UNIWERSYTET Andrzeja Frycza Modrzewskiego w Krakowie

BEZPIECZEŃSTWO TEORIA I PRAKTYKA
SECURITY THEORY AND PRACTICE

e-ISSN 2451-0718
ISSN 1899-6264

2026
Nr 2

Copyright© 2026 by the Author(s)
This is an open access article under the CC BY-NC-ND 4.0 license

https://doi.org/10.31749/2451-0718-btip-2026-2-002
Received: 2.02.2026
Accepted: 30.08.2026

Cybersecurity Services: Definition and Relationship with Risk & Control Frameworks

Arkadiusz Rokicki

PhD, independent researcher
https://orcid.org/0000-0002-5621-2040

Introduction

In an era dominated by digital transformation, the proliferation of cyber threats has emerged as one of the most pressing challenges facing organizations worldwide. The rapid evolution of technology, coupled with increasing interconnectivity, has amplified vulnerabilities, making cybersecurity an indispensable facet of organizational resilience. This study examines the concept of cybersecurity services and their relationship with organizational risk and control (R&C) frameworks, addressing a significant gap in current literature.

Background and Rationale

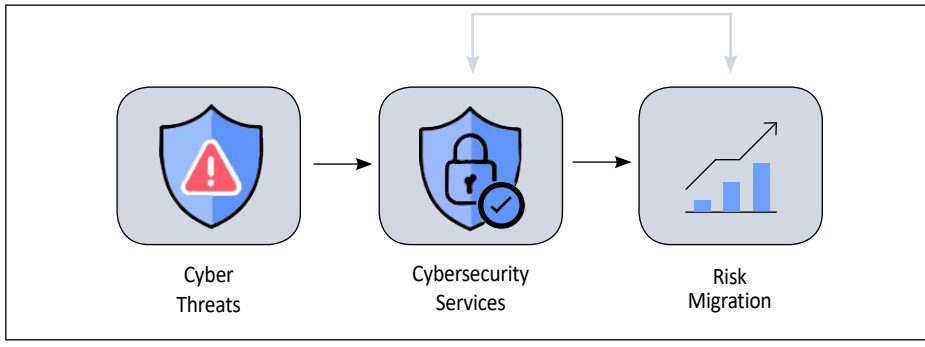
The landscape of cyber threats has intensified dramatically over the past decade, with incidents such as ransomware attacks and data breaches becoming commonplace. Ransomware, for instance, involves malicious software that encrypts an organization's data, rendering it inaccessible until a ransom is paid. These attacks not only disrupt operations but also inflict substantial financial and reputational damage. According to recent statistics, ransomware remains the predominant global cybersecurity threat, affecting 72.7% of organizations (*Cyberthreat Defense Report* 2024: 27). In 2025,

45% of surveyed respondents identified ransomware as their top organizational cyber risk (*Global Cybersecurity Outlook* 2025: 12), underscoring its persistence despite advancements in defensive measures.

The financial repercussions of such incidents are staggering. The IBM Cost of a Data Breach Report 2025 reveals that the global average cost of a data breach has declined slightly to $4.44 million, down 9% from $4.88 million in 2024 (*Cost of a Data Breach Report 2025*), marking the first drop in five years. However, this figure varies significantly by region and sector; in the United States, recovery costs exceed $10 million per breach (Kapko, 2025), whilst breaches involving multiple environments average $5.05 million globally (*Cost of a Data Breach Report 2025*). These costs encompass not only direct expenses such as forensics and notification, but also indirect impacts like lost business and regulatory fines.

Organizations require dedicated cybersecurity services to mitigate these risks effectively. These services, provided internally by security departments, encompass a range of activities from threat monitoring to incident response, ensuring proactive defence rather than reactive measures. The necessity stems from the recognition that traditional IT security, focused primarily on perimeter defences like firewalls, is insufficient against modern, polymorphic threats. Instead, a holistic approach is essential, integrating people, processes and technology to foster resilience. The relationship between threats, risks and cybersecurity services is presented in Figure 1.

Figure 1. Rationale for cybersecurity services



Source: created by the author.

Knowledge Gap and Research Objectives

Despite growing recognition of cybersecurity's importance, significant gaps persist in how cybersecurity services are conceptualized and operationalized within organizations. The current literature exhibits three primary deficiencies:

Firstly, the field is plagued by terminological inconsistencies. Recent scholarship highlights persistent divergences between 'information security' and variants of 'cyber security'/'cybersecurity', with semantic, etymological and practical implications that

affect research, policy and operational clarity (Henrico, Putter, 2025: 2–8; Jean, Myriam, 2025). A systematic review examining 922 articles from 2018 to 2023 reports 'cybersecurity' as the dominant form with 30,160 mentions compared to 14,798 for 'cyber security', yet this fragmentation complicates academic indexing and machine learning applications (Henrico, Putter, 2025: 15).

Secondly, existing definitions of cybersecurity services predominantly address external threat mitigation or managed service provider offerings, neglecting internal organizational dynamics. Few studies examine how internal security departments deliver value to other business units through structured service offerings (Werlinger et al., 2009: 6). This oversight is particularly problematic given that internal cybersecurity functions must balance technical capabilities with managerial integration to enable organizational objectives.

Thirdly, whilst risk and control frameworks such as ISO 27001 and NIST CSF are well established, the literature lacks explicit mapping between these frameworks and cybersecurity service delivery. Studies address either framework implementation or service taxonomy, but rarely integrate both perspectives to demonstrate how services operationalize framework requirements (Culot et al., 2021: 84–85).

This paper addresses these gaps through three primary objectives:

1. To synthesize the extant literature on cybersecurity services, tracing their evolution and identifying key definitions and frameworks.
2. To propose a unified definition of cybersecurity services focused on internal organizational provisions that safeguard assets through advisory, preventive, detective and responsive activities.
3. To examine relationships between these services and risk/control frameworks, elucidating how they integrate to enhance overall security posture.

Research Questions

Guiding this inquiry are the following research questions:

- What constitutes cybersecurity services in an organizational context, particularly those offered by internal security departments?
- How do these services integrate with risk management frameworks to enhance security and mitigate threats?

