KOŠICKA BEZPEČNOSTNÁ REVUE

KOSICE SECURITY REVUE

Vol. 16, No. 1 (2026), p. 12 – 23

ISSN 1338-4880 (print ver.), ISSN 1338-6956 (online ver.)

Cybersecurity Due Diligence as Legal Defence: Using Risk Management Evidence to Reduce Corporate and Managerial Liability in the EU

Odborná starostlivosť v kybernetickej bezpečnosti ako právna obrana: využitie dôkazov z riadenia rizík na zníženie zodpovednosti organizácie a manažmentu v EÚ

Július HANDLOVSKÝ[1]

[1]*The University of Security Management in Košice*

The manuscript was received on 19.01.2026 and was accepted after revision for publication on 09.02.2026

Abstract:

Cyber incidents increasingly trigger not only operational disruption but also regulatory enforcement, civil claims, and reputational harm. In this environment, "due diligence" in cybersecurity becomes a legal question: what an organisation and its management can prove they did before, during, and after an incident. This article argues that risk management is most valuable when designed for defensibility—i.e., when governance and documentation can demonstrate compliance with EU data protection and cybersecurity expectations and help mitigate corporate and managerial liability. Building on a doctrinal analysis of EU accountability concepts and cybersecurity duties, the paper maps legal expectations to concrete, auditable artefacts: risk registers and treatment plans, security policies and controls, training and awareness records, supplier and cloud risk documentation, incident response playbooks, incident logs, post-incident reviews, and (where relevant) impact assessments. Using short illustrative scenarios, the article shows how gaps in evidence—not only gaps in controls—often drive adverse legal outcomes. The paper concludes with a minimal "defensible set" of documentation and governance practices that supports credible claims of professional cybersecurity care and strengthens an organisation's liability position.

Keywords: *cybersecurity due diligence; managerial liability; accountability; risk management documentation; incident response evidence; GDPR compliance; NIS2 obligations; defensibility; corporate governance*

Abstrakt:

Kybernetické incidenty čoraz častejšie nevyvolávajú iba prevádzkové výpadky, ale aj regulačné zásahy, civilnoprávne nároky a reputačné škody. V tomto prostredí sa „due diligence" v kybernetickej bezpečnosti stáva právnou otázkou: čo vie organizácia a jej manažment preukázať, že urobili pred incidentom, počas incidentu a po incidente. Článok vychádza z tézy, že riadenie rizík je najhodnotnejšie vtedy, keď je navrhnuté s ohľadom na obhájiteľnosť – teda keď riadenie a dokumentácia umožňujú preukázať súlad s požiadavkami EÚ v oblasti ochrany osobných údajov a kybernetickej bezpečnosti a tým zmierniť právnu zodpovednosť organizácie a manažmentu. Na základe doktrinálnej analýzy konceptu zodpovednosti a povinností v právnom rámci EÚ článok mapuje právne očakávania na konkrétne preukázateľné výstupy: register rizík a plán ich ošetrenia, bezpečnostné politiky a kontrolné mechanizmy, záznamy o školeniach, dokumentáciu riadenia rizík dodávateľov a cloudu, postupy reakcie na bezpečnostné udalosti, incidentné logy, post-incidentné vyhodnotenia a (ak je relevantné) posúdenia dopadov. Pomocou krátkych ilustračných scenárov článok ukazuje, že nepriaznivé právne dôsledky často spôsobujú nie iba nedostatky v opatreniach, ale aj nedostatky v dôkazoch. Záver prináša minimálny „obhájiteľný balík" dokumentácie a postupov správy a riadenia, ktorý podporuje tvrdenie o odbornej starostlivosti v kybernetickej bezpečnosti a posilňuje pozíciu organizácie pri posudzovaní zodpovednosti.

Kľúčové slová: *odborná starostlivosť v kybernetickej bezpečnosti; zodpovednosť manažmentu; zodpovednosť a preukazovanie; dokumentácia riadenia rizík; dôkazy pri riešení incidentov; súlad s GDPR; povinnosti podľa NIS2; obhájiteľnosť; správa spoločnosti*

Introduction

Cybersecurity incidents have matured from being a purely technical disruption into a multi-layered legal event. [10] When systems fail, data is exposed, or services are unavailable, organisations increasingly face parallel consequences: regulatory scrutiny, administrative sanctions, contractual disputes, civil claims for damages, and—depending on governance and decision-making—questions about individual responsibility within management.

