欧洲联盟

NIS2 指令

(Directive EU 2022/2555)

关于在欧盟范围内实现网络安全高度统一水平的措施

面向首席信息安全官及合规负责人的中文摘要

文件参考信息

字段	内容
正式名称	Directive (EU) 2022/2555
通过日期	2022年12月14日
发布日期	2022年12月27日（OJ L 333/80）
生效日期	2023年1月16日
各成员国转化截止日期	2024年10月17日
废止文件	Directive (EU) 2016/1148（NIS1）

> 本文件是对2022年12月14日欧盟NIS2指令的非官方摘要，不构成权威性翻译。如需具有法律约束力的解释，请参阅OJ L 333/80（2022年12月27日）的官方文本。

目录

1. 执行摘要

NIS2 指令（Directive EU 2022/2555）于2022年12月14日由欧洲议会和欧盟理事会通过，是欧盟网络安全基准的总体性指令。自2024年10月18日起，该指令废止并取代此前的NIS1指令（Directive 2016/1148）。

审查评估表明，NIS1虽有助于提升欧盟整体网络韧性，但已不足以应对当前及未来的网络安全威胁。NIS2 大幅扩展了适用范围，引入了统一标准，强化了风险管理和事件报告义务，并规定了更具威慑力的执法条款。

指令的五大支柱

1. **扩大适用范围**：纳入更多行业和企业。
2. **强化风险管理**：Article 21 规定了10项最低技术和组织措施，具有强制性。
3. **分阶段快速报告事件**：24小时预警、72小时事件通报、1个月最终报告。
4. **管理机构责任**：高级管理层可承担个人法律责任。
5. **具有威慑力的处罚**：行政罚款最高可达全球年营业额的2%或1000万欧元。

2. 目的与法律依据

该指令的法律依据为**《欧盟运作条约》（TFEU）第114条**，该条款授权采取措施协调各国规则，以建立并确保内部市场的正常运作。

指令的主要目标包括：

- 消除成员国之间的重大差异，建立共同的最低网络安全规则；
- 建立跨境合作与信息共享的有效机制；
- 更新须承担网络安全义务的行业和活动清单，以反映当前的威胁态势；
- 提供执法和救济机制，确保义务的有效落实；
- 增强关键基础设施运营者和数字服务提供商的网络韧性能力。

该指令在适用时不损害欧盟个人数据保护法律（GDPR，Regulation EU 2016/679）及电子通信隐私法律（Directive 2002/58/EC）的效力，并与上述法律保持一致。

3. 从NIS1到NIS2：为何制定新法规?

NIS1于2016年生效，是欧盟第一部横向网络安全法规。审查过程揭示了成员国在实施层面存在严重差异，适用范围的认定在很大程度上由各成员国自主决定，由此造成了内部市场的碎片化。

NIS1 已识别的不足

问题领域	NIS1 状况	NIS2 解决方案
范围认定	由成员国自主决定，实践中差异显著。	在欧盟范围内统一适用"规模上限"规则（中型和大型企业）。
行业清单	纳入行业数量有限，数字经济的重要部分被排除在外。	大幅扩展行业覆盖范围，纳入数字基础设施、公共行政、航天等领域。
事件报告	单阶段报告，截止时间和内容因成员国而异。	多阶段报告：24小时预警 + 72小时通报 + 1个月最终报告。
风险管理	措辞笼统，具体最低措施不明确。	Article 21 列明10项强制性最低措施类别。
处罚	各成员国处罚水平差异极大。	在欧盟范围内统一设定最高罚款上限（1000万欧元或营业额的2%）。
高级管理层责任	规定不明确。	管理机构对合规承担个人责任，须强制参加培训。

NIS2 并非对NIS1的修订，而是一次整体替代，旨在建立**覆盖全欧盟的统一且可执行的网络安全框架**。

4. 适用范围与除外领域

该指令主要适用于在欧盟境内**Annex I（高度关键）**或**Annex II（其他关键）**行业运营、且至少符合中型企业定义的实体。根据《委员会建议2003/361/EC》附件第2条，中型企业是指员工人数少于250人、年营业额不超过5000万欧元（或资产负债表总额不超过4300万欧元）的企业。NIS2 适用于达到或超过中型企业门槛的实体：纳入范围的实际最低门槛为员工50人或营业额1000万欧元（即同一建议中"小型企业"的上限）。