These questions facilitate a structured exploration, enabling the study to address gaps in current knowledge regarding intra-organizational service delivery.

Scope and Contribution

The scope of this study is confined to internal cybersecurity services, excluding external vendors or managed security service providers (MSSPs). This focus allows for in-depth analysis of how security departments function as internal service hubs, delivering value to other organizational units. The investigation is limited to enterprise

settings, encompassing large organizations with complex structures and significant digital footprints.

The paper makes three principal contributions. Firstly, it synthesizes the fragmented literature on cybersecurity services to propose a unified, service-oriented definition grounded in management science theory. Secondly, it develops a four-domain service taxonomy that bridges technical and managerial perspectives. Finally, it develops a structured mapping between cybersecurity services and established R&C frameworks (ISO 27001 Annex A and NIST CSF 2.0), demonstrating how services operationalize framework requirements in practice.

Literature Review and Conceptual Development

Review Approach

This study employs a structured literature synthesis to examine how cybersecurity services are conceptualized, classified and related to organizational risk management. Literature was identified through structured searches in Scopus and Google Scholar using combinations of terms relating to *cybersecurity services*, *cybersecurity as a service*, *information security services*, *cybersecurity capabilities*, *cybersecurity management*, *risk management*, *security controls*, *ISO/IEC 27001* and the *NIST Cybersecurity Framework*. Searches were refined to account for terminology variations across the multidisciplinary literature. Relevant academic publications, standards, framework documents and authoritative institutional sources were considered where they addressed the conceptualization, organizational delivery, governance or control of cybersecurity services. The selected literature was thematically analyzed according to service definitions, organizational purpose, delivery characteristics, risk relationships and framework alignment. Recurring concepts were consolidated into the four service domains proposed in this study: governance, core operations, engineering and assurance, and cross-cutting and business services. A subsequent conceptual mapping examined their relationship with NIST CSF 2.0 functions and the four ISO/IEC 27001:2022 control groups. The final synthesis comprised of around 50 sources.

The overall analytical process comprised, therefore, the following steps: structured search → source selection → thematic extraction → service coding → four-domain taxonomy → framework mapping → conceptual propositions → proposed empirical validation.

Evolution of Cybersecurity Services

The field of cybersecurity services has undergone significant evolution, shaped by technological advancements, escalating threats and shifting definitional paradigms.

Central to this discourse are persistent inconsistencies in terminology, particularly between 'information security' and variants of 'cyber security'/'cybersecurity'.

A 2025 conference paper explores the evolution of 'cyber()security' through historical and semantic analysis, revealing a pre-2003 preference for 'cyber security' associated with information security and infrastructure protection (Jean, Myriam, 2025). Post-2003, amid rising cyberattacks, usage shifted towards the compound 'cybersecurity'. The paper distinguishes 'cybersecurity' as broader, extending to all entities in cyberspace beyond traditional 'information security'. A further contribution directly contrasts the terms, defining information security as safeguarding data in any form (emphasizing confidentiality, integrity and availability) against cybersecurity's narrower focus on digital systems, networks and online threats (Raxmonberdiyeva, 2025: 234–235).

The evolution of cybersecurity services can be traced through four distinct phases:

1. Early IT Security (1960s–1980s): The origins can be trace back to mainframe computing, with milestones like the development of MULTICS (1965), which introduced access controls and passwords to protect shared systems (Karger, Schell, 2002: 119, 121). Early definitions focused on 'computer security' as preventing unauthorized access. The 1980s saw the rise of personal computers and networks leading to the first viruses, with services evolving to include antivirus software and firewalls (Bhargava et al., 2022: 39; Valcesia, Rigo, 2019: 3).
2. Network-Centric Security (1990s–2000s): The internet's commercialization spurred milestones such as the first DDoS attacks and the establishment of CERT. Services expanded to network security, with definitions incorporating 'cyber security' (coined in 1989) to address online threats beyond traditional IT (Dawkins, 2025). Post-9/11, cybersecurity became critical infrastructure-focused, with frameworks like NIST SP 800-53 emerging. Definitions broadened to 'cybersecurity services' as managed offerings integrating compliance and risk management (Liu et al., 2025: 1, 2, 5).
3. Holistic Integration (2010s): Cloud computing and IoT proliferation drove milestones such as the NIST Cybersecurity Framework (2014). Services evolved to include threat hunting and zero-trust models, with definitions emphasizing holistic strategies: people (training), processes (incident response) and technology (AI-driven analytics) to achieve resilience (*The NIST Cybersecurity Framework 2.0*, 2024: 4–6).
4. Adaptive Ecosystem Approaches (2020s–Present): The COVID-19 pandemic accelerated remote work threats, leading to widespread adoption of AI/ML for predictive security and quantum-resistant cryptography (Egbuagha, Ikwunna, 2025: 2). Modern definitions view cybersecurity services as ecosystem-wide, including supply chain security and cyber-physical integration, for adaptive, proactive defence.

Cybersecurity Services Definitions

The literature offers multiple perspectives on cybersecurity services, each emphasizing different dimensions:

Socio-technical perspective: Craigen, Diakun-Thibault and Purse (2014: 17) define cybersecurity services as the organization and collection of resources, processes and structures that coordinate people, technology and policy to reduce harm from cyberspace, emphasizing that cybersecurity is inherently multidisciplinary and must integrate governance, human factors and technical controls.

Risk-management perspective: A comprehensive review frames cyber security services as capabilities and practices that identify, assess and mitigate vulnerabilities and threats across systems, covering prevention (secure design, access controls), detection (monitoring, analytics) and response (forensics, recovery), with explicit focus on vulnerability detection methodologies and continuous improvement (Bennouk et al., 2024: 853–866).

Service delivery perspective: Academic treatments of Cybersecurity as a Service describe cyber security services as managed offerings delivered by third-party providers that provide continuous monitoring, threat detection, incident response and security orchestration on behalf of clients, thereby addressing skills shortages and enabling 24/7 resilience (Morris et al., 2024: 141).

