Cybersecurity Evidence Registry (SSOT) - Structured Overview

This is a comprehensive **Dutch Cybersecurity Evidence Registry** that serves as a Single Source of Truth (SSOT) for compliance documentation. It appears to follow the **NIST Cybersecurity Framework** structure with five main functions: Identify, Protect, Detect, Respond, and Recover.

Document Structure

The registry defines required evidence across **5 main security functions**, each with multiple categories:

1. IDENTIFY (ID) - Understanding Security Context

ID.AM - Asset Management

Purpose: Maintain inventory of all IT/OT assets and their security requirements

Key Evidence Types:

- **Databases**: Asset inventories, software platforms, GDPR registers, connection registers
- **Procedures**: Lifecycle management, unauthorized hardware detection, software inventory updates
- **Logs**: Asset updates, lifecycle actions, unauthorized hardware incidents
- **Screenshots**: Configuration proofs, inventory snapshots
- **Forms/Templates**: Exception documentation for non-standard hardware/software

Sub-categories covered:

- AM-1: Physical & virtual IT/OT asset inventory
- AM-2: Software platforms and applications inventory
- AM-3: Data flow mapping (GDPR register, connection register)
- AM-4: External service providers and connections
- AM-5: Asset classification and prioritization
- AM-6: Security roles and responsibilities assignment

ID.BE - Business Environment

Purpose: Understand organization's role in critical infrastructure and supply chain

Key Evidence Types:

- **Policy Documents**: Supply chain position, critical sector status, strategic priorities

- **Procedures**: Chain position identification, security measures against supply chain risks
- **Reports**: Supply chain risk assessments, sector role documentation
- **Meeting Minutes**: Discussions about chain position with relevant departments
- **Logs**: Incidents from supply chain, detection of supply chain threats

ID.GV - Governance

Purpose: Establish cybersecurity policies and legal compliance framework

Key Evidence Types:

- **Policy Documents**: Approved cybersecurity policies with version control
- **Registers**: Relevant laws and regulations (GDPR, NIS2, sector requirements)
- **Procedures**: Periodic policy evaluation, implementation of new regulations
- **Logs**: Policy changes, approvals, compliance checks
- **Review Reports**: Audit reports, compliance control results
- **Screenshots**: Intranet policy pages, compliance tool overviews

ID.RA - Risk Assessment

Purpose: Identify and assess cybersecurity risks and vulnerabilities

Key Evidence Types:

- **Registers**: ICT/OT risks and vulnerabilities overview
- **Procedures**: Risk identification methods, threat analysis workflows
- **Reports**: Threat analysis, emerging vulnerabilities
- **Logs**: New or changed risks, threat intelligence feeds
- **Contracts**: Threat intelligence subscriptions (CERT, ENISA, ISAC)
- **Screenshots**: Threat monitoring tools, SIEM interfaces

Sub-categories:

- RA-1: Risk and vulnerability identification (ICT & OT)
- RA-2: Threat intelligence sharing and reception
- RA-5: Periodic risk reassessment
- RA-6: Risk response strategy and prioritization

ID.RM - Risk Management

Purpose: Define organizational risk tolerance and management processes

Key Evidence Types:

- **Policy Documents**: Risk management policy, risk tolerance definitions
- **Procedures**: Risk tolerance determination, priority setting

- **Review Reports**: Risk tolerance evaluations, risk management effectiveness
- **Checklists**: Risk management parameters, stakeholder lists
- **Distribution Proofs**: Communication of risk management processes

ID.SC - Supply Chain Risk Management

Purpose: Manage cybersecurity risks in the supply chain

Key Evidence Types:

- **Policy Documents**: Supply chain risk management process
- **Procedures**: Supply chain risk assessment, vendor evaluation
- **Reports**: Vendor risk assessments, compliance evaluations
- **Contracts**: Security clauses with suppliers, SLAs
- **Logs**: Vendor lists, supply chain changes
- **Checklists**: Contract controls, vendor security requirements

2. PROTECT (PR) - Implement Safeguards

PR.AC - Access Control

Purpose: Manage and control access to assets and information

Key Evidence Types:

- **Policy Documents**: Identity/credential policies, physical access control, remote access policies, network segmentation
- **Procedures**: Credential management, access rights procedures, authorization processes
- **Registers**: Credential registries, revoked credentials, authorized personnel lists, access rights per system
- **Logs**: Physical access logs, remote access sessions, access rights changes
- **Review Reports**: Periodic access rights reviews, privilege audits
- **Screenshots**: IAM system configurations, MFA settings, firewall rules

Sub-categories:

- AC-1: Identity and credential management (issuance, verification, revocation)
- AC-2: Physical access control to facilities and equipment
- AC-3: Remote access management (VPN, MFA requirements)
- AC-4: Access permissions management (least privilege, separation of duties)
- AC-5: Network segmentation and firewall management
- AC-6: Identity verification before credential issuance
- AC-7: Authentication proportional to transaction risk

PR.AT - Awareness and Training

Purpose: Ensure personnel understand their security responsibilities

Key Evidence Types:

- **Policy Documents**: Training policies for employees, privileged users, third parties, senior leadership
- **Procedures**: Training program procedures, onboarding for third parties
- **Training Materials**: Presentations, content, simulation scenarios
- **Checklists**: Training attendance tracking, role acceptance confirmations
- **Reports**: Training effectiveness evaluations, awareness campaign results
- **Review Reports**: Training program evaluations, knowledge assessments
- **Distribution Proofs**: Communication of responsibilities to stakeholders
- **Registers**: Qualified privileged users, informed personnel lists

PR.DS - Data Security

Purpose: Protect data at rest, in transit, and during disposal

Key Evidence Types:

- **Policy Documents**: Data protection at rest, data in transit, data transfer/disposal, capacity management, data leak prevention, integrity controls, environment separation, hardware integrity
- **Procedures**: Data protection procedures, transfer/disposal methods, capacity management, integrity verification
- **Registers**: Protected data inventories, secured data transfers, disposal logs
- **Screenshots**: Encryption tools, DLP systems, monitoring dashboards
- **Checklists**: Data protection verification, environment separation controls
- **Review Reports**: Data protection effectiveness, capacity management evaluations
- **Reports**: Hardware integrity test results, capacity planning reports

PR.IP - Information Protection Processes

Purpose: Maintain protective technology and processes

Key Evidence Types:

- **Policy Documents**: Baseline configuration, system development lifecycle, change management, backup policies, physical security, data destruction, improvement processes, information sharing, response/recovery planning, personnel management, vulnerability management

- **Procedures**: Configuration procedures, SDLC procedures, change control, backup procedures, physical security procedures, destruction methods, testing procedures, forensic analysis
- **Overviews**: Baseline configurations, system lifecycles, changes made, backup schedules, physical measures, destruction records, improvement actions, shared information
- **Logs**: Configuration changes, backup executions, physical access, destruction activities, improvement tracking
- **Checklists**: Configuration checks, SDLC requirements, change control steps, backup verification, physical security inspections, destruction verification
- **Review Reports**: Configuration reviews, SDLC evaluations, change management effectiveness, backup testing, physical security audits, destruction process validation, improvement assessments
- **Reports**: Test results, validation reports, forensic reports

PR.MA - Maintenance

Purpose: Ensure secure maintenance of systems and equipment

Key Evidence Types:

- **Policy Documents**: Maintenance and repair policies, preventive maintenance requirements, maintenance equipment management
- **Procedures**: Maintenance procedures, approval processes for diagnostic tools, inspection and scanning procedures, post-maintenance verification
- **Logs**: Maintenance activities, tool usage monitoring, inspection results, corrective actions
- **Checklists**: Maintenance tasks, approved tools verification, physical security of maintenance equipment
- **Overviews**: Maintenance schedules, approved maintenance tools, maintenance equipment inventory
- **Registers**: Maintenance tickets, maintenance equipment inventory, approved tool lists
- **Reports**: Maintenance test results, post-maintenance verification

PR.PT - Protective Technology

Purpose: Implement technical security solutions

Key Evidence Types:

- **Policy Documents**: Logging/monitoring, removable media, minimal functionality, network security, time synchronization, audit failure warnings, deny-all execution policy, data flow management, external interfaces
- **Procedures**: Logging procedures, media procedures, disabling unnecessary functions, network protection, time sync, audit expansion, flow management

- **Overviews**: Log sources/audit events, media in use, disabled functionalities, network security measures, time sources, alarm thresholds, allowed/forbidden flows, official external channels
- **Logs**: Audit events, media scans, detected warnings, network usage, time sync events, audit failures, flow violations
- **Screenshots**: Logging configurations, media configuration, detection tools, SIEM dashboards, threshold settings, flow blocking
- **Checklists**: Logging monitoring, media security, minimal functionality, network security, autorun disabled, ports/protocols checks
- **Reports**: Log analysis, network security evaluations, threshold effectiveness, flow compliance
- **Review Reports**: Logging effectiveness, media policy updates, functionality reviews, network security assessments

3. DETECT (DE) - Identify Cybersecurity Events

DE.AE - Anomalies and Events

Purpose: Detect and analyze anomalous activity

Key Evidence Types:

- **Procedures**: Network baseline procedures, event analysis, logging/correlation, impact determination, alarm threshold setting
- **Policy Documents**: Network monitoring policy, event analysis policy, logging policy, impact analysis policy, alarm policy
- **Overviews**: Network baselines, event sources/sensors, alarm thresholds, automated analysis chains
- **Logs**: Event correlations, event logs from multiple sources, generated warnings, automation chains
- **Screenshots**: Baseline monitoring, threat monitors, SIEM tools, threshold configurations
- **Checklists**: Baseline requirements, event analysis steps, logging/correlation checks, impact determination, threshold settings
- **Reports**: Event analysis reports, impact assessments, automation evaluations
- **Review Reports**: Baseline effectiveness, analysis process reviews, logging effectiveness, threshold evaluations

DE.CM - Continuous Monitoring

Purpose: Monitor systems continuously for security events

Key Evidence Types:

- **Procedures**: Network monitoring, physical monitoring, personnel activity monitoring, malware detection, mobile code detection, external service provider monitoring, unauthorized usage monitoring, vulnerability scanning
- **Policy Documents**: Monitoring policies, authorized software policies, vendor compliance monitoring, continuous security monitoring, configuration compliance
- **Overviews**: Monitoring actions, anti-malware tools, allowed/blocked mobile code, external connections, monitoring measures, detection mechanisms, scanning schedules
- **Logs**: Network usage, physical events, suspicious activities, malware detections, mobile code detections, external access, unauthorized incidents, scan results
- **Screenshots**: Monitoring tools, malware alerts, mobile code detection, external access monitoring, SOC dashboards, scan results
- **Checklists**: Monitoring checks, anti-malware measures, detection checks, vendor monitoring, configuration checks
- **Reports**: Vulnerability scan reports, monitoring effectiveness, vendor compliance scorecards, configuration compliance
- **Review Reports**: Monitoring process evaluations, detection effectiveness, vendor monitoring reviews, configuration management reviews

DE.DP - Detection Processes

Purpose: Maintain and improve detection capabilities

Key Evidence Types:

- **Procedures**: Compliance with detection requirements, testing detection processes, communicating detected events, continuous improvement
- **Overviews**: Applicable requirements/controls, communication parties, improvement actions, detection automation chains
- **Checklists**: Compliance checks, testing checklists, communication checklists, improvement checklists
- **Reports**: Test/validation reports, improvement test reports
- **Review Reports**: Compliance reviews, testing effectiveness, communication process reviews, improvement process reviews

4. RESPOND (RS) - Take Action on Detected Events

RS.RP - Response Planning

Purpose: Execute incident response plans

Key Evidence Types:

- **Policy Documents**: Incident response policy, incident response plans
- **Procedures**: Incident response procedures, execution procedures

- **Overviews**: Roles/responsibilities/contacts, continuity objectives, prioritization scales
- **Reports**: Incident response execution reports, recovery planning
- **Checklists**: Incident response action lists, immediate recovery actions
- **Distribution Proofs**: Communication of recovery procedures
- **Review Reports**: Response plan evaluations, plan testing results
- **Logs**: Recovery actions registration

RS.CO - Communications

Purpose: Coordinate response activities and communications

Key Evidence Types:

- **Procedures**: Roles and priorities, incident reporting, information sharing, coordination with stakeholders, voluntary information exchange, external notifications
- **Policy Documents**: Communication policies, PR/crisis management policies
- **Overviews**: Roles and objectives, reporting criteria/contacts, shared information/stakeholders, stakeholder coordination, external stakeholders, stakeholder matrix, external notifications
- **Agreements**: Reporting criteria overviews
- **Checklists**: Incident knowledge, incident reporting, information sharing, coordination, voluntary exchange, external communication
- **Review Reports**: Knowledge level reviews, reporting process reviews, information sharing effectiveness, coordination effectiveness, voluntary exchange reviews
- **Logs**: Notifications and follow-ups
- **Registers**: External notifications and recipients
- **Forms/Templates**: Regulator/customer notification templates

RS.AN - Analysis

Purpose: Analyze incidents to understand impact and root cause

Key Evidence Types:

- **Procedures**: Detection alert investigation, impact analysis, forensic analysis, incident categorization, vulnerability management, automated triage
- **Overviews**: Impact analyses performed, forensic cases, incident categories, vulnerabilities and mitigations, automated analysis chains, mitigation channels
- **Logs**: Detection analysis, impact analysis and findings, received vulnerabilities, automated impact analysis
- **Screenshots**: Analysis environments, automated analysis tools
- **Checklists**: Investigation steps, impact determination, forensic analysis, categorization, vulnerability management
- **Reports**: Forensic reports, root cause analysis, impact assessments