This article starts from a practical legal observation: in the EU compliance environment, cybersecurity is increasingly judged through the lens of accountability and risk-based "appropriate measures". The applicable legal logic rarely prescribes a single "correct" technical solution; instead, it requires organisations to adopt and maintain organisational and technical measures proportionate to risk and to be able to demonstrate responsible governance and control over relevant processes.[1] In parallel, EU cybersecurity rules emphasise cybersecurity risk-management measures and structured obligations around incident handling and reporting.[5]

As a result, cybersecurity due diligence becomes inseparable from evidence—policies, decisions, records, and traceable governance that can withstand ex post review by regulators, courts, auditors, business partners, and insurers. Against this backdrop, risk management is frequently implemented as a management routine or certification exercise. Yet its core legal value lies in **defensibility**: the ability to credibly reconstruct and justify how risks were identified and prioritised, why controls were selected, how responsibilities were assigned and supervised, and how incidents were handled, documented, and learned from.[9]

The objective of this paper is therefore practical and legal at the same time: to translate EU-facing cybersecurity and data-protection expectations into a set of **audit-ready, court-ready artefacts** and governance practices that support a due diligence narrative.

The focus is not on proposing new technical controls, but on explaining how documentation and governance can function as a legal shield—mitigating corporate exposure and reducing the likelihood that managerial conduct is characterised as negligent, careless, or organisationally deficient.

Methodologically, the article adopts a doctrinal approach supported by practice-oriented reasoning. It maps legal expectations of accountability and "appropriate measures" to concrete evidence objects: risk registers and treatment plans; internal policies and control baselines; training and awareness records; supplier and cloud risk documentation; incident response plans and logs; and post-incident reviews.[1][9] Short illustrative scenarios demonstrate a recurring pattern: adverse legal outcomes often hinge on gaps in evidence (missing decisions, unclear ownership, inconsistent records), not merely on gaps in technology.

1. The legal logic of cybersecurity due diligence: accountability, risk-based measures, and evidence

Cybersecurity due diligence in the EU is best understood as an **accountability problem**: the law expects organisations to implement measures that are appropriate to risk and, crucially, to be able to **demonstrate** that appropriateness through governance and records. This is not a purely formal requirement. In enforcement and dispute contexts, the decisive question is often whether the organisation can credibly show how it assessed risk, selected measures, assigned responsibilities, and supervised execution—before the incident forced scrutiny.

1.1 Accountability as an evidentiary standard (GDPR as the archetype)

EU data protection law illustrates the evidentiary nature of due diligence particularly clearly. The GDPR's accountability principle requires that compliance is not only achieved but also **provable** through organisational arrangements and documentation.[1] In the security context, the GDPR frames security of processing as a risk-based obligation: controllers and processors must implement "appropriate technical and organisational measures" taking into account context, costs, state of the art and—most importantly—risk to rights and freedoms.[1] This structure has two immediate consequences for cybersecurity due diligence.

First, the legal standard is **open-textured**: it does not mandate a single control set for all organisations. Second, because the standard is contextual, the organisation's **decision trail** becomes legally material. The organisation must be able to explain *why* selected measures were appropriate to its processing operations and threat landscape, and how those measures were maintained over time.[1] Without this evidentiary layer, compliance becomes difficult to defend even when some controls existed in practice.

1.2 From "security measures" to "risk-management measures" (NIS2 and implementing requirements)

While the GDPR focuses on personal data and risk to individuals, the EU cybersecurity framework increasingly stresses structured **cybersecurity risk-**

management measures and organisational readiness. The NIS2 Directive formalises this shift by requiring covered entities to adopt risk-management measures and to handle incidents through defined processes, including reporting obligations.[5] The legal significance is that "security" is treated not as a static technical state, but as an **ongoing governance duty**.

This is reinforced by more technical EU-level specification for certain digital sectors through Commission Implementing Regulation (EU) 2024/2690, which sets detailed technical and methodological requirements for cybersecurity risk-management measures and further specifies when incidents are "significant" for the covered entity types listed in the regulation.[7] For due diligence analysis, this matters because the compliance benchmark becomes increasingly **testable**: regulators can compare an entity's measures and evidence against an articulated baseline.