Systemic resilience perspective: Comprehensive treatments describe cyber security services as activities that manage and mitigate systemic risk across socio-technical systems, aiming to preserve confidentiality, integrity and availability whilst enabling safe use of digital infrastructure (Cornish, 2021: 15–18). Services therefore span prevention, detection, response, recovery and continuous improvement to maintain operational resilience.

Service Categories in Literature

The literature consistently identifies ranges of services that organizations provide. These services are often categorized into governance, preventive, detective, responsive and advisory domains, emphasizing socio-technical integration. Analysis of recent literature reveals common service themes:

Governance services: Papers emphasize risk-based governance, mapping controls to business objectives and regulatory requirements, and integrating risk assessment into decision cycles (Pinninti, 2025: 77–80; Aghazadeh Ardebili et al., 2024: 11807).

Preventive controls: Research on network segmentation, endpoint detection, secure SDLC (Software Development Lifecycle) and cryptographic best practices shows that defence-in-depth and secure engineering reduce attack surface and limit lateral movement (Mhaskar et al., 2021: 1–30; Masukawa et al., 2025: 136806–136815).

Identity and access management: Studies highlight IAM (Identity and Access Management) as foundational, with provisioning, SSO (Single Sign On), MFA (Multifactor Authentication) and privileged access management reducing credential misuse and insider risk (Glöckler et al., 2024: 425–433; Feng et al., 2025).

Detection and monitoring: Literature on SOCs (Security Operations Centre), SIEM (Security Information and Event Management) and MDR (Managed Detection and Response) stresses continuous telemetry, analytics and human-machine workflows (Vielberth et al., 2020: 227756–227775; Chamkar et al., 2024: 777–780).

Vulnerability management: Approaches focus on context-aware prioritization and patch orchestration (Ahmedi Mehri et al., 2022: 3580; Alqahtani, Almukaynizi, 2026: 1–12).

Incident response: Papers document playbook design, containment strategies and the role of ML in triage (Salfati, Pease, 2022: 10–15; Binnar et al., 2024: 1–12).

Threat intelligence: Research shows that IZACs (Information Sharing and Analysis Centres) and structured sharing improve situational awareness, but governance, trust and standardization are critical (Dykstra et al., 2023: 1–12; Wagner et al., 2020: 1–27).

Training and culture: Empirical studies of phishing simulations demonstrate measurable behaviour change when programmes are continuous and contextualized (Ho et al., 2025: 37–54; Alluqmani et al., 2025: 177–184).

Assurance activities: Penetration testing, red teaming and architecture reviews are validated as essential for continuous improvement (Teichmann, Boticiu, 2023: 387–397; Radanliev, 2025: 1–18).

Gaps in Service Definition Literature

A critical gap exists in the literature addressing services specifically from security departments to internal stakeholders. Few studies focus on intra-organizational dynamics where cybersecurity functions deliver value to business units. The ITIL framework defines service as 'a means of enabling value co-creation by facilitating outcomes that customers want to achieve, without the customer having to manage specific costs and risks' (Axelos, 2019: 12). From this perspective, cybersecurity departments should provide defined services that produce outcomes for service customers. Even if customers are other departments in the same organization.

Existing classifications address strategies, decision support systems or threat taxonomies, but few explicitly catalogue services with customer-facing value propositions. For instance, Oliveira et al. (2023: 1–18) classify cybersecurity strategies based on goals and attack types, whilst François, Arduin and Merad (2023: 8–10) analyze decision support systems for cybersecurity without defining underlying services. These approaches address technical classifications rather than service delivery models that answer the question: what value does cybersecurity provide to internal customers?

This gap matters because services must describe what users want to do, include desired outcomes, encompass all steps between users and providers, and include everything involved in delivering them (Tarling, 2023: 21). Without explicit service definitions oriented towards internal value creation, organizations struggle to position cybersecurity as an enabling function rather than a cost centre.

Defining Cybersecurity Services

Proposed Definition

Based on synthesis of the ITIL definition of services and cybersecurity literature, this paper proposes the following definition:

Cybersecurity services are business-facing, outcome-oriented offerings orchestrated by the cybersecurity department to safeguard organizational assets in cyberspace. They enable value protection and co-creation by facilitating secure business outcomes that internal teams seek to achieve, whilst managing specialized costs, complexity and risks on their behalf (through systematic risk evaluation, resource deployment and performance monitoring), allowing teams to pursue their objectives with confidence.

This definition advances existing conceptualizations in three ways. Firstly, it explicitly positions cybersecurity as a service function rather than merely a technical capability, aligning with service management theory (Vargo, Lusch, 2004: 1–5). Secondly, it emphasizes outcome orientation and value co-creation with internal customers, addressing the gap in literature that overlooks intra-organizational service dynamics. Thirdly, it acknowledges the dual role of cybersecurity in both protecting existing value and enabling new value creation, recognizing that security should facilitate rather than impede business objectives.

Four-Domain Service Taxonomy

To operationalize this definition, a four-domain service taxonomy is proposed:

Governance Services establish strategic direction and ensure compliance:

- Risk assessment and management
- Policy and standards management
- Compliance and audit support
- Third-party and supply chain risk management
- Security strategy and advisory

Core Operations Services provide continuous protection and response:

- SOC monitoring
- Incident response and recovery
- Vulnerability management

- Identity and access management
- Threat intelligence and threat hunting
- Endpoint detection and response operations

Engineering and Assurance Services embed security in systems and validate controls:

- Application security (AppSec)
- Cloud security and DevSecOps
- Network and perimeter security
- Cryptography and key management
- Adversarial security testing
- Secure architecture and design reviews
- Security engineering and automation

Cross-cutting and Business Services support organizational capabilities:

- Security awareness and training
- Data protection and privacy services
- Business continuity and resilience
- Security advisory and Virtual CISO
- Security reporting and metrics

This taxonomy advances literature by categorizing services according to their organizational function rather than technical implementation, making them more accessible to business stakeholders. Each service addresses specific customer needs and delivers measurable outcomes, transforming cybersecurity from a technical silo into an integrated business function.

Service-Oriented Naming Convention

To enhance accessibility and adoption, service-oriented naming conventions are recommended. Traditional technical labels (e.g. 'IAM', 'EDR', 'SIEM') are meaningful to security professionals but opaque to business users. Service-oriented names describe the task or outcome rather than the technology (Downe, 2022: 52–55).