不论规模均须纳入的实体

- 公共电子通信网络提供商及公众可用电子通信服务提供商；
- 信任服务提供商（依据eIDAS Regulation EU 910/2014）；
- 顶级域名（TLD）注册机构及DNS服务提供商；
- 在某成员国内属于某项服务唯一提供者、或服务中断可能对公共安全、健康或人身安全产生重大影响的实体；
- 所有中央公共行政实体（由各成员国自行界定）。

除外领域

主要从事**国家安全、公共安全、国防或执法**（犯罪行为的预防、调查、侦查和起诉）活动的公共实体，不适用本指令。成员国驻第三国的外交及领事代表机构，以及在封闭系统中使用的信任服务，同样被排除在适用范围之外。

5. 关键定义

正确理解指令中的若干基本概念至关重要。

术语	定义
网络和信息系统	电子通信网络、处理数字数据的任何设备或设备组，以及为运营、使用、保护和维护上述系统而处理的全部数字数据。
网络安全	保护网络和信息系统、用户及其他人员免受网络威胁所必需的全部活动。
事件	损害网络和信息系统中存储、传输或处理的数据，或通过该系统提供或访问的服务的可用性、真实性、完整性或保密性的事件。
重大事件	已造成或可能造成相关实体服务严重运营中断或财务损失，或已对其他自然人或法人造成或可能造成相当程度实质性或非实质性损害的事件。
网络威胁	可能损坏、破坏或以其他方式对网络和信息系统产生不利影响的任何潜在情况、事件或行为。
重大网络威胁	根据其技术特征，可以认定具有对实体的网络和信息系统、其用户或其他人员造成严重影响（包括实质性或非实质性重大损害）潜力的网络威胁。
漏洞	ICT产品或服务中可被网络威胁利用的弱点、易受攻击性或缺陷。
未遂事件	可能损害存储、传输或处理的数据，或通过网络和信息系统提供或访问的服务的可用性、真实性、完整性或保密性，但已被成功阻止未能发生的事件。
CSIRT	计算机安全事件响应团队，负责事件处置的技术团队。
ENISA	欧盟网络安全局，在指令实施中发挥核心咨询和支持作用。

6. 实体类别：重要实体与关键实体

指令将所有适用范围内的实体划分为两大类别，该划分决定了义务的适用方式及监督/执法制度的具体安排。

判定标准	关键实体	重要实体
所属行业	Annex I 高度关键行业	Annex II 其他关键行业（以及Annex I中的中型企业）
规模	大型企业（员工250人以上或年营业额超过5000万欧元）	中型企业（员工50至249人）
监督制度	事前监督与事后监督并行	仅在有证据或投诉时进行事后监督
最高行政罚款	1000万欧元或全球年营业额的2%（取较高者）	700万欧元或全球年营业额的1.4%（取较高者）
高级管理层制裁	可适用临时管理禁令	不适用临时管理禁令

> **重要说明：** 若某实体在NIS1框架下已被认定为"基本服务运营商"，成员国可决定该实体直接认定为NIS2下的关键实体。此外，依据Directive 2022/2557（CER指令）被认定为"关键实体"的所有实体，在NIS2下自动被视为关键实体。

7. 适用范围内的行业（Annex I 与 Annex II）

Annex I，高度关键行业

上述行业中的大型企业为关键实体；中型企业为重要实体。

行业	子行业/实体类型
能源	电力（发电、输电、配电、供电）；区域供热/供冷；石油（管道、生产、储存、输送）；天然气；氢气的生产、储存和输送
交通运输	航空（航空公司、机场、空中交通管制）；铁路（基础设施管理方、铁路运营商）；水运（海上/内河运营商）；道路（智能交通系统、道路运营商）
银行业	依据Regulation (EU) 575/2013认定的信用机构
金融市场基础设施	交易场所（交易所）及中央对手方（CCP）
医疗卫生	医疗服务提供商；欧盟参考实验室；开展药品研发活动的实体；药品制造商；公共卫生紧急情况期间被认定为关键医疗设备的制造商（依据Regulation (EU) 2022/123）
饮用水	供应和分发供人饮用水的实体
废水处理	收集、处置或处理城市污水、生活污水或工业废水的实体
数字基础设施	互联网交换点（IXP）；DNS服务提供商（不含根DNS）；TLD注册机构；云计算服务提供商；数据中心服务提供商；内容分发网络（CDN）提供商；信任服务提供商；公共电子通信网络/服务提供商
ICT服务管理（B2B）	托管服务提供商（MSP）；托管安全服务提供商（MSSP）
公共行政	由成员国界定的中央和区域政府实体
航天	由成员国或私营部门运营的地面基础设施运营商