ENISA's technical implementation guidance adds a practical compliance layer by translating these requirements into **implementation advice, examples of evidence, and mappings** that organisations can use to structure controls and documentation.[9] In other words, the due diligence question becomes less about whether an organisation can claim it "takes cybersecurity seriously" and more about whether it can present evidence that it follows a coherent, risk-based governance model aligned with EU expectations.[5][7][9]

1.3 National cyber regimes as early "documentation-heavy" models (Slovak example)

National cybersecurity regimes pre-dating NIS2 often already reflected the same evidentiary logic: compliance is inseparable from structured documentation. Slovakia's Cybersecurity Act (Act No. 69/2018 Coll.) is a useful example of a framework that operationalises cybersecurity through defined roles, obligations, and oversight mechanisms.[2] Implementing rules have historically required a recognisable set of security measures and accompanying documentation structures, making the "paper trail" a core part of cyber compliance rather than a secondary artefact.[3]

The broader point for this paper is not to compare national transpositions in detail, but to emphasise a consistent legal pattern: as cybersecurity law matures, it increasingly evaluates organisations through **governance maturity** and **evidentiary readiness**, not only through post-incident technical remediation.

1.4 What counts as "due diligence" in practice: why evidence is often the missing control

From a liability and enforcement perspective, "due diligence" is rarely lost because a single technical control was imperfect. It is often lost because the organisation cannot show:

a) that risks were identified and prioritised in a systematic way,

b) that control choices followed an articulated rationale,

c) that responsibilities were clearly owned and supervised,

d) that testing, monitoring, and improvement occurred,

e) that incident response was executed according to a prepared plan and recorded consistently.

EDPB materials illustrate how supervisory authorities interpret security obligations and data breach scenarios in real cases, revealing recurring evidentiary weaknesses (e.g., unclear accountability, inadequate records, inconsistent breach handling).[8] EDPB breach-notification guidance further underscores that incident handling is not merely operational; it is procedural and evidence-driven, because the organisation must justify decisions, timelines, and risk assessments when notifying (or deciding not to notify).[6]

This is the bridge to the article's central thesis: **risk management documentation is not "bureaucracy"; it is legal infrastructure.** It turns cybersecurity activity into defensible due diligence by creating an auditable narrative of professional care, aligned with EU expectations and increasingly shaped by sector-specific implementing requirements.[1][5][7][9]

2. A defensibility-oriented evidence map: what "professional cybersecurity care" looks like on paper

If cybersecurity due diligence is assessed *ex post*, then evidence is the organisation's main interface with law. Regulators, courts, auditors, and business partners rarely reconstruct an incident from engineering telemetry alone; they reconstruct it from **governance traces**: decisions, responsibilities, approvals, logs, and records. This section therefore proposes an **evidence map**—a structured set of artefacts that translate the EU's risk-based and accountability-driven expectations into audit-ready documentation.

The aim is not to create "paper compliance", but to ensure that security work is **legible** in legal terms: what was known, what was decided, by whom, and on what rationale.

2.1 The legal function of evidence: from controls to justifiable decisions

EU obligations in data protection and cybersecurity are predominantly **reasonableness standards**. The GDPR requires "appropriate" organisational and technical measures and expects accountability that can be demonstrated.[1] NIS2 similarly frames cybersecurity as a set of risk-management duties and incident-handling obligations.[5] For certain digital providers, the Implementing Regulation further specifies technical and methodological requirements—effectively increasing the evidentiary burden by making expectations more concrete.[7] ENISA guidance explicitly operationalises this by providing practical advice and examples of evidence aligned with these EU-level requirements.[9]

In such a framework, the decisive question is often not "Did the organisation have *any* controls?" but "Can the organisation show a rational, risk-based path from **risk identification → control selection → control operation → incident handling → learning**?"[1][5][7][9]

2.2 Core evidence domains

A defensible cybersecurity posture is usually evidenced through six interlocking domains. Each domain should produce artefacts that are coherent, current, and internally consistent.

a) Governance and accountability evidence

This domain answers: **Who is responsible, and how is responsibility supervised?**

Minimal defensible artefacts typically include:

i. a defined security governance structure (roles, reporting lines, decision rights);

ii. management-approved security policies (and a record of versioning and communication);

iii. evidence of oversight (management minutes, risk committee notes, security reporting cadence);

iv. assignment of operational responsibility (RACI-type clarity), including escalation paths.