For example, 'Identity and Access Management Services' becomes 'Manage user access and privileges', whilst 'Security Operations Centre Monitoring' becomes '24/7 threat monitoring and alerting'. This approach offers several advantages:

1. Improved discoverability: Plain-language names enable users to locate services by intent rather than jargon, reducing search friction.
2. Aligned expectations: Task-focused names describe deliverables rather than technical implementation, reframing conversations from technology to outcomes.
3. Reduced ambiguity: Avoiding acronyms prevents divergent interpretations across teams, decreasing hand-off errors.
4. Appropriate ownership: When service names specify problems addressed, assigning accountability becomes clearer.
5. Enhanced adoption: Action-oriented names increase uptake and adherence to required processes.

A practical challenge arises when cybersecurity teams prefer traditional nomenclature. Consequently, catalogue entries should support dual-label searchability (both legacy technical identifiers and service-oriented names) on a transitional basis, facilitating discoverability for diverse stakeholder groups. A list of "user-friendly" service names is presented in Annex 1.

Organizational Value Proposition

Cybersecurity services solve the organization's problem of operating safely in a hostile digital environment. Their core value proposition encompasses:

Enabling safe value creation: Services allow organizations to operate digitally with confidence – launching new products, expanding online, adopting cloud or AI – without security concerns halting progress or exposing the business to unacceptable risk.

Protecting existing value: Services safeguard critical assets (data, intellectual property, revenue streams, reputation) from theft, disruption or destruction, preventing financial losses, regulatory fines and loss of customer trust.

Transferring cost, complexity and risk: Business units avoid acquiring deep security expertise, investing in specialized tools, maintaining 24/7 vigilance or bearing full consequences of incidents. The cybersecurity department absorbs these on their behalf, delivering security as a reliable, shared utility.

Value can be measured across dimensions: financial protection (reduced breach costs), operational resilience (faster recovery), compliance and trust (regulatory adherence), strategic enablement (accelerated innovation) and risk reduction (lower overall cyber risk exposure). In essence, cybersecurity services transform security from a cost centre into a business enabler, delivering peace of mind, resilience and competitive advantage.

Relationship with Risk and Control Frameworks

Risk and Control Framework Overview

A risk and control framework provides a structured approach through which organizations identify key risks, design controls to mitigate them and monitor control effectiveness (Spira, Page, 2003: 23). Two widely recognized frameworks are NIST CSF 2.0 and ISO 27001.

NIST CSF 2.0 organizes cybersecurity into six continuous functions designed to be iterative and integrated (*The NIST Cybersecurity Framework 2.0*, 2024: 4–6):

- Govern: Establish and oversee cybersecurity strategy, risk management, roles and compliance.
- Identify: Understand assets, risks, vulnerabilities and organizational context.
- Protect: Implement safeguards such as access control, secure configuration and training.
- Detect: Identify anomalies, events and potential cybersecurity incidents.

- Respond: Contain, mitigate and communicate about incidents.
- Recover: Restore services and capabilities after incidents whilst incorporating lessons learnt.

The framework stresses that these functions are not linear but ongoing and interconnected, enabling adaptive risk management in dynamic environments.

ISO 27001 defines requirements for an Information Security Management System (ISMS). It requires organizations to perform ongoing risk assessments, select risk-based controls from its Annex A, monitor control effectiveness and continually improve the ISMS (*ISO/IEC 27001:2022*: 4–6). With ISO 27001, risk identification and mitigation are meant to be continuous, not one-off activities.

Layered Ecosystem Model

Cybersecurity services and risk/control frameworks are two sides of the same governance coin: the framework defines how risks are identified, prioritized and controlled (policies, procedures, technical controls), whilst cybersecurity services deliver the people, processes and technologies that implement, monitor and adapt those controls. Services operationalize the framework by translating risk decisions into detection, prevention, response and assurance activities.

In ISO/IEC 27001:2022, the relationship between security services, policies, procedures and technical controls forms an integrated structure supporting ISMS operation. Policies provide strategic direction and define security objectives and risk appetite, whilst security services operationalize these objectives by delivering capabilities required to manage and mitigate risk. Procedures translate policy requirements into consistent, repeatable actions that enable services to function effectively (*ISO/IEC 27001:2022*: Clause 7.5). Technical controls, selected through risk treatment (Clause 6.1.3), implement safeguards necessary to address identified risks. Annex A contains 93 controls grouped into four themes (Organizational, People, Physical and Technological) which services integrate into operational activities. The literature highlights that organizations must interpret and adapt these controls to their context, as implementation challenges vary with technological maturity (Culot et al., 2021: 84–85).

The layered ecosystem comprises:

Policies sit at the highest level, providing strategic direction ('what' must be achieved and 'why'). They define security objectives, risk appetite and governance principles. Example: 'Information Security Policy' establishes organizational commitment to protecting assets.

Standards specify mandatory requirements and benchmarks ('what' must be met). They translate policy intent into measurable criteria. Example: 'Encryption Standard' mandates AES-256 for data at rest.

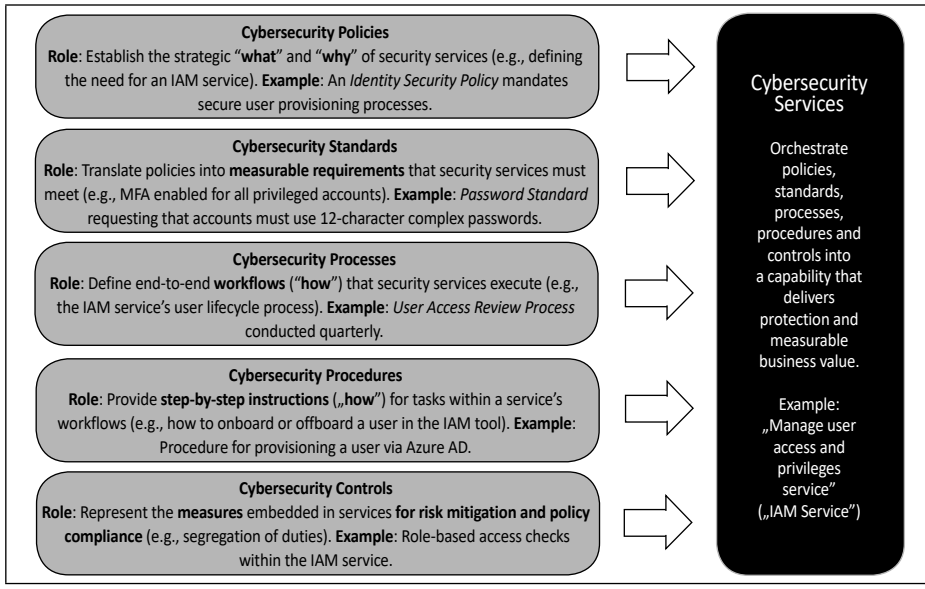
Procedures document step-by-step instructions for implementing standards ('how' to execute tasks). They ensure consistency and repeatability. Example: 'Incident Response Procedure' details escalation paths and containment steps.

