1. Vulnerability Assessment & Penetration Testing

Module	Fields (Scoring & Evidence)
Computers	**certificate_file** (Compliance Cert PDF) – *Evidence***certificate_status** (Verified/Missing) – *Scoring/Evidence* (device compliance status)
Security Measures	**document_reference** (Policy/Config Document PDF) – *Evidence* (e.g. vulnerability scan procedures or patch policy documents)

2. Threat Intelligence & Security Awareness

Module	Fields (Scoring & Evidence)
No dedicated module fields	*This category's scoring is based on qualitative assessment of threat intel usage and overall staff awareness.* (Note: **Staff training metrics** are covered under Card 8, and general security measures like threat intel programs would appear as part of **Implemented Security Measures**.)

3. Business Continuity

Module	Fields (Scoring & Evidence)

Business Continuity	**plan_owner** (Person/Team) – *Evidence* (accountable owner of BCP/DR plan)**last_reviewed_at** (Date) – *Scoring/Evidence* (last plan update date)**recovery_objective_rto** (Hours) – *Scoring* (Recovery Time Objective)**recovery_objective_rpo** (Hours) – *Scoring* (Recovery Point Objective)**tested_recently** (Yes/No) – *Scoring* (whether drills/tests conducted)**last_test_date** (Date) – *Evidence* (date of last BCP/DR test)**test_result_summary** (Textarea) – *Evidence* (outcome of last test/drill)**offsite_backup** (Yes/No) – *Scoring* (offsite backups in place)**redundant_systems** (Yes/No) – *Scoring* (redundant systems available)**power_backup_available** (Yes/No) – *Scoring* (backup power in place)**communication_plan** (Yes/No) – *Scoring* (crisis communication plan exists)**external_vendor_involved** (Yes/No) – *Scoring* (critical external dependencies identified)
Risk & Impact	**service_disruption** (Yes/No) – *Scoring* (flags risks that could disrupt essential services)

4. Network & Information Security

Module	Fields (Scoring & Evidence)
Computers	**antivirus_installed** (Yes/No) – *Scoring* (endpoint anti-malware present)**encryption_enabled** (Yes/No) – *Scoring* (disk/data encryption enabled)**vpn_enabled** (Yes/No) – *Scoring* (secure remote access enabled)**admin_privileges** (Yes/No) – *Scoring* (user has admin rights; least privilege)**network_access** (Yes/No) – *Scoring* (device is

	network-connected)**certificate_file** (Compliance Config PDF) – *Evidence* (device security configuration certificate/log)**certificate_status** (Verified/Missing) – *Scoring/Evidence* (device config compliance status)
Security Measures	**document_reference** (Security Policy/Config PDF) – *Evidence* (supporting docs for network controls – e.g. firewall configs, network policies)

5. Incident Response & Risk Management

Module	Fields (Scoring & Evidence)
Data Handlers	**has_privileged_access** (Yes/No) – *Scoring* (flags high-risk staff/admins requiring stricter IR plans)
Risk & Impact	**status** (Open/Mitigated) – *Scoring* (risk status – unresolved open risks elevate overall risk)**follow_up_needed** (Yes/No) – *Scoring* (whether further risk mitigation actions are pending)**existing_controls** (Textarea) – *Scoring* (documented current controls for each risk)**mitigation_action** (Textarea) – *Scoring* (planned mitigation steps for each risk)**target_resolution_date** (Date) – *Evidence* (target date to resolve risk – shows proactive remediation timeline)**supporting_document** (PDF upload) – *Evidence* (attached risk assessment reports or discovery docs supporting risk identification)**control_evidence** (PDF upload) – *Evidence* (proof of implemented controls for a risk – logs, screenshots, etc.)**certificate_status** (Pending/Confirmed) – *Evidence*

	(approval status of risk entry by management; confirms governance sign-off on risk)
Incident Mgmt	**incident_title** / **incident_description** – *Evidence* (record of incident details as reported)**resolved_by** (User) – *Evidence* (who responded/resolved the incident, showing assigned IR roles)**response_summary** (Textarea) – *Evidence* (description of actions taken in response to incident)**external_notified** (Yes/No) – *Scoring/Evidence* (whether regulators or external parties were notified when required, indicating compliance with NIS2 reporting obligations)**incident_report_file** (Upload) – *Evidence* (attached formal incident report or post-mortem document)**incident_notes** / **last_updated** (Timestamp) – *Evidence* (internal tracking notes and the last update time, showing an audit trail for incident handling)