Annex II，其他关键行业

行业	子行业/实体类型
邮政和快递	邮政服务提供商（含快递服务）
废物管理	提供废物收集、回收和处置服务的实体
化工	从事化学品生产、加工和分销的实体
食品	从事食品生产、加工和批发分销的大型企业
制造业	医疗器械/体外诊断医疗器械；计算机、电子和光学产品；电气设备；机械和设备（其他未分类）；机动车辆、拖车及半拖车；其他运输设备制造
数字提供商	在线市场；在线搜索引擎；社交网络服务平台
科研	以商业为目的开展研究的科研机构

8. 成员国义务

该指令不仅对私营部门实体规定义务，也对成员国本身规定了义务。每个成员国须采取以下措施：

国家网络安全战略。 制定具有明确战略目标、优先事项和治理框架的国家网络安全战略，涵盖供应链安全、勒索软件应对、中小企业支持、开源安全及主动网络防御等议题。

主管部门。 指定或设立一个或多个主管部门，负责确保指令的实施和监督。

单一联络点（SPOC）。 指定一个单一联络点，负责欧盟层面的跨境协调工作。

CSIRT。 建立或指定一个或多个CSIRT，负责事件处置、主动监测、协调漏洞披露以及国内外合作。

实体清单。 维护、定期更新并向欧盟委员会报送关键实体、重要实体及提供域名注册服务的实体清单。

协调漏洞披露。 指定CSIRT担任协调机构，为漏洞研究人员提供法律明确性。

相互援助。 在跨境监督和执法事项上向其他成员国提供相互援助。

中小企业支持。 为小型和微型企业提供指导、免费工具及国家/区域联络点。

9. 网络安全风险管理措施（Article 21）

Article 21 是该指令中最重要的技术性条款。它列明了关键实体和重要实体必须实施的最低技术、运营和组织措施，所采用的方式基于**"全灾害"视角**，不仅涵盖网络攻击，还涵盖物理损坏、自然灾害、设备故障和人为失误等威胁。

Article 21，十项最低措施

编号	措施	说明
1	风险分析与信息系统安全策略	对所有风险进行分析，并以书面形式制定通用信息安全策略。
2	事件处置	建立事件预防、检测、响应和恢复流程。
3	业务连续性	备份管理、灾难恢复和危机管理。
4	供应链安全	涵盖供应商的安全实践；在与直接供应商的合同中纳入网络安全条款。
5	网络和信息系统的采购、开发和维护安全	全生命周期安全保障，包括漏洞处理与披露。
6	措施有效性评估	定期评估风险管理措施的有效性。
7	基本网络卫生实践与安全培训	网络卫生实践以及面向员工的安全意识培训。
8	密码学与加密	加密使用策略；在适当情况下采用端对端加密。
9	人力资源安全、访问控制与资产管理	人员安全审查、授权管理与资产清单。
10	多因素认证与安全通信	在适当情况下使用MFA、持续身份验证、安全的语音/视频/文字通信，以及紧急情况下的安全通信系统。

上述措施依据**比例原则**实施，综合考量实体的风险敞口、规模、行业重要性及事件的潜在影响。

10. 事件报告义务（Article 23）

指令中最重要的运营创新在于多阶段事件报告制度。关键实体或重要实体须在以下时限内，向CSIRT或主管部门报告**重大事件**，即造成严重运营中断、财务损失或对其他人员产生重大影响的事件。

阶段	截止时间	报告内容
预警	知悉事件后24小时内	怀疑事件由非法/恶意行为引起；跨境影响的可能性；使CSIRT能够知悉的基本信息。
事件通报	知悉事件后72小时内	对预警的更新；事件严重程度、影响范围，以及可获取的入侵指标（IoC）。
中期/最终报告	事件通报后不超过1个月	对事件的详细描述，包括严重程度和影响范围；所利用威胁的类型；已采取和计划采取的缓解措施；跨境影响（如有）。
进度报告	若最终报告到期时事件仍在持续	就事件当前状态提交进度报告；待事件处置完成后1个月内提交最终报告。