This domain directly supports GDPR-style accountability claims and reduces the risk that failures are characterised as organisational negligence.[1] It also aligns with NIS2's expectation that cybersecurity is embedded as a management-level responsibility rather than delegated informally to technical staff.[5]

b) Risk assessment and risk treatment evidence

This domain answers: **What risks were recognised and what was done about them?**

A defensible set generally includes:

i. a risk methodology (criteria, scales, assumptions, review cycle);

ii. a risk register with ownership, ratings, and rationales;

iii. a risk treatment plan showing selected controls, target dates, and residual risk acceptance;

iv. formal risk acceptance decisions for high residual risks (signed and dated).

This is where "appropriate measures" becomes explainable: the organisation can demonstrate that measures were chosen proportionately and reviewed periodically.[1] It also creates a bridge to sector-specific expectations under NIS2 and its implementing requirements where applicable.[5][7]

(Note: ISO/IEC 27001 is not a legal source, but it is often used as a defensibility scaffold because it demands risk-based control selection and continuous improvement, which can support an evidence narrative when organisations claim structured governance.)[4]

c) Operational control evidence

This domain answers: **Were controls actually implemented and maintained?**

Here, "evidence" means more than a policy PDF. Examples include:

i. control baselines (e.g., secure configuration standards);

ii. access management records (joiner/mover/leaver, privileged access reviews);

iii. patching and vulnerability management records (prioritisation, exceptions, remediation timelines);

iv. logging and monitoring standards plus evidence of routine review.

ENISA's guidance is particularly useful here because it connects abstract requirements to concrete evidence examples for implementation and verification.[9] For entities within scope of the Implementing Regulation, the evidentiary value of this domain increases because expectations are more prescriptive and therefore easier to benchmark in enforcement contexts.[7][9]

d) Supplier and cloud risk evidence

This domain answers: **What was outsourced, and how was that risk controlled?**

A defensible package typically includes:

i. supplier risk assessment templates and completed assessments for critical vendors;

ii. contractual security clauses (including incident notification, audit rights, sub-processor controls where relevant);

iii. documented onboarding/offboarding and periodic reassessment;

iv. evidence of assurance (audit reports, certifications, attestation letters) proportionate to risk.

This domain is frequently decisive in real incidents because third-party failures are common while accountability remains with the organisation that depends on the supplier.[1][9]

e) Incident response and breach-handling evidence

This domain answers: **How did the organisation respond, and can it justify timelines and decisions?**

At minimum, a defensible system includes:

i. an incident response plan and playbooks (with roles, thresholds, and communications);

ii. incident logs and decision logs (time-stamped, with escalation and containment actions);

iii. post-incident reviews (lessons learned and control improvements).

For personal data breaches, EDPB breach-notification guidance highlights the need for structured internal handling and decision-making, because organisations must justify assessments and, where required, notifications.[6] The EDPB case digest similarly illustrates how authorities evaluate security-of-processing and breach scenarios in practice, with repeated attention to governance weaknesses and inadequate evidence trails.[8]

f) Training, awareness, and competence evidence

This domain answers: **Was staff prepared, and is security operationally embedded?**

A defensible baseline includes:

i. training plans and attendance records (with role-based differentiation);

ii. evidence of communication of policies and key procedures;

iii. exercises and simulations (table-tops), especially for incident handling.

This supports the narrative that measures were not merely designed but operationalised in the organisation's human processes—an aspect repeatedly relevant in real-world enforcement and incident post-mortems.[1][6][8]

2.3 Quality criteria: what makes evidence "court-ready"

Not all documentation is defensible. Three quality criteria consistently separate credible evidence from compliance theatre:

a) **Traceability:** each artefact should connect to a risk, a decision, or an obligation (and not exist as an orphan template).

b) **Currency:** review cycles are documented and respected; outdated policies often weaken credibility.

c) **Consistency:** risk registers, policies, incident logs, and training records tell the same story about responsibilities and priorities.