6. Supply Chain & Third-Party Security

Module	Fields (Scoring & Evidence)
Business Continuity	**external_vendor_involved** (Yes/No) – *Scoring* (flags if critical processes rely on third parties, linking continuity risk to supply chain)

Supply Chain	**vendor_name** (Text) – *Evidence* (name of third-party supplier/service)**service_provided** (Text) – *Evidence* (description of service or product provided by vendor)**criticality_level** (High/Med/Low) – *Scoring* (internal rating of vendor's criticality to operations)**has_system_access** (Yes/No) – *Scoring* (whether the vendor has access to internal systems — "Yes" increases inherent risk)**data_shared** (Data Type) – *Scoring* (type of sensitive data shared with vendor, if any — more sensitive data implies higher impact if vendor is breached)**contract_in_place** (Yes/No) – *Scoring* (whether a security agreement/contract or DPA exists with the vendor — "No" indicates non-compliance and high risk)**contract_review_date** (Date) – *Evidence* (date of last contract security review or update, demonstrating due diligence in third-party agreements)

7. Implemented Security Measures

Module	Fields (Scoring & Evidence)
Computers	**antivirus_installed** (Yes/No) – *Scoring* (baseline anti-malware deployed on endpoints)**encryption_enabled** (Yes/No) – *Scoring* (devices have encryption for data at rest)**admin_privileges** (Yes/No) – *Scoring* (least privilege on endpoints – many "Yes" implies weak access control)

Security Measures	**measure_name** (Text) – *Scoring* (name of each security control/measure implemented; comprehensive coverage of all required controls is expected)**measure_type** (Technical/Organizational/Policy) – *Scoring* (classification of control; ensures a balanced mix of control types per NIS2 requirements)**implementation_status** (Dropdown) – *Scoring* (degree of implementation for each measure – fully in place vs partially or not implemented)**scope** (Company-wide / Dept / Asset) – *Scoring* (scope of application of the control – broader coverage yields better compliance)**last_reviewed_at** (Date) – *Scoring/Evidence* (last effectiveness audit/review date for the control; recent reviews indicate an active ISMS and improve mitigation scoring)**responsible_person** (Text/Dropdown) – *Evidence* (owner responsible for the control – evidences governance and accountability for each measure)**document_reference** (PDF upload) – *Evidence* (attached documentation for the control, e.g. policy or configuration file supporting the existence and communication of the measure)**notes** (Textarea) – *Evidence* (internal notes on control implementation or changes – provides an audit trail for control maintenance)

8. Staff Training

Module	Fields (Scoring & Evidence)

Data Handlers	**has_privileged_access** (Yes/No) – *Scoring* (identifies admin/high-privilege staff requiring training priority)**training_passed** (Yes/No) – *Scoring* (whether each staff member has completed required training)**trained_at** (Date) – *Scoring* (date of last training completed – recency of training)**next_training_due** (Date) – *Scoring* (scheduled next training date – ensures periodic training frequency)**certificate_status** (Verified/Expired) – *Scoring* (status of individual's training certification – expired certifications signal lapses and increase risk)**certificate_file** (Training Certificate PDF) – *Evidence* (proof of course completion on record for each employee)**policy_acceptance_doc** (File upload) – *Evidence* (signed policy acceptance/acknowledgment from staff, showing compliance with security policy awareness requirements)

Placement in UI: In the **Evaluation & Reports** page, each of the above cards will have its own section (following the existing HTML structure in `index.html`). Under each card's section header, the corresponding field table (as detailed above) will be inserted. This aligns with the NIS2 compliance framework by presenting, for each NIS2 category (card), all relevant data inputs — both those contributing to the risk **Scoring** and those serving as **Supporting Evidence** — grouped by their source module. This integrated view under each card ensures that evaluators can see not only the calculated risk metrics but also the concrete evidence supporting the organization's compliance in that domain, in a manner consistent with the provided PDF mapping and the existing UI layout. Each table is placed in-line under its card heading without introducing new layout elements, using the current page structure to display field groupings per NIS2 category. This way, the **Evaluation & Reports** page provides a comprehensive, section-by-section breakdown of how each NIS2 domain's score is derived and which evidentiary artifacts back it up, exactly reflecting the mapping of modules/fields to the eight NIS2 evaluation cards.