- **Review Reports**: Investigation process reviews, impact analysis effectiveness, forensic process reviews, categorization effectiveness, vulnerability management reviews
- **Registers**: Forensic evidence, evidence provenance, distribution lists

RS.MI - Mitigation

Purpose: Contain and eliminate threats

Key Evidence Types:

- **Policy Documents**: Incident response plans covering all phases
- **Procedures**: Detection and triage, containment and decision ladder, eradication and clearance, recovery and validation
- **Plans**: Incident Response Plans covering preparation, detection, analysis, containment, eradication, recovery
- **Overviews**: Impact and priority scales
- **Registers**: Risk acceptance for policy application

RS.IM - Improvements

Purpose: Learn from incidents and improve processes

Key Evidence Types:

- **Policy Documents**: Post-incident evaluation process, plan update policies
- **Procedures**: Incident review and lessons learned, change management for response/recovery plans
- **Distribution Proofs**: Shared lessons learned, communication of changed plans
- **Review Reports**: Post-incident evaluations, plan revision reports
- **Training Materials**: Training based on lessons learned
- **Checklists**: Implementation steps for lessons learned

5. RECOVER (RC) - Restore Capabilities

RC.RP - Recovery Planning

Purpose: Execute recovery processes

Key Evidence Types:

- **Policy Documents**: Recovery plans for disasters and cyber incidents, continuity objectives
- **Procedures**: Recovery procedures, transition to recovery, degradation and prioritization
- **Plans**: Degradation and prioritization plans
- **Overviews**: Essential functions and thresholds
- **Checklists**: Immediate recovery action lists

- **Distribution Proofs**: Communication of recovery procedures
- **Review Reports**: Recovery action evaluations, plan evaluations
- **Reports**: Recovery actions and continuity status
- **Logs**: Executed recovery actions, maintained service delivery cases

RC.IM - Improvements

Purpose: Incorporate lessons learned into recovery processes

Key Evidence Types:

- **Policy Documents**: Lessons learned integration policy
- **Procedures**: Processing and implementing lessons learned
- **Training Materials**: Training on new/changed procedures
- **Review Reports**: Testing or evaluation of changed procedures, recovery plan evaluations
- **Distribution Proofs**: Communication of changed procedures
- **Checklists**: Implementation steps for lessons learned

RC.CO - Communications

Purpose: Manage recovery communications

Key Evidence Types:

- **Policy Documents**: Communication and PR policy for crisis management, reputation recovery strategies
- **Procedures**: Communication procedures during recovery, reputation recovery procedures, recovery communication procedures
- **Distribution Proofs**: Communicated statements, recovery action communications, recovery activity communications
- **Reports**: Reputation recovery action reports
- **Review Reports**: Communication approach evaluations, reputation recovery evaluations, recovery communication evaluations
- **Methodology Documents**: Crisis management strategies for reputation recovery
- **Contracts**: PR Officer appointment decisions

Evidence Type Summary

Across all categories, the framework requires:

1. **Policy Documents (Beleidsdocument)** - Formal approved policies
2. **Procedures (Procedure)** - Step-by-step process descriptions
3. **Registers (Register)** - Maintained lists and inventories
4. **Logs (Log)** - Activity records and audit trails
5. **Screenshots (Screenshot)** - Visual proof of implementations

6. **Checklists (Checklist)** - Verification and control lists
7. **Reports (Rapport)** - Analysis and assessment documents
8. **Review Reports (Reviewverslag)** - Periodic evaluation reports
9. **Forms/Templates (Formulier/Sjabloon)** - Standardized documentation templates
10. **Overviews (Overzichtsdocument)** - Summary documents and matrices
11. **Distribution Proofs (Verspreidingsbewijs)** - Evidence of communication
12. **Contracts/Agreements (Overeenkomst/Contract)** - Legal agreements
13. **Training Materials (Awareness & Training)** - Educational content
14. **Minutes (Minutes)** - Meeting records
15. **Plans (Plan)** - Strategic and tactical plans
16. **Methodology Documents (Methodedocument)** - Approach descriptions

Key Observations

1. **Comprehensive Coverage**: The framework covers the complete cybersecurity lifecycle from identification through recovery
2. **Multiple Evidence Types**: Each control requires multiple forms of evidence (policy + procedure + proof of execution)
3. **Audit-Ready**: Structured for compliance audits and assessments
4. **SSOT Designation**: Serves as the authoritative source for evidence requirements
5. **Dutch Compliance Focus**: References NIS2, GDPR, and other European regulations
6. **Practical Implementation**: Includes not just policies but operational proof (logs, screenshots, reports)