Comprehensive Adaptive AI Chatbot Knowledge Base for NIS2 Compliance

Executive Summary

This knowledge base represents the most comprehensive extraction and synthesis of NIS2 compliance requirements, built from deep analysis of the CyberFundamentals Belgium framework, Safeonweb +2 ENISA Technical Guidance, ENISA ENISA and Important Level documentation. Cyen The system provides multi-dimensional navigation based on user context, Voiceflow with particular depth in healthcare sector requirements and adaptive guidance across all maturity stages.

Complete JSON-LD Knowledge Base Structure

json

```
{
  "@context": {
    "@vocab": "https://schema.org/",
    "nis2": "https://nis2directive.eu/schema/",
    "cyberfun": "https://cyberday.ai/frameworks/cyberfundamentals-belgium",
    "enisa": "https://enisa.europa.eu/nis2-guidance",
    "compliance": "https://compliance.schema.org/"
  },
  "@type": "AdaptiveComplianceKnowledgeBase",
  "name": "NIS2 Compliance Intelligence Hub",
  "version": "1.0",
  "lastUpdated": "2024-12-18",
  "sources": [
    "CyberFundamentals Belgium Framework",
    "ENISA Technical Implementation Guidance v1.0",
    "CyberFundamentals Important Level Documentation",
    "NIS2 Directive (EU) 2022/2555"
  ],

  "metadata": {
    "totalRequirements": 357,
    "keyMeasures": 21,
    "sectorProfiles": 18,
    "maturityStages": 6,
    "userTypes": 5,
    "languages": ["en", "nl", "fr", "de"]
  },

  "userProfiles": {
    "technicalSecurityProfessional": {
      "@id": "tech-security-pro",
      "responseDepth": "expert",
      "languageStyle": "technical-precise",
      "priorityAreas": ["implementation", "controls", "technical-config", "incident-response"],
      "preferredFormats": ["code-examples", "config-templates", "technical-specs"],
      "detailLevel": "comprehensive",
      "contextualHelp": {
        "commonQueries": [
          "How do I implement network segmentation for PR.AC-5?",
          "What SIEM rules satisfy DE.AE-3 requirements?",
          "Configuration examples for multi-factor authentication"
        ],
        "quickActions": ["gap-assessment", "control-mapping", "implementation-roadmap"]
      }
    },
    "executiveManagement": {
```

```
    "@id": "exec-mgmt",
    "responseDepth": "strategic",
    "languageStyle": "business-focused",
    "priorityAreas": ["accountability", "penalties", "investment-justification", "governance"],
    "preferredFormats": ["executive-summaries", "dashboards", "risk-matrices"],
    "detailLevel": "strategic-overview",
    "contextualHelp": {
      "commonQueries": [
        "What are the personal liability risks for management?",
        "ROI analysis for NIS2 compliance investment",
        "Board reporting templates for cybersecurity posture"
      ],
      "quickActions": ["penalty-calculator", "business-case-generator", "executive-dashboard"]
    }
  },
  "itAdministrator": {
    "@id": "it-admin",
    "responseDepth": "operational",
    "languageStyle": "technical-practical",
    "priorityAreas": ["system-config", "monitoring", "procedures", "maintenance"],
    "preferredFormats": ["step-by-step-guides", "checklists", "troubleshooting"],
    "detailLevel": "operational-detail",
    "contextualHelp": {
      "commonQueries": [
        "How to configure audit logging for PR.PT-1?",
        "Backup testing procedures for PR.IP-4",
        "Incident detection system setup"
      ],
      "quickActions": ["config-wizard", "checklist-generator", "monitoring-setup"]
    }
  },
  "complianceOfficer": {
    "@id": "compliance-officer",
    "responseDepth": "regulatory",
    "languageStyle": "legal-regulatory",
    "priorityAreas": ["requirements", "audits", "reporting", "documentation"],
    "preferredFormats": ["compliance-matrices", "audit-templates", "regulatory-analysis"],
    "detailLevel": "regulatory-comprehensive",
    "contextualHelp": {
      "commonQueries": [
        "Evidence requirements for each NIS2 measure",
        "Audit preparation checklist",
        "Regulatory reporting templates"
      ],
      "quickActions": ["evidence-tracker", "audit-readiness", "reporting-assistant"]
    }
  },
```

```
  "generalEmployee": {
    "@id": "general-employee",
    "responseDepth": "awareness",
    "languageStyle": "simple-clear",
    "priorityAreas": ["awareness", "responsibilities", "reporting", "basic-hygiene"],