Controls are technical, physical or administrative safeguards that implement procedures and enforce standards. ISO 27001 Annex A and NIST CSF provide control catalogues. Example: Multi-factor authentication (MFA) as a technical control implementing access management procedures.

Cybersecurity services operate across all layers, interpreting policies, executing procedures, implementing controls and measuring outcomes. Services transform governance artefacts into real-world protection and measurable business value.

This layered relationship is illustrated in Figure 2, which traces how each governance artefact (i.e. policies, standards, processes and procedures) is interpreted and executed by a cybersecurity service.

Figure 2. Risk & control framework artefacts and their relationship with cybersecurity services



Source: created by the author based on NQA ISO 27001:2022; Lineman, 2023; *Policy vs standard*... (n.d.).

Service Integration with Frameworks

Cybersecurity services map directly to framework functions and controls. For NIST CSF 2.0:

- Govern function is delivered through governance services (risk assessment, policy management, strategy and advisory).
- Identify function is supported by asset inventory, vulnerability management and threat intelligence services.
- Protect function is implemented through IAM, network security, application security and training services.

- Detect function is delivered by SOC monitoring, EDR and threat hunting services.
- Respond function is executed through incident response and forensics services.
- Recover function is supported by business continuity, backup/restore and lessons-learnt services.

For ISO 27001 Annex A, services implement specific control categories:

- Organizational controls (e.g. A.5 Information Security Policies) are delivered through policy management and compliance services.
- People controls (e.g. A.6 Security Awareness) are delivered through training and awareness services.
- Physical controls (e.g. A.7 Physical Security) intersect with facility security and asset management.
- Technological controls (e.g. A.8 Access Control, A.12 Network Security) are delivered through IAM, network security and cryptography services.

The mapping in table 1 illustrates how selected individual cybersecurity services translate framework requirements into operational activities. The relationship is not one-to-one: a single service may support multiple framework functions or control areas, while individual controls may depend on several services. The mapping therefore represents the principal operational contribution of each service rather than a direct equivalence between a service and a specific control.

Table 1. Illustrative mapping of cybersecurity services to NIST CSF 2.0 and ISO/IEC 27001:2022

Cybersecurity service (service-oriented name)	NIST CSF 2.0	ISO/IEC 27001:2022 control group(s)	Principal contribution
Manage user access and privileges	Protect	Technological; Organizational; People	Controls identities, authentication, access rights and privileges.
24/7 threat monitoring and alerting	Detect	Technological; Organizational	Continuously monitors activity and identifies suspicious events.
Respond to and recover from security incidents	Respond / Recover	Organizational; Technological; People	Coordinates containment, investigation, communication and recovery.
Find and fix security weaknesses	Identify / Protect	Technological; Organizational	Identifies, prioritizes and tracks remediation of vulnerabilities.
Security awareness and training	Protect	People; Organizational	Develops security awareness, competence and secure behaviour.
Assess and manage supplier security	Govern / Identify	Organizational; People	Assesses and manages security risks arising from suppliers and partners.
Secure application design and testing	Protect	Technological; Organizational	Embeds security into application design, development and testing.

Source: Author's synthesis based on the cybersecurity service taxonomy developed in this study, NIST Cybersecurity Framework 2.0 (NIST, 2024) and ISO/IEC 27001:2022.

This integration demonstrates how services operationalize framework requirements. Rather than treating frameworks as compliance checklists, organizations can map services to controls, ensuring that each service delivers specific risk mitigation outcomes aligned with framework guidance.

Discussion

Theoretical Implications

The theoretical implications of this paper lie in its contribution to conceptualizing cybersecurity services as managerial constructs that bridge technical defences with organizational strategy. The definition of cybersecurity services as business-facing, outcome-oriented offerings shifts emphasis from external threat-centric models to intra-organizational processes, addressing a noted gap where cybersecurity is often treated as a peripheral IT function rather than a core managerial activity (Wilson et al., 2020).

Management science, with roots in optimization and decision-making, provides a lens to view these services as mechanisms for resource allocation and performance enhancement. From a resource-based view (RBV), cybersecurity services represent unique capabilities that enhance competitive advantage. Services like threat intelligence and incident response protect intellectual property and operational continuity, transforming security from a cost to a value driver (Werlinger et al., 2009: 5–6).

Contingency theory posits that effective cybersecurity services must adapt to organizational context, including size, industry and risk profile. This implies a dynamic approach where services are tailored rather than standardized to mitigate risks in varying environments (Siponen, Willison, 2009: 267). Emphasis on internal adaptability extends contingency applications to specific service delivery, filling a theoretical void in how organizations configure security amid uncertainty.

Systems theory enriches this advancement, framing cybersecurity services as interconnected subsystems within the larger organizational ecosystem (Yan, 2020: 2–5). Services do not operate in isolation but interact with other functions to maintain system stability. The paper's focus on internal dynamics reveals how services contribute to organizational resilience through feedback loops (for example, performance monitoring informing policy updates) thus promoting a holistic view over fragmented technical silos.