Where national regimes already impose structured documentation (as in Slovakia's cyber framework and implementing documentation requirements), these criteria become even more important, because the expected documentation is not merely best practice but an element of compliance itself.[2][3]

2.4 Interim conclusion: the "minimal defensible set"

Combining the domains above, the **minimal defensible set** can be summarised as: governance clarity + risk register/treatment plan + proof of operating controls + supplier controls + incident evidence + training and review. This set is deliberately modest: it does not demand perfect security, but it does demand **legible professional care**, aligned with EU accountability logic and increasingly detailed cybersecurity expectations.[1][5][7][9]

3. When liability turns on evidence: three scenarios and the "minimal defensible set"

This final chapter demonstrates a recurring enforcement-and-dispute pattern: organisations do not lose the "due diligence narrative" solely because a control failed, but because they cannot **reconstruct and justify** decisions, responsibilities, and timelines with credible evidence.[1][6][8] The scenarios below are simplified, but they mirror typical fact patterns in which regulators and counterparties focus on **governance**

traceability rather than technical sophistication.[8] The chapter ends with a compact "minimal defensible set" that can be implemented proportionately.

3.1 Scenario A: Ransomware and service outage (availability + incident reporting)

Fact pattern (typical): A ransomware incident disrupts critical systems for multiple days. The organisation restores from backups, but the business impact is severe. Later, questions arise: Were backups tested? Was patching delayed? Was monitoring adequate? Were incident decisions documented?

Legal exposure (EU logic): Even where the GDPR is the primary legal frame, availability and resilience are part of "appropriate technical and organisational measures" for security of processing.[1] Where NIS2 applies, the same incident may trigger cyber risk-management expectations and structured incident handling/reporting duties at the organisational level.[5] In sectors covered by more detailed implementing requirements, the compliance benchmark becomes easier to test against a defined baseline.[7]

Evidence that strengthens the defence:

a) backup policy + **restore test records** (dates, results, remedial actions)

b) vulnerability/patch management records showing prioritisation and exception handling

c) security monitoring/alert handling logs showing detection and escalation

d) an incident decision log (containment, isolation choices, business continuity steps)

Why organisations lose defensibility: The most damaging gap is usually not "we had no backup," but "we cannot prove we *maintained* our backup and recovery capability." ENISA's implementation guidance and threat landscape reporting both implicitly reinforce this: preparedness is assessed through repeatable processes and evidence of execution, not slogans.[9][11] In practice, a thin or inconsistent evidence trail invites the conclusion that governance was weak or merely paper-based.[8]

3.2 Scenario B: Cloud/SaaS supplier compromise (outsourcing does not outsource accountability)

Fact pattern (typical): A key SaaS provider suffers an intrusion that exposes customer data or disrupts services. The affected organisation argues it was "the vendor's fault."

Legal exposure (EU logic): Under the GDPR, accountability and security obligations remain legally material for the organisation depending on its role (controller/processor) and the concrete processing arrangement.[1] NIS2 and related EU expectations increasingly treat supply-chain controls as part of cyber risk management and operational resilience.[5] What matters legally is whether the organisation exercised

governed supplier risk management that is proportionate to the criticality of the vendor relationship.[9]

Evidence that strengthens the defence:

a) vendor risk assessments showing criticality classification and required controls

b) contractual clauses (incident notification, cooperation, audit/assurance rights, sub-supplier controls)

c) onboarding/offboarding records; periodic reassessments

d) assurance evidence (independent audits/certifications/attestations), where proportionate

Regional anchoring (CZ practice tool): The Czech national guidance for the new cyber regime explicitly frames compliance implementation around risk management, incident handling, and organisational preparedness—reinforcing that oversight of regulated services and dependencies is not an optional formality.[13] Even where a document is not "academic literature," it is valuable as an authoritative, practitioner-facing interpretation of how duties are expected to be operationalised.

Why organisations lose defensibility: They cannot show a structured vendor governance trail - only a procurement file and a generic DPA. In litigation terms, the organisation looks passive: it relied on marketing claims rather than risk-based oversight.

3.3 Scenario C: Misconfiguration and personal data breach (breach handling as a procedural test)

Fact pattern (typical): A cloud storage bucket is misconfigured; personal data becomes publicly accessible or is exfiltrated. The organisation fixes the configuration quickly, but later faces scrutiny about breach assessment and notification decisions.