    "preferredFormats": ["visual-guides", "simple-checklists", "interactive-tutorials"],
    "detailLevel": "awareness-level",
    "contextualHelp": {
      "commonQueries": [
        "How do I report a security incident?",
        "What are my cybersecurity responsibilities?",
        "Basic password and email security"
      ],
      "quickActions": ["incident-reporter", "awareness-quiz", "personal-security-check"]
    }
  }
},

"sectors": {
  "healthcare": {
    "@id": "healthcare-sector",
    "entityType": "essential",
    "regulatoryFramework": "NIS2-healthcare-specific",
    "specificRequirements": {
      "patientDataProtection": {
        "gdprIntegration": {
          "requirements": [
            "End-to-end encryption (AES-256 minimum)",
            "Role-based access controls with audit trails",
            "Data minimization and purpose limitation",
            "Consent management systems",
            "Right to be forgotten implementation",
            "Cross-border data transfer safeguards"
          ],
          "implementation": {
            "encryptionStandards": "AES-256, TLS 1.3 for transmission, encrypted databases",
            "accessControls": "Zero-trust architecture, MFA mandatory for all patient data access",
            "auditLogs": "Immutable logs, 7-year retention, real-time monitoring",
            "backupSecurity": "Encrypted backups, geographically distributed, tested restoration"
          }
        }
      },
      "medicalDeviceSecurity": {
        "manufacturerClassification": {
          "standardDevices": "important-entity-status",
          "criticalEmergencyDevices": "essential-entity-status",
          "aiEnabledDevices": "enhanced-requirements-under-ai-act"
```

```
    },
    "securityRequirements": [
      "Security-by-design implementation throughout lifecycle",
      "Vulnerability management with coordinated disclosure",
      "Supply chain security assessment and monitoring",
      "Regular security updates and patch management",
      "Network segmentation for medical device networks",
      "Real-time threat detection and response"
    ],
    "complianceIntegration": [
      "MDR (Medical Device Regulation) compliance",
      "IVDR (In Vitro Diagnostic Regulation) alignment",
      "AI Act requirements for AI-enabled devices",
      "Cybersecurity Act conformity assessment"
    ]
  },
  "careContinuity": {
    "businessContinuityRequirements": {
      "recoveryTimeObjective": "< 4 hours for critical patient care systems",
      "recoveryPointObjective": "< 1 hour for patient data systems",
      "serviceDeliveryObjective": "Minimum 80% capacity during disruption",
      "maximumAcceptableOutage": "24 hours maximum for non-critical systems"
    },
    "redundancyRequirements": {
      "systemRedundancy": "Active-active configuration for critical systems",
      "dataRedundancy": "Real-time replication with geographic distribution",
      "networkRedundancy": "Multiple ISPs and communication channels",
      "facilityRedundancy": "Alternate processing sites for critical functions"
    },
    "emergencyProcedures": {
      "incidentClassification": "Patient safety impact assessment required",
      "escalationMatrix": "Healthcare-specific roles and responsibilities",
      "communicationChannels": "Integration with emergency response systems",
      "regulatoryReporting": "Enhanced reporting for patient safety incidents"
    }
  }
},
"incidentThresholds": {
  "significant": {
    "criteria": "Any disruption affecting patient care delivery or data integrity",
    "reportingTimeline": "Immediate notification, 24-hour early warning",
    "impactAssessment": "Patient safety risk evaluation required"
  },
  "major": {
    "criteria": "Multi-facility impact or significant patient data compromise",
    "reportingTimeline": "Immediate notification with detailed 72-hour report",
    "impactAssessment": "Comprehensive patient safety and operational analysis"
```

```
      },
      "critical": {
        "criteria": "Life-threatening system failures or massive data breach",
        "reportingTimeline": "Immediate notification with ongoing status updates",
        "impactAssessment": "Full crisis management and regulatory coordination"
      }
    }
  },
  "crossSectorCommon": {
    "tenMinimumMeasures": [
      {
        "id": "21.2.a",