Contemporary research highlights persistent gaps, such as underemphasis on cultural integration and human-centric risks (Rahman et al., 2021: 1–5; Kour et al., 2024: 5, 8, 10), where services like awareness training are pivotal yet underexplored in internal contexts. This paper's proposed definition and structure fill these voids by positioning services as managerial tools that optimize internal resources and processes, advancing the field towards more integrated, organization-centric models.

Practical Implications

The practical implications highlight advantages of framing cybersecurity as a service (CaaS), where the cybersecurity department delivers tailored, outcome-oriented provisions to internal customers. Organizations can transform security from a siloed cost centre into a strategic enabler, allowing business units to achieve objectives without directly managing complex threats or compliance burdens.

For example, services like vulnerability management or incident response, when offered via a centralized catalogue, reduce operational friction and enhance resilience, as evidenced by lowered breach costs and faster recovery times. Alignment of CaaS with frameworks like NIST CSF 2.0 ensures services integrate seamlessly into workflows, with functions like Protect and Detect enabling proactive scanning and monitoring without disrupting core activities.

Leaders should implement clear ownership models (e.g. centralized for SOC monitoring, embedded for AppSec in development teams) and KPIs to measure value, such as reduced downtime or improved compliance rates. This approach creates tangible benefits, including cost efficiencies through shared resources, heightened trust amongst stakeholders and a competitive edge in threat-laden environments, positioning security as a collaborative service that drives organizational success.

Limitations

Several limitations constrain this study's scope and generalizability. Firstly, as a conceptual paper based on literature synthesis rather than empirical data collection, its findings may not fully capture practical implementation challenges across diverse organizational contexts. Secondly, the rapid evolution of cyber threats means that specific service taxonomies may require periodic updates to remain relevant. Thirdly, the focus on internal cybersecurity services excludes external vendors and MSSPs, limiting applicability to organizations that heavily outsource security functions. Finally, the study's emphasis on enterprise settings with formal risk frameworks may not translate directly to SMEs with different resource constraints and security needs.

Conclusions and Future Research

Summary of Contributions

This paper has examined the definition of cybersecurity services and their relationship to risk and control frameworks, drawing on a structured literature synthesis to propose a clear understanding tailored to internal organizational dynamics. The study defines cybersecurity services as business-facing, outcome-oriented offerings

orchestrated by the cybersecurity department to safeguard organizational assets in cyberspace, enabling value co-creation by facilitating secure business outcomes whilst managing specialized costs, complexity and risks on behalf of internal teams.

Key contributions include: (1) synthesis of fragmented literature to address terminological inconsistencies and trace evolutionary milestones from reactive data protection to proactive, holistic approaches; (2) a four-domain service taxonomy categorizing offerings into governance, core operations, engineering and cross-cutting services, each with clear ownership and value propositions; (3) demonstration of how services operate within layered risk-mitigation ecosystems, where policies direct services, procedures implement them and technical controls execute safeguards, as exemplified in ISO 27001 Annex A (93 controls across four themes) and NIST.

The theoretical implications extend management science by addressing gaps in internal dynamics, particularly underemphasis on cultural integration and human-centric risks. The practical implications recommend organizations adopt this service model to transform security into a value enabler, aligning with NIST for enhanced risk control and fostering resilience.

Future Research Directions

Future research should empirically evaluate the effectiveness of cybersecurity services across diverse organizational contexts. Longitudinal studies could examine how services such as incident response and threat hunting influence recovery times and cost savings, applying quantitative methods in sectors including finance and healthcare. Randomized controlled trials comparing integrated and siloed service models would help quantify value co-creation and resilience gains.

Further work is needed on AI's role in service automation (for example, AI-driven anomaly detection or predictive risk assessment) and on how machine learning can enhance human-centric services such as awareness training in the face of evolving threats. Qualitative case studies could explore cultural and organizational barriers to adoption, while cross-cultural comparisons might highlight regional differences in implementation and inform the development of global standards.

Future research could usefully be organized around three validation questions:

1. Construct validity
   Does the four-domain taxonomy accurately represent the cybersecurity services organizations actually provide? Possible designs include surveys of CISOs and security managers, Delphi studies, expert panels and factor analysis of service categories.

2. Applicability
   Can organizations use the taxonomy to structure cybersecurity service catalogues? Possible designs include multiple organizational case studies, implementation studies, interviews with cybersecurity and business stakeholders, and before-and-after evaluations of catalogue adoption.
3. Effectiveness
   Does organizing cybersecurity as services improve organizational outcomes? Possible designs in such research could include longitudinal studies, quasi-experimental comparisons of organizations or business units, and contrasts between service-oriented and siloed models.

Concluding Remarks

There is a strong imperative for integrated approaches in today's volatile digital environment, where isolated security efforts falter against sophisticated threats. Organizations must prioritize these services not only to defend against disruptions but also to drive competitive advantage through secure operations. A call to action urges leaders to implement centralized catalogues, measure value via KPIs and invest in cross-functional collaboration, ensuring cybersecurity evolves from a reactive necessity to a proactive strategic asset that underpins sustainable growth.

References

Aghazadeh Ardebili, A., Lezzi, M., Pourmadadkar, M. (2024). Risk assessment for cyber resilience of critical infrastructures: methods, governance, and standards. *Applied Sciences*, *14*(24), 11807, https://doi.org/10.3390/app142411807

Ahmedi Mehri, V., Arlos, P., Casalicchio, E. (2022). Automated context-aware vulnerability risk management for patch prioritization. *Electronics*, *11*(21), 3580, https://doi.org/10.3390/electronics11213580

Alluqmani, K., Karrar, A.E., Alhaidari, M., Alharbi, R., Alharbi, S. (2025). Assessing the efficacy of security awareness training in mitigating phishing attacks: a review. *International Journal of Advanced Trends in Computer Science and Engineering*, *14*(3), 177–184, https://doi.org/10.30534/ijatcse/2025/141432025

Alqahtani, N., Almukaynizi, M. (2026). VulnScore: a deployed system for patch prioritization combining human input and temporal threat intelligence. *International Journal of Information Security*, 25, art. 2, https://doi.org/10.1007/s10207-025-01164-3

Axelos (2019). *ITIL Foundation: ITIL 4 Edition*. TSO (The Stationery Office).

