	SHARED	Torchsec configures and enforces MFA, SSO, and least-privilege baselines; client approves access requests and role assignments.	M365 / Google Workspace IAM; SaaS Alerts
Zero-trust network access PR.AA-05	TORCHSEC	Torchsec deploys and manages ZTNA for remote and internal access; client confirms who requires access.	Cytracom Control One (ZTNA)
Endpoint protection (EDR/XDR) PR.PS / DE.CM	TORCHSEC	Torchsec deploys and manages endpoint protection against fileless and script-based execution across all managed devices.	Datto AV; Datto EDR/MDR; ThreatLocker (allowlisting, ringfencing)
Application allowlisting & control PR.PS-01	TORCHSEC	Torchsec operates default-deny allowlisting, ringfencing, storage & network control, and privileged-elevation management.	ThreatLocker (Allowlisting, Ringfencing, Storage/Network Control, Elevation)
Data-at-rest encryption PR.DS-01	SHARED	Torchsec enforces disk/file encryption (AES-256) on managed endpoints and sensitive data stores; client owns encryption within their own SaaS/line-of-business apps.	BitLocker/FileVault management; Actifile (file-level)
Data-in-transit encryption PR.DS-02	TORCHSEC	Torchsec requires modern TLS (TLS 1.2+/1.3) for managed services and remote access.	Managed platform configuration
Email security & anti-phishing PR.PS / DE.CM	TORCHSEC	Torchsec deploys and tunes email threat protection; client reports suspicious messages via the help desk.	Avanan (Check Point); Inky
Web / DNS-layer protection PR.PS / DE.CM	TORCHSEC	Torchsec filters malicious domains and enforces web policy at the DNS layer.	DNS Filter
Patch & configuration management PR.PS-02 / -03	TORCHSEC	Torchsec patches OS and managed applications and enforces secure configuration baselines; client approves reboot/change windows.	Datto RMM; ThreatLocker Configuration Manager
Physical security of premises PR.AA-06	CLIENT	Client owns physical access controls to their facilities and on-premise equipment.	—

Detect DE — Continuous monitoring & analysis

Finding and analyzing possible cybersecurity attacks and compromises.

CONTROL AREA	OWNER	RESPONSIBILITY SPLIT	TORCHSEC TOOLING
Continuous security monitoring (SOC) DE.CM	TORCHSEC	Torchsec provides continuous, 24×7×365 logging, monitoring, and behavioral analysis through a managed SOC correlation layer.	RocketCyber (Managed SOC); Kaseya SIEM; Datto EDR/MDR
Endpoint telemetry & behavioral detection DE.CM-01	TORCHSEC	Torchsec ingests and analyzes endpoint telemetry for anomalies and early indicators of compromise.	Datto EDR/MDR; ThreatLocker Endpoint Detect
Network telemetry & anomaly detection DE.CM-06	TORCHSEC	Torchsec monitors network topology, performance, and anomalies across managed infrastructure.	Auvik; DNS Filter; Ubiquiti/UniFi management
Cloud & identity event monitoring DE.CM-03	TORCHSEC	Torchsec monitors M365/Google Workspace identity events (impossible travel, MFA fatigue, privilege changes).	SaaS Alerts; native M365 / Google Workspace logs
Alert triage & correlation DE.AE	TORCHSEC	Torchsec correlates alerts from all detection sources, triages severity, and escalates true positives into tickets.	Kaseya SIEM correlation; RocketCyber → Autotask PSA
Backup health monitoring DE.CM / PR.DS	TORCHSEC	Torchsec monitors backup success/failure and recoverability across endpoints, servers, and SaaS.	Datto BCDR; Spanning (M365); Datto File Protection

Respond & Recover RS / RC — Incident management & resilience

Taking action on detected incidents and restoring assets and operations affected by an incident.

CONTROL AREA	OWNER	RESPONSIBILITY SPLIT	TORCHSEC TOOLING
Incident response management RS.MA	TORCHSEC	Torchsec executes the IR plan — triage, severity classification, and coordination — per the documented runbooks; client authorizes business-impacting actions.	Autotask PSA; Torchsec Triage Framework
Containment & eradication RS.MI	TORCHSEC	Torchsec isolates affected endpoints, blocks malicious activity, and removes threats; client is notified and consulted on operational trade-offs.	Datto EDR/MDR (isolation); ThreatLocker; DNS Filter
Incident communications & reporting RS.CO	SHARED	Torchsec provides technical incident reporting and notification to designated contacts; client owns external/regulatory/legal notifications.	Autotask PSA; defined comms protocol
Backup & disaster recovery RC.RP	TORCHSEC	Torchsec maintains hourly backups and restores systems toward agreed RTOs of under 4 hours for critical systems.	Datto BCDR; Spanning; Datto Workplace
Immutable / air-gapped recovery points RC.RP-01	TORCHSEC	Torchsec maintains immutable, off-site recovery points protected from tampering and ransomware.	Datto BCDR (cloud + immutable)
Recovery communications & lessons learned RC.CO / RS.AN	SHARED	Torchsec leads the post-incident review and feeds improvements back into Govern/Identify; client participates and approves process changes.	myITprocess; IT Glue (runbook updates)
Business continuity planning RC.RP / BCDR	SHARED	Torchsec provides the technical recovery capability and BCDR framework; client owns the business-side continuity plan (staffing, facilities, priorities).	Datto BCDR; documented recovery runbooks

The bottom line: Torchsec operates the detection, protection, and response machinery around the clock. Your organization's responsibilities are deliberately narrow — set risk appetite, approve access and change windows, keep contacts current, and own physical security and external legal/regulatory notification. Everything else, we run.

Assumptions & exclusions

This matrix assumes devices and identities are enrolled in Torchsec's managed platforms and that the client maintains active service. Unmanaged (BYOD/shadow-IT) assets, client-retained third-party tools, and systems explicitly excluded from scope fall to the client. Specific coverage, cadences, and service levels are defined by tier and governed by the executed Torchsec service agreement.