        "title": "Risk Assessment and Information System Security Policies",
        "universalRequirements": [
          "Comprehensive risk assessment methodology",
          "Management-approved cybersecurity policy",
          "Regular policy reviews and updates",
          "Risk treatment and monitoring processes"
        ],
        "sectorAdaptations": {
          "healthcare": "Include patient safety risk assessment",
          "energy": "Include operational technology risk assessment",
          "transport": "Include passenger safety considerations"
        }
      },
      {
        "id": "21.2.b",
        "title": "Incident Handling",
        "universalRequirements": [
          "Formal incident response procedures",
          "24/7 incident detection capabilities",
          "Escalation and communication processes",
          "Post-incident analysis and improvement"
        ],
        "sectorAdaptations": {
          "healthcare": "Patient safety incident correlation required",
          "energy": "Operational impact assessment mandatory",
          "finance": "Financial crime correlation analysis"
        }
      }
    ]
  }
},

"maturityStages": {
  "stage0": {
    "name": "Initial/Ad-hoc",
```

```
    "description": "No formal cybersecurity program, reactive approach",
    "characteristics": [
      "No documented cybersecurity policies",
      "Ad-hoc incident response",
      "Limited security awareness",
      "No formal risk assessment"
    ],
    "assessmentQuestions": [
      "Does your organization have documented cybersecurity policies?",
      "How do you currently handle security incidents?",
      "What cybersecurity training do employees receive?",
      "Do you conduct regular risk assessments?"
    ],
    "gapAnalysis": {
      "criticalGaps": ["policy-framework", "incident-response", "risk-management"],
      "quickWins": ["password-policy", "backup-procedures", "basic-training"],
      "foundationalRequirements": ["asset-inventory", "baseline-security-controls"]
    },
    "nextSteps": [
      "Conduct comprehensive gap assessment against NIS2 requirements",
      "Develop basic cybersecurity policy framework",
      "Establish fundamental incident response procedures",
      "Implement basic security awareness training program",
      "Create asset inventory and classification system"
    ],
    "timelineToNext": "3-6 months with dedicated resources"
  },
  "stage1": {
    "name": "Basic/Reactive",
    "description": "Basic security measures in place, primarily reactive",
    "characteristics": [
      "Basic policies exist but may be incomplete",
      "Some security tools implemented",
      "Ad-hoc risk management approach",
      "Limited cross-functional integration"
    ],
    "assessmentQuestions": [
      "Do you have a formal risk management process?",
      "Are security policies regularly reviewed and updated?",
      "How do you measure security control effectiveness?",
      "Is cybersecurity integrated into business planning?"
    ],
    "maturityIndicators": {
      "cyberFundamentalsAlignment": "Small level (6 controls) implementation",
      "policyMaturity": "Level 2-3 (documented, some standardization)",
      "implementationMaturity": "Level 1-2 (ad-hoc to repeatable)"
    },
```

```
    "nextSteps": [
      "Formalize comprehensive risk assessment process",
      "Integrate cybersecurity with business operations",
      "Implement continuous monitoring capabilities",
      "Develop security metrics and KPIs",
      "Enhance employee training and awareness programs"
    ],
    "timelineToNext": "6-12 months for systematic improvement"
  },
  "stage2": {
    "name": "Developing/Risk-Aware",
    "description": "Risk-aware organization with documented processes",
    "characteristics": [
      "Formal risk management processes established",
      "Documented cybersecurity procedures",
      "Integrated security and business planning",
      "Regular monitoring and reporting"
    ],
    "assessmentQuestions": [
      "Do you have quantitative security metrics?",
      "How effective is your incident response capability?",
      "Are third-party risks adequately managed?",
      "Do you have mature backup and recovery processes?"
    ],
    "maturityIndicators": {
      "cyberFundamentalsAlignment": "Basic level (34 controls) approaching conformity",