Bennouk, K., Ait Aali, N., El Bouzekri El Idrissi, Y., Sebai, B., Faroukhi, A.Z., Mahouachi, D. (2024). A comprehensive review and assessment of cybersecurity vulnerability detection methodologies. *Journal of Cybersecurity and Privacy*, *4*(4), 853–908. https://doi.org/10.3390/jcp4040040

Bhargava, P., Choudhary, R., Gupta, A. (2022). A review study on computer virus. *World Journal of Research and Review*, *14*(5), 39–44.

Binnar, P., Bhirud, S., Kazi, F. (2024). Security analysis of cyber physical system using digital forensic incident response. *Cyber Security and Applications*, 2, art. 100034. https://doi.org/10.1016/j.csa.2023.100034

Chamkar, S.A., Maleh, Y., Gherabi, N. (2024). Security operations centers: use case best practices, coverage, and gap analysis based on MITRE adversarial tactics, techniques, and common knowledge. *Journal of Cybersecurity and Privacy*, *4*(4), 777–793. https://doi.org/10.3390/jcp4040036

Cornish, P. (Ed.) (2021). *The Oxford Handbook of Cyber Security*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198800682.001.0001

Cost of a Data Breach Report 2025. IBM. https://www.ibm.com/reports/data-breach [accessed: 18.01.2026].

Craigen, D., Diakun-Thibault, N., Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21. https://doi.org/10.22215/timreview/835

Culot, G., Nassimbeni, G., Podrecca, M., Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *The TQM Journal*, *33*(7), 76–105. https://doi.org/10.1108/TQM-09-2020-0202

Cyberthreat Defense Report 2024. CyberEdge Group. https://cyberedgegroup.com/wp-content/uploads/2024/05/CyberEdge-2024-CDR-Report-v1.0.pdf [accessed: 18.01.2026].

Dawkins, J. (2025). *What's in a Name? The Origin of Cyber*. The CISO Inc. https://www.ciso.inc/blog-posts/origin-cyber/ [accessed: 18.01.2026].

Downe, L. (2022). *Good Services: How to Design Services That Work*. BIS Publishers.

Dykstra, J., Gordon, L.A., Loeb, M.P., Zhou, L. (2023). Maximizing the benefits from sharing cyber threat intelligence by government agencies and departments. *Journal of Cybersecurity*, *9*(1), tyad003. https://doi.org/10.1093/cybsec/tyad003

Egbuagha, O., Ikwunna, E. (2025). Post-quantum cryptography in practice: a literature review of protocol-level transitions and readiness. *Cryptology ePrint Archive*, 048. https://eprint.iacr.org/2025/048 [accessed: 18.01.2026].

Feng, Z., Li, Z., Cui, H., Whitty, M.T. (2025). Identity management systems: a comprehensive review. *Information*, *16*(9), 778. https://doi.org/10.3390/info16090778

François, M., Arduin, P.E., Merad, M. (2023). Classification of decision support systems for cybersecurity. In *15th Mediterranean Conference on Information Systems (MCIS) and the 6th Middle East & North Africa Conference on Digital Information Systems (MENACIS)*. https://aisel.aisnet.org/mcis2023/12

Global Cybersecurity Outlook 2025. Insight report (2025). World Economic Forum. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf [accessed: 18.01.2026].

Glöckler, J., Sedlmeir, J., Frank, M., Fridgen, G. (2024). A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity. *Business & Information Systems Engineering*, *66*(4), 421–440. https://doi.org/10.1007/s12599-023-00830-x

Henrico, S., Putter, D. (2025). Cyber what??? – a systematic review. *Journal of Applied Security Research*, *21*(1), 1–34. https://doi.org/10.1080/19361610.2025.2544184

Ho, G., Mirian, A., Luo, E., Tong, K., Lee, E., Liu, L. Voelker, G.M. (2025). Understanding the efficacy of phishing training in practice. In *Proceedings of the IEEE Symposium on Security and Privacy* (pp. 37–54). https://doi.org/10.1109/SP61157.2025.00076

ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements. (2022). International Organization for Standardization.

Jean, B., Myriam, M. (2025). Decoding cybersecurity: how terminology shapes the field. In *ESREL SRA-E 2025*. Research Publishing. https://doi.org/10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P5323-cd

Kapko, M. (2025). *Research shows data breach costs have reached an all-time high*. CyberScoop, 30.07. https://cyberscoop.com/ibm-cost-data-breach-2025/ [accessed: 18.01.2026].

Karger, P.A., Schell, R.R. (2002). Thirty years later: lessons from the Multics security evaluation. In *18th Annual Computer Security Applications Conference, 2002. Proceedings* (pp. 119–126). IEEE. https://doi.org/10.1109/CSAC.2002.1176291

Kour, R., Karim, R., Dersin, P., Venkatesh, N. (2024). Cybersecurity for Industry 5.0: trends and gaps. *Frontiers in Computer Science*, 6, 1434436. https://doi.org/10.3389/fcomp.2024.1434436

Lineman, D. (2023). *Security policies, standard and procedures: what's the difference?* Information Shield, 27.10. https://informationshield.com/2023/10/27/security-policies-standard-and-procedures-whats-the-difference/ [accessed: 18.01.2026].

Liu, M., Shore, M., Yeoh, W., Jiang, F., Zeadally, S. (2025). Toward effective cybersecurity management: a hierarchical process model with performance assessment. *Journal of Cybersecurity*, *11*(1), tyaf020. https://doi.org/10.1093/cybsec/tyaf020

Masukawa, R., Yun, S., Jeong, S., Bastian, N.D., Imani, M. (2025). TriageHD: A HyperDimensional LearningtoRank Framework for Dynamic MicroSegmentation in ZeroTrust Network Security. *IEEE Access*, 13, 136806–136815. https://doi.org/10.1109/ACCESS.2025.3592877

Mhaskar, N., Alabbad, M., Khedri, R. (2021). A formal approach to network segmentation. *Computers & Security*, 103, 102162. https://doi.org/10.1016/j.cose.2020.102162

Morris, J., Tatschner, S., Heinl, M.P., Heinl, P., Newe, T., Plaga, S. (2024). Cybersecurity as a service. In K. Naseer Qureshi, T. Newe, G. Jeon, A. Chehri (Eds.), *Cybersecurity Vigilance and Security Engineering of Internet of Everything* (pp. 130–145). Springer (Internet of Things). https://doi.org/10.1007/978-3-031-45162-1_9

The NIST Cybersecurity Framework 2.0. (2024). National Institute of Standards and Technology, 26.02. https://doi.org/10.6028/NIST.CSWP.29

ISO 27001:2022. Information Security Implementation Guide. NQA. https://www.nqa.com/getmedia/ae12c945-4dbb-4b73-a4e3-996261a540af/NQA-ISO-27001-Implementation-Guide.pdf [accessed: 18.01.2026].