向服务接受者发出通知： 当重大网络威胁可能发生时，实体须及时且免费地向其服务接受者通报可能的缓解措施，并在适当情况下以清晰易懂的语言告知威胁本身。

未遂事件与自愿报告

除强制报告义务外，实体**可自愿向CSIRT或主管部门报告未遂事件和重大网络威胁**。不在指令适用范围内的实体也可自愿报告。自愿报告不为报告方带来额外义务。

> **实践影响：** 24小时预警要求迫使实体在事件被发现后能够立即启动网络事件响应计划和通信流程。依赖手动和碎片化流程在规定时限内完成报告极为困难。

11. 供应链安全

近年来，大多数重大网络攻击并非直接攻击目标组织，而是通过供应商和软件提供商渗透进来。因此，该指令将供应链风险置于风险管理义务的核心位置。

- 实体须评估其供应商和服务提供商产品/服务的**质量、安全实践及安全开发流程**。
- **与直接供应商的合同中必须包含网络安全要求。**
- 在选择**托管安全服务提供商（MSSP）**时须格外审慎；这类提供商是攻击者的高价值目标。
- 合作组与欧盟委员会及ENISA共同对关键供应链开展**协调安全风险评估**（此前已就5G网络开展过类似评估）。
- **非技术性风险因素**同样纳入评估范围，包括第三国对供应商的潜在不当影响、隐藏漏洞/后门，以及对提供商的依赖性风险。

12. 管理机构责任

该指令确保网络安全事务不再仅局限于技术部门，而是纳入**高级管理层的直接责任范畴**。根据 Article 20，关键实体和重要实体的管理机构：

- 负责**批准** Article 21 规定的风险管理措施，并监督其实施；
- 可就违反上述义务的行为**承担个人法律责任**；
- 须定期接受网络安全培训，以掌握充分的知识和技能；
- 应鼓励员工参加类似培训。

> **重要说明：** 对于关键实体，主管部门可申请对高级管理层（首席执行官或法定代表人级别）实施**临时管理禁令**。该措施为最后手段，仅在穷尽所有其他执法选项后方可适用。

13. 欧盟层面的合作机制

该指令规范或强化了确保成员国间有效合作的各类机制：

机制	职能
合作组	支持战略层面的合作；制定两年期工作计划；发布指导文件；对关键供应链开展协调风险评估。
CSIRT 网络	运营层面的合作；事件信息共享；相互援助；联合响应。
EU-CyCLONe	欧洲网络危机联络组织网络；在大规模事件和危机中连接技术与政治层面；开展影响分析。
ENISA	建立并维护欧洲漏洞数据库；提供技术支持；制定指导文件；监测成员国网络卫生政策。
IPCR 安排	欧盟综合政治危机响应安排（Council Implementing Decision 2018/1993），应对大规模危机的欧盟层面危机管理机制。
EU-CSIRT 协调漏洞披露协调员	每个成员国指定一个CSIRT担任协调员，负责管理跨境协调漏洞披露工作。

与第三国的合作： 欧盟可依据TFEU Article 218与第三国或国际组织签订国际协议。此类协议在维护欧盟利益和数据保护的前提下，可允许相关方参与合作组、CSIRT 网络或EU-CyCLONe的活动。

14. 监督与执法

该指令针对两类实体规定了不同的监督制度。**关键实体**同时适用事前监督和事后监督；**重要实体**仅在有证据或投诉时进行事后监督。

主管部门的监督权力

- 开展现场检查和远程监督；
- 要求进行定向安全审计（实体可能须承担相关费用）；
- 下令开展安全扫描；
- 要求提供合规风险管理措施的证明文件；
- 要求提供涉嫌违反指令行为的相关信息；
- 在必要时要求提供涉及个人数据和流量数据访问权限的相关信息。

可采取的执法措施

- 发出警告和具有约束力的指令；
- 在规定期限内下令采取具体措施或修复漏洞；
- 下令开展独立审计以核实风险管理措施；
- 要求实体告知服务接受者违规行为的性质；
- 发表公开声明（披露实体名称及违规性质）；
- 对关键实体（最后手段）：暂停认证或授权资质，并对高级管理层实施临时管理禁令；
- 处以或申请处以行政罚款。