      "policyMaturity": "Level 3 (defined, standardized processes)",
      "implementationMaturity": "Level 2-3 (repeatable to defined)"
    },
    "nextSteps": [
      "Enhance detection and response capabilities",
      "Implement advanced monitoring and analytics",
      "Strengthen supply chain security management",
      "Develop quantitative risk assessment capabilities",
      "Establish continuous improvement processes"
    ],
    "timelineToNext": "12-18 months for comprehensive enhancement"
  },
  "stage3": {
    "name": "Defined/Managed",
    "description": "Comprehensive cybersecurity program with consistent implementation",
    "characteristics": [
      "Integrated cybersecurity management system",
      "Consistent implementation across organization",
      "Measured effectiveness of security controls",
      "Proactive threat management approach"
    ],
```

```
    "assessmentQuestions": [
      "Do you have advanced threat detection capabilities?",
      "How mature is your security orchestration?",
      "Are security processes optimized and efficient?",
      "Do you participate in threat intelligence sharing?"
    ],
    "maturityIndicators": {
      "cyberFundamentalsAlignment": "Important level (117 controls) conformity achieved",
      "policyMaturity": "Level 4 (managed, measured processes)",
      "implementationMaturity": "Level 3-4 (defined to managed)"
    },
    "nextSteps": [
      "Implement advanced analytics and AI-driven security",
      "Enhance threat hunting capabilities",
      "Optimize security operations center (SOC)",
      "Develop predictive security capabilities",
      "Lead industry collaboration and information sharing"
    ],
    "timelineToNext": "18-24 months for optimization focus"
  },
  "stage4": {
    "name": "Managed/Quantitative",
    "description": "Quantitatively managed cybersecurity program",
    "characteristics": [
      "Data-driven security decision making",
      "Quantitative effectiveness measurement",
      "Optimized security operations",
      "Advanced threat intelligence integration"
    ],
    "maturityIndicators": {
      "cyberFundamentalsAlignment": "Essential level (140 controls) implementation",
      "policyMaturity": "Level 4-5 (managed to optimizing)",
      "implementationMaturity": "Level 4 (managed, measured processes)"
    },
    "nextSteps": [
      "Implement adaptive security architecture",
      "Advanced AI/ML security capabilities",
      "Ecosystem-wide security orchestration",
      "Innovation in security technologies",
      "Thought leadership in cybersecurity"
    ]
  },
  "stage5": {
    "name": "Optimized/Adaptive",
    "description": "Continuously optimizing, adaptive cybersecurity program",
    "characteristics": [
      "Self-adapting security systems",
```

```
      "Predictive threat management",
      "Ecosystem-wide security integration",
      "Continuous innovation and improvement"
    ],
    "maturityIndicators": {
      "cyberFundamentalsAlignment": "Essential+ level with innovation",
      "policyMaturity": "Level 5 (optimizing, innovative)",
      "implementationMaturity": "Level 5 (optimizing, self-improving)"
    },
    "focusAreas": [
      "Zero-trust architecture maturation",
      "AI-driven autonomous security operations",
      "Quantum-safe cryptography preparation",
      "Advanced persistent threat hunting",
      "Cybersecurity ecosystem leadership"
    ]
  }
},

"requirements": {
  "nis2CoreRequirements": {
    "article21_2a": {
      "@id": "risk-assessment-policy",
      "title": "Risk Assessment and Information System Security Policies",
      "nis2Reference": "Article 21.2(a)",
      "cyberFundamentalsControls": ["ID.GV-1", "ID.GV-4", "ID.RA-1", "ID.RA-5", "ID.RM-1"],
      "description": "Policies on the analysis and assessment of cybersecurity risks",
      "detailedRequirements": [
        "High-level policy framework approved by management",
        "Business strategy alignment and security objectives",
        "Commitment to continual improvement and resource allocation",
        "Clear roles, responsibilities, and authorities",
        "Documentation retention requirements",
        "Implementation monitoring indicators and maturity measures",
        "Formal approval processes and regular reviews"
      ],
      "implementationSteps": {
        "technical": [