Legal exposure (EU logic): This scenario commonly becomes a test of (i) security governance (appropriate measures) and (ii) procedural integrity of breach handling. GDPR compliance requires risk-based security measures and accountability.[1] The EDPB's breach-notification guidance emphasises structured internal processes and reasoned decision-making because an organisation must be able to justify what happened, when it was detected, how risk was assessed, and why notification was (or was not) made.[6] The EDPB case digest illustrates that supervisory authorities repeatedly focus on evidence gaps around security-of-processing, governance clarity, and breach response consistency.[8]

Evidence that strengthens the defence:

a) secure configuration baseline + periodic configuration reviews

b) access control review records and change management logs

c) incident timeline (detection → containment → assessment → decision)

d) documented risk assessment for notification decisions (including rationale)

Why organisations lose defensibility: They treat breach handling as an ad hoc operational action ("we fixed it") rather than a governed legal process ("we assessed, decided, recorded, improved"). The absence of a coherent timeline and rationale is often more damaging than the underlying misconfiguration.[6][8]

3.4 The minimal defensible set (implementation-focused summary)

Across all three scenarios, the same "evidence spine" repeatedly determines whether due diligence is credible. A proportionate **minimal defensible set** therefore consists of:

a) **Governance & accountability:** clear roles, escalation paths, management oversight cadence (minutes/briefings). [1][5]

b) **Risk register + treatment plan:** ownership, rationale, review cycle, and signed risk acceptance where relevant. [1][9]

c) **Operational proof of controls:** patch/vulnerability management records, backup restore tests, monitoring and alert handling evidence. [7][9][11]

d) **Supplier & cloud governance:** risk-based vendor classification, contractual controls, assurance evidence, reassessments. [1][9][13]

e) **Incident response evidence:** playbooks + time-stamped decision logs + post-incident review and improvements. [5][6][8]

f) **Competence evidence:** role-based training records and exercises (table-tops), especially for incident handling. [6][8]

For Slovak practice, a key message used in national awareness and guidance materials is that cybersecurity responsibility ultimately sits with the statutory level of the organisation - not only with a security manager. That organisational framing supports the article's central thesis: defensibility is built (or lost) at the governance level.[12]

Conclusion

EU cybersecurity compliance is increasingly judged through **risk-based accountability** and, in parts of the digital economy, through more detailed implementing baselines.[1][5][7] In that setting, cybersecurity due diligence is inseparable from evidence: the organisation's ability to demonstrate structured risk governance, operationalised controls, supplier oversight, and procedurally sound incident handling.[6][8][9] The practical implication is straightforward: organisations should treat risk-management documentation not as paperwork, but as legal infrastructure that converts security work into defensible professional care - reducing corporate exposure and making managerial oversight demonstrably reasonable.

References:

[1] Regulation (EU) 2016/679 (General Data Protection Regulation), OJ L 119, 4.5.2016.

[2] Slovak Republic: Act No. 69/2018 Coll. on Cybersecurity (Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti).

[3] Decree of the National Security Authority of the Slovak Republic No. 362/2018 Coll. (Vyhláška NBÚ č. 362/2018 Z. z.).

[4] ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO/IEC, 2022.

[5] Directive (EU) 2022/2555 (NIS2 Directive), OJ L 333, 27.12.2022.

[6] European Data Protection Board (EDPB). *Guidelines 01/2021 on Examples regarding Personal Data Breach Notification*, adopted 3.1.2022.

[7] Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024.

[8] European Data Protection Board (EDPB). *One-Stop-Shop Case Digest on Security of Processing and Data Breach Notification*, 2024.

[9] ENISA. *Technical Implementation Guidance on Cybersecurity Risk Management Measures*, Version 1.0, June 2025.

[10] SAVIN, A. Cybersecurity. In: *EU Internet Law*. Cheltenham: Edward Elgar Publishing, 2025 (Chapter 12).

[11] ENISA. *ENISA Threat Landscape 2025*. European Union Agency for Cybersecurity, October 2025.

[12] Národný bezpečnostný úrad (NBÚ SR). *KYBER 2025* (PDF), 17 June 2025.

[13] NÚKIB. Průvodce novým zákonem o kybernetické bezpečnosti (online guidance), 1.November 2025.

Author:

[1]**JUDr. Július Handlovský, DBA–** full-time doctoral student**,** The University of Security Management in Košice, Košťova 1, 040 01 Košice, Slovak republic, e-mail: julter1@gmail.com