15. 行政罚款

该指令为成员国所适用的行政罚款设定了**欧盟统一的最高门槛**。与GDPR类似，上述门槛与实体的全球营业额挂钩。

实体类型	最高金额（取较高者）
关键实体	1000万欧元或全球年营业额的2%
重要实体	700万欧元或全球年营业额的1.4%

确定罚款金额的考量因素

- 违规行为的性质、严重程度和持续时间；
- 已造成的实质性或非实质性损害；
- 违规行为系故意还是过失；
- 为防止或减轻损害所采取的措施；
- 责任程度及过往违规记录；
- 与主管部门的合作程度；
- 其他加重或减轻情节。

罚款须遵循**比例原则**，在适用过程中须保障辩护权、无罪推定及获得有效救济权等基本权利。成员国也可就违反国内法的行为规定刑事制裁；但任何人不得就同一行为被处罚两次，以遵守**一事不再罚**（ne bis in idem）原则。

16. 实施时间表与过渡安排

日期	事件
2022年12月14日	欧洲议会和欧盟理事会通过指令
2022年12月27日	在欧盟官方公报发布（OJ L 333/80）
2023年1月16日	指令生效（发布后第20天）
2024年10月17日	成员国将指令转化为国内法的截止日期
2024年10月18日	指令开始适用
2024年10月18日	Directive (EU) 2016/1148（NIS1）正式废止
2025年4月17日	成员国向欧盟委员会报送关键实体和重要实体清单的截止日期
2027年10月17日起	欧盟委员会对指令实施情况开展定期审查（每36个月一次）

> **重要说明：** NIS2 是一项指令，不具有直接适用效力。每个成员国须将其转化为本国法律。因此，适用于特定实体的具体义务和处罚取决于该实体所在成员国通过的国内转化法案。

17. 对欧盟以外企业的影响

尽管NIS2 是一项欧盟指令，但对欧盟以外的企业，尤其是服务欧盟市场或向欧盟关键实体供货的企业，具有重大影响。

直接受影响的欧盟以外企业

- 在欧盟提供服务的非欧盟**DNS提供商、云服务提供商、数据中心运营商、CDN提供商、托管服务和托管安全服务提供商、在线市场、搜索引擎及社交网络平台**，须指定欧盟代表并遵守指令义务；
- 在欧盟设有子公司或分支机构的非欧盟企业，可能通过上述单位受到指令约束；
- 向欧盟关键实体或重要实体提供产品/服务的非欧盟供应商，将须遵守客户依据 Article 21(2)(d) 提出的**供应链安全合同要求**；
- 服务于欧盟数字基础设施或金融实体的非欧盟MSP/MSSP，可能直接落入指令适用范围。

间接影响

- 欧盟客户的供应链风险评估将迫使非欧盟供应商提升自身网络安全标准；
- 指令引入的标准（ISO/IEC 27001、ENISA 指导文件等）正逐渐成为全球市场的**事实参考基准**；
- 非欧盟司法管辖区在制定本国网络安全法规时，越来越多地将NIS2 作为参考依据。

18. 实际合规路线图（10个步骤）

以下10步路线图可作为在欧盟经营的企业及希望自愿对标NIS2 标准的企业的实践指南。

步骤	活动
1. 范围认定	确定企业是否属于Annex I 或Annex II 行业，是否满足规模标准，并确定其类别（关键/重要）。
2. 差距分析	对照 Article 21 的10项措施类别评估现有信息安全管理体系，梳理差距。
3. 治理架构	在董事会/高级管理层层面明确职责、汇报路径和审批流程，建立定期培训机制。
4. 政策与文档	制定或更新信息安全政策、风险管理政策、事件响应政策、可接受使用政策及其他相关文件。
5. 风险评估	开展资产清查、威胁分析，以全灾害方式进行风险评估，制定风险接受标准。
6. 技术控制措施实施	部署MFA、加密、网络分段、零信任架构、日志管理、SIEM、EDR/XDR、备份和灾难恢复方案。
7. 事件响应能力建设	编制事件响应计划，明确角色和职责，建立24小时预警通信流程，开展桌面推演。
8. 供应链管理	建立供应商清单，按风险等级分类，在合同模板中加入网络安全条款，定期开展审计。
9. 培训与意识提升	每年面向全体员工开展网络卫生培训，为管理机构提供专项培训，开展网络钓鱼模拟演练。
10. 持续改进	开展内部和外部审计，跟踪KPI，从每次事件中汲取经验，每年更新风险评估，推进认证工作（ISO/IEC 27001、欧盟网络安全认证）。