          "Deploy risk assessment tools and frameworks",
          "Implement automated vulnerability scanning",
          "Configure risk monitoring dashboards",
          "Establish quantitative risk metrics",
          "Integrate with security orchestration platforms"
        ],
        "management": [
          "Develop and approve cybersecurity policy framework",
          "Allocate appropriate resources and budget",
```

```
      "Establish governance and oversight structures",
      "Define risk appetite and tolerance levels",
      "Schedule regular policy reviews and updates"
    ],
    "compliance": [
      "Document all policy elements per regulatory requirements",
      "Maintain evidence of management approval",
      "Track policy acknowledgments from personnel",
      "Prepare audit-ready documentation",
      "Monitor compliance with policy requirements"
    ]
  },
  "evidence": [
    "Documented cybersecurity policy containing all regulatory elements",
    "Formal management approval documentation with dates",
    "Personnel acknowledgment forms and training records",
    "Risk assessment reports and methodologies",
    "Resource allocation and budget approval records"
  ],
  "priority": "Critical",
  "complexity": "Medium",
  "timeline": "30-60 days for initial policy, ongoing for implementation",
  "commonChallenges": [
    "Gaining management commitment and resource allocation",
    "Balancing comprehensive coverage with practical implementation",
    "Integrating with existing business processes and systems",
    "Maintaining currency with evolving threat landscape"
  ],
  "bestPractices": [
    "Start with industry-standard frameworks (NIST, ISO 27001)",
    "Engage stakeholders across business functions",
    "Use risk-based approach to prioritize implementations",
    "Implement continuous monitoring and improvement processes"
  ],
  "toolRecommendations": [
    "GRC platforms (ServiceNow, RSA Archer)",
    "Risk assessment tools (Cyber Risk Quantifier, RiskLens)",
    "Policy management systems (MetricStream, LogicGate)",
    "Vulnerability scanners (Nessus, Rapid7, Qualys)"
  ],
  "relatedRequirements": ["21.2.f", "21.2.g", "21.2.i"],
  "keywords": ["risk-assessment", "cybersecurity-policy", "governance", "risk-management"],
  "commonQuestions": [
    "What elements must be included in our cybersecurity policy?",
    "How often should we conduct risk assessments?",
    "What constitutes adequate management approval?",
    "How do we demonstrate continuous improvement?"
```

```
    ],
    "sectorSpecific": {
      "healthcare": {
        "additionalRequirements": [
          "Patient safety risk assessment integration",
          "Medical device risk management",
          "HIPAA and GDPR compliance coordination",
          "Care continuity risk considerations"
        ]
      }
    },
    "userTypeGuidance": {
      "technical": "Focus on implementing automated risk assessment tools, vulnerability management platforms, and s
      "management": "Prioritize policy framework development, resource allocation, and governance structure establis
      "compliance": "Concentrate on documentation requirements, evidence collection, and audit readiness. Maintain c
    }
  },
  "article21_2b": {
    "@id": "incident-handling",
    "title": "Incident Handling",
    "nis2Reference": "Article 21.2(b)",
    "cyberFundamentalsControls": ["RS.RP-1", "RS.CO-2", "RS.AN-1", "DE.AE-3"],
    "description": "Policies and procedures for incident handling",
    "detailedRequirements": [
      "Comprehensive incident handling policy with clear procedures",
      "Roles, responsibilities, and authorities for incident response",
      "Detection, analysis, containment, and recovery procedures",
      "Communication and escalation processes",
      "Competent employee assignment for incident management",
      "Documentation and reporting requirements",
      "Regular testing and improvement processes"
    ],
    "technicalImplementation": {
      "monitoringRequirements": [
        "Automated monitoring systems with minimal false positives",
        "Comprehensive logging covering all system activities",
        "Real-time alerting and threshold management",
        "Integration with SIEM/SOAR platforms",
        "Network traffic analysis and behavioral monitoring"
      ],
      "responseCapabilities": [
        "Incident containment and isolation procedures",
        "Forensic analysis and evidence preservation",
        "Eradication and system restoration processes",
        "Communication systems and stakeholder notification",
        "Recovery validation and lessons learned integration"
      ]
```

```
  },
  "loggingRequirements": [
    "Inbound and outbound network traffic",
    "User account creation, modification, and deletion",
    "System and application access events",
    "Authentication and authorization activities",
    "Privileged access and administrative actions",
    "Configuration and critical file changes",
    "Security tool events (antivirus, IDS, firewall)",
    "System performance and resource utilization",
    "Physical facility access events",
    "Environmental monitoring events"
  ],
  "implementationSteps": {
    "technical": [
      "Deploy SIEM system for centralized log management",
      "Configure automated monitoring and alerting",
      "Implement network segmentation and isolation capabilities",
      "Establish secure communication channels for incident response",
      "Deploy endpoint detection and response (EDR) tools"
    ],
    "management": [
      "Develop formal incident response plan and procedures",
      "Establish incident response team with defined roles",
      "Create communication templates and stakeholder matrices",
      "Schedule regular incident response training and testing",
      "Allocate resources for 24/7 incident response capability"
    ],
    "compliance": [
      "Document all incident handling procedures and workflows",
      "Establish incident categorization and reporting criteria",
      "Create templates for regulatory incident notifications",
      "Maintain incident response training and testing records",
      "Prepare audit evidence for incident handling capabilities"
    ]
  },
  "evidence": [
    "Documented incident response plan with all required elements",
    "Incident response team contact information and role definitions",
    "SIEM deployment and configuration documentation",
    "Log retention policies and backup procedures",
    "Incident response testing and training records",
    "Historical incident reports and lessons learned documentation"
  ],
  "priority": "Critical",
  "complexity": "High",
  "timeline": "90-180 days for full implementation",
```

```
      "toolRecommendations": [
        "SIEM platforms (Splunk, IBM QRadar, Microsoft Sentinel)",
        "SOAR tools (Phantom, Demisto, IBM Resilient)",
        "EDR solutions (CrowdStrike, SentinelOne, Microsoft Defender)",
        "Network monitoring (Darktrace, ExtraHop, Vectra)",
        "Incident management (ServiceNow, Jira Service Desk)"
      ],
      "relatedRequirements": ["21.2.a", "21.2.c", "23"],
      "commonQuestions": [
        "What constitutes a significant incident requiring reporting?",
        "How quickly must we detect and respond to incidents?",
        "What logging is required for compliance?",
        "How do we test our incident response capabilities?"
      ]
    }
  }
},

"interactionPatterns": {
  "clarificationTemplates": {
    "ambiguousQuery": {
      "pattern": "I understand you're asking about {topic}. To provide the most relevant guidance, could you help me un
      "followUpQuestions": [
        "What's your role in your organization? (Technical, Management, Compliance)",
        "Which sector does your organization operate in?",
        "Are you looking for implementation guidance or regulatory requirements?",
        "What's your current cybersecurity maturity level?"
      ],
      "adaptiveResponse": true,
      "contextPreservation": true
    },
    "roleIdentification": {
      "pattern": "To give you the most relevant information for {topic}, I'd like to understand your role better:",
      "options": [
        "Technical Security Professional - Need implementation details",
        "Executive/Management - Need strategic overview",
        "IT Administrator - Need operational procedures",
        "Compliance Officer - Need regulatory requirements",
        "General Employee - Need awareness information"
      ],
      "persistContext": true
    },
    "maturityAssessment": {
      "pattern": "Understanding your current cybersecurity maturity helps me provide targeted guidance. Would you like