19. 结论与评估

NIS2 指令大幅提升了欧盟的网络安全基准。它不仅规定了技术要求，还将网络安全纳入**企业治理结构和业务运营的有机组成部分**。

指令的优势

- **覆盖面广**：欧盟27国范围内约涵盖18个行业，超过10万家实体纳入管辖；
- **统一标准**：通过在欧盟范围内统一认定标准和执法制度，为内部市场创造公平竞争环境；
- **治理导向**：通过追究高级管理层的责任，确保网络安全意识渗透企业各个层级；
- **供应链重视**：回应了现代攻击大多经由供应链渗透这一现实；
- **合作机制**：通过合作组、CSIRT 网络和EU-CyCLONe构建多层次的欧盟协调体系。

批评与挑战

- 成员国转化工作出现延迟和分歧，欧盟27国范围内的统一落实在实践中参差不齐；
- 特别是对中型企业而言，合规成本和缩小技术能力差距构成严峻挑战；
- 在尚未具备足够成熟度的情况下实施24小时预警截止要求，可能导致报告流程流于形式或出现偏差；
- 与行业性法规的重叠领域（DORA适用于金融业、eIDAS适用于信任服务、航空行业监管等）可能为相关实体带来合规复杂性。

综合评估

NIS2 将网络安全从技术议题重新定位为关乎**业务连续性、公司治理与客户信任**的核心事项。对于在欧盟运营或与欧盟存在业务往来的实体而言，合规既是法律义务，也是提升运营韧性的有效途径。

对于欧盟以外的企业，NIS2 正在确立进入欧盟市场的新**事实标准**，并在全球范围内提升对网络安全的预期水平。提前达到合规要求有助于履行合同义务，并全面改善网络韧性。

> **最终说明：** 本文件以中文读者为对象，对指令的主要条款进行摘要介绍。如需了解适用于贵组织的具体合规要求，请参阅官方文本（OJ L 333/80，2022年12月27日）、所在成员国的国内转化法案及行业专项法规，并在必要时咨询法律和网络安全专业顾问。

资料来源

- Directive (EU) 2022/2555，EUR-Lex CELEX编号32022L2555
- Official Journal of the EU L 333/80，2022年12月27日
- ENISA，欧盟网络安全局（www.enisa.europa.eu）
- 欧盟委员会数字战略门户（digital-strategy.ec.europa.eu）

Rediacc 关于NIS2的深度资源

本摘要梳理了指令的结构与义务。rediacc.com 上的配套指南将上述义务转化为具体的运营和采购决策。

三份配套指南

- **Article 21(2)(d) 与自托管。** 当数据平面从不离开您的租户时，第三方ICT登记册如何缩减。面向正在2026年重新谈判DPA的首席信息安全官和采购负责人。
- **无形式主义的持续有效性。** Article 21(2)(e)、(f) 与 Article 23 的综合解读。让每周演练切实可行的恒定时间分叉机制，以及若无法医级证据则无法满足的 Article 23 报告时间线。面向SRE和运营负责人。
- **NIS2 合规的结构性成本。** 中端市场关键实体正在悄然搭建的五工具技术栈、自托管控制平面可以整合的内容，以及无论如何都由您承担的费用项目。面向进入续约周期的CFO和采购方。

获取途径

上述三份指南及本摘要的可下载PDF版本，均可在以下地址获取：

rediacc.com/resources/nis2-directive-summary

Rediacc OÜ 是一家在爱沙尼亚注册的自托管基础设施平台（注册码17363830，增值税号EE102920091）。该产品不能替代安全计划，而是一个工具层，用于消除传统备份、灾难恢复和测试数据工具无法消除的数据平面供应商风险。免费社区版及付费版本起价349美元/月。

> 本文件及配套指南仅供学习参考。针对贵组织的具体合规决策，须咨询法律顾问，并参考所在司法管辖区的国内转化法案。