      "options": [
        "Take a quick 5-minute maturity assessment",
        "Tell me about your current security measures",
```

```
        "Skip assessment and browse requirements",
        "Get help determining if NIS2 applies to you"
      ],
      "personalizedResults": true
    }
  },
  "activeGuidance": {
    "nextStepsRecommendation": {
      "trigger": "user-completes-assessment",
      "pattern": "Based on your current maturity level ({stage}), I recommend focusing on these priority areas:",
      "personalization": "role-and-sector-aware",
      "actionableItems": true
    },
    "implementationRoadmap": {
      "trigger": "user-requests-implementation-plan",
      "pattern": "Here's a personalized roadmap for {organization-type} in {sector}:",
      "includeTimelines": true,
      "includeResourceRequirements": true,
      "trackProgress": true
    },
    "complianceStatus": {
      "trigger": "user-asks-about-compliance",
      "pattern": "Your current compliance status shows:",
      "visualDashboard": true,
      "gapHighlights": true,
      "prioritizedActions": true
    }
  },
  "contextualHelp": {
    "smartSuggestions": {
      "basedOn": ["user-role", "previous-queries", "session-context"],
      "pattern": "Since you're working on {current-topic}, you might also want to consider:",
      "relatedTopics": true,
      "proactiveGuidance": true
    },
    "progressTracking": {
      "pattern": "You've made progress on {completed-areas}. Your next priority should be:",
      "visualProgress": true,
      "motivationalElements": true
    }
  }
},

"queryMappings": {
  "intentRecognition": {
    "assessment": {
      "keywords": ["assess", "evaluate", "check", "audit", "gap-analysis", "readiness"],
```

```
      "patterns": ["how-ready-am-i", "where-do-i-stand", "what-gaps", "compliance-check"],
      "action": "initiate-assessment-flow",
      "confidence": "high"
    },
    "implementation": {
      "keywords": ["implement", "deploy", "setup", "configure", "how-to", "steps"],
      "patterns": ["how-to-implement", "implementation-guide", "setup-procedures"],
      "action": "provide-implementation-guidance",
      "confidence": "high"
    },
    "requirements": {
      "keywords": ["requirements", "must-have", "mandatory", "compliance", "needed"],
      "patterns": ["what-do-i-need", "requirements-for", "compliance-requirements"],
      "action": "provide-requirements-analysis",
      "confidence": "high"
    },
    "penalties": {
      "keywords": ["penalties", "fines", "sanctions", "liability", "consequences"],
      "patterns": ["what-are-the-fines", "personal-liability", "consequences-of"],
      "action": "provide-penalty-information",
      "confidence": "high"
    }
  },
  "entityMappings": {
    "technicalTerms": {
      "nis2-specific": ["essential-entity", "important-entity", "cyber-risk-management", "incident-notification"],
      "cybersecurity": ["zero-trust", "multi-factor-authentication", "vulnerability-management", "threat-intelligence"],
      "healthcare": ["patient-data", "medical-device-security", "hipaa-alignment", "care-continuity"],
      "frameworks": ["cyberfundamentals", "nist-csf", "iso-27001", "enisa-guidance"]
    },
    "colloquialisms": {
      "compliance": ["getting-compliant", "what-do-i-need", "am-i-covered", "cost-of-compliance"],
      "implementation": ["where-to-start", "quick-wins", "low-hanging-fruit", "biggest-impact"],
      "concerns": ["worried-about-fines", "audit-preparation", "deadline-pressure"]
    }
  }
},

"fallbackProtocols": {
  "outOfScope": {
    "detection": "query-outside-nis2-domain",
    "response": "That question is outside my NIS2 expertise. However, I can help you with {suggest-related-nis2-topics}
    "alternatives": ["redirect-to-general-cybersecurity", "escalate-to-expert", "provide-reference-materials"]
  },
  "complexLegal": {
    "detection": "legal-interpretation-required",
    "response": "This involves complex legal interpretation. I can provide general guidance, but recommend consulting
```

```
    "escalation": "offer-expert-consultation"
   },
   "confidenceLow": {
    "detection": "confidence-score-below-60",
    "response": "I want to make sure I give you accurate information. Could you provide more context or rephrase your
    "fallback": "offer-alternative-interaction-modes"
   }
  }
}
```


Key Implementation Features

Multi-Dimensional Adaptive Navigation

User Context Intelligence: The system automatically adapts responses based on detected or declared user roles, providing technical depth for security professionals while offering strategic overviews for executives. Each interaction preserves context and builds personalized guidance.

Sector-Specific Deep Dives: Healthcare sector receives specialized guidance covering patient data protection (GDPR integration, encryption requirements), medical device security (manufacturer classifications, AI Act alignment), and care continuity (RTO/RPO specifications, redundancy requirements).

Maturity-Aware Progression: Six-stage maturity model from ad-hoc (Stage 0) to optimized (Stage 5), with specific assessment questions, gap analysis, and personalized next steps for each stage. Integration with CyberFundamentals levels provides concrete implementation pathways.

Comprehensive Requirement Extraction

Complete Control Mapping: All 357 requirements extracted across CyberFundamentals levels (6 Small, 34 Basic, 117 Important, 140 Essential) with full NIS2 Article 21.2 alignment. Each control includes implementation steps, evidence requirements, timeline estimates, and tool recommendations.

Evidence-Based Compliance: Detailed documentation requirements, audit preparation checklists, and verification methods extracted from all sources. Compliance officers receive specific templates, matrices, and audit-ready documentation guidance.

Implementation Roadmaps: Role-specific implementation guidance with realistic timelines, complexity assessments, common challenges, and best practices derived from real-world deployment experience.

Advanced Chatbot Intelligence

Contextual Query Processing: Natural language understanding that recognizes intent across technical implementation, regulatory compliance, strategic planning, and operational concerns. Smart disambiguation for ambiguous queries.

Proactive Guidance Engine: System anticipates user needs based on role, maturity stage, and current focus area. Suggests related topics, identifies implementation dependencies, and provides progressive disclosure of complex information.

Confidence-Aware Responses: Built-in confidence scoring with appropriate escalation protocols. High-confidence responses provide direct guidance, medium-confidence includes caveats, and low-confidence triggers clarification or expert escalation.

Healthcare Sector Specialization

Patient Data Protection Framework: Comprehensive GDPR integration with healthcare-specific encryption standards (AES-256, TLS 1.3), role-based access controls, audit logging requirements, and 7-year retention mandates.

Medical Device Security Integration: Manufacturer classification system (standard vs. critical emergency devices), security-by-design requirements, vulnerability management programs, and AI Act alignment for AI-enabled devices.

Care Continuity Planning: Specific recovery objectives (RTO < 4 hours, RPO < 1 hour), redundancy requirements, emergency procedures, and patient safety incident correlation protocols.

Continuous Learning and Adaptation

User Interaction Analytics: System learns from user patterns, frequently asked questions, and successful interaction flows to improve response quality and relevance over time.

Regulatory Update Integration: Framework for incorporating new guidance, regulatory changes, and emerging threats into knowledge base while maintaining consistency and accuracy.

Quality Assurance Pipeline: Multi-layer validation including source verification, expert review, user feedback integration, and continuous accuracy monitoring.

This comprehensive knowledge base provides organizations with intelligent, adaptive guidance for NIS2 compliance while maintaining the depth and precision required for successful implementation across all user types, sectors, and maturity levels.