Oliveira, S., Leal, A.B., Teixeira, M., Lopes, Y.K. (2023). A classification of cybersecurity strategies in the context of discrete event systems. *Annual Reviews in Control*, 56, 100907. https://doi.org/10.1016/j.arcontrol.2023.100907

Pinninti, V.P. (2025). Automating governance, risk, and compliance (GRC) in cloud computing: a case study on ServiceNow and NIST framework integration. *Internet of Things and Cloud Computing*, *13*(4), 77–86. https://doi.org/10.11648/j.iotcc.20251304.11

Policy vs standard vs control vs procedure. (n.d.). Compliance Forge. https://complianceforge.com/grc/policy-vs-standard-vs-control-vs-procedure [accessed: 18.01.2026].

Radanliev, P. (2025). Red teaming quantum-resistant cryptographic standards: a penetration testing framework integrating AI and quantum security. *Journal of Defense Modeling and Simulation*, 1–18. https://doi.org/10.1177/15485129251364901

Rahman, T., Rohan, R., Pal, D., Kanthamanon, P. (2021). Human factors in cybersecurity: a scoping review. In *Proceedings of the 12th International Conference on Advances in Information Technology* (pp. 1–11). https://doi.org/10.1145/3468784.3468789

Raxmonberdiyeva, S. (2025). Differences between information security and cybersecurity. *Modern Science and Research*, *4*(6), 234–237. https://inlibrary.uz/index.php/science-research/article/view/104279

Salfati, E., Pease, M. (2022). *Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT)*. NIST IR 8428. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8428

Siponen, M., Willison, R. (2009). Information security management standards: problems and solutions. *Information & Management*, *46*(5), 267–270. https://doi.org/10.1016/j.im.2008.12.007

Spira, L.F., Page, M. (2003). *Risk Management: The Reinvention of Internal Control and the Changing Role of Internal Audit*. ICAEW.

Tarling, K. (2023). *The Service Organization*. London Publishing Partnership.

Teichmann, F.M., Boticiu, S.R. (2023). An overview of the benefits, challenges, and legal aspects of penetration testing and red teaming. *International Cybersecurity Law Review*, 4, 387–397. https://doi.org/10.1365/s43439-023-00100-2

Valcesia, T.M., Rigo, A.L. (2019). Physical or virtual firewall for perimeter protection in cloud computer infrastructure. In *16th CONTECSI – International Conference on Information Systems and Technology Management*. https://doi.org/10.5748/16CONTECSI/ITM-6115

Vargo, S.L., Lusch, R.F. (2004). Evolving to a new dominant logic for marketing. *Journal of Marketing*, *68*(1), 1–17. https://doi.org/10.1509/jmkg.68.1.1.24036

Vielberth, M., Böhm, F., Fichtinger, I., Pernul, G. (2020). Security operations center: a systematic study and open challenges. *IEEE Access*, 8, 227756–227775. https://doi.org/10.1109/ACCESS.2020.3045514

Wagner, T.D., Mahbub, K., Palomar, E., Abdallah, A.E. (2020). Cyber threat intelligence sharing: survey and research directions. *Computers & Security*, 87, art. 101589. https://doi.org/10.1016/j.cose.2019.101589

Werlinger, R., Hawkey, K., Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security*, *17*(1), 4–19. https://doi.org/10.1108/09685220910944722

Wilson, S., Hamilton, D., Stallbaum, S. (2020). *The unaddressed gap in cybersecurity: human performance*. MIT Sloan Management Review, 26.05. https://sloanreview.mit.edu/article/the-unaddressed-gap-in-cybersecurity-human-performance/ [accessed: 18.01.2026].

Yan, D. (2020). A systems thinking for cybersecurity modeling. *arXiv preprint*, arXiv:2001.05734. https://arxiv.org/pdf/2001.05734 [accessed: 18.01.2026].

Annex 1

Lou Downe recommends a structured approach to the following (Downe, 2022: 55):

1. Naming: The designation of a service constitutes a primary determinant of its discoverability and usability. An effective name should accurately convey the service's intended function and employ terminology that aligns with users' conceptual models and linguistic expectations.
2. Description: A service description should answer the following questions: a) What does the service do? b) How does the service work? c) Who is the service for? d) Why does the service exist?

A list of "user-friendly" cybersecurity service-oriented names and descriptions is presented in Table 2.

Table 2. Service-oriented naming convention for cybersecurity services

Traditional name	Service oriented name	Service description
Risk Assessment and Management	Identify and prioritize security risks	What: Identify and rank organizational security risks; How: risk workshops, assetbased assessments, risk register and treatment plans; (for) Who: business owners, product teams, executives; Why: to focus investment and reduce the most important risks.
Policy and Standards Management	Set security rules and guidance	What: Create and maintain security policies and standards; How: policy drafting, approval cycles, and publication with exception process; Who: all employees and system owners; Why: to provide clear expectations and consistent controls across the organization.
Compliance and Audit Support	Help with regulatory and audit requirements	What: Support compliance with laws and standards and prepare audit evidence; How: gap assessments, control mapping, evidence collection and remediation tracking; Who: legal, compliance, auditors, business units; Why: to meet legal obligations and reduce regulatory risk.
ThirdParty and Supply Chain Risk Management	Assess and manage supplier security	What: Evaluate and monitor supplier security posture; How: questionnaires, risk scoring, contractual controls and periodic reviews; Who: procurement, vendor managers, business owners; Why: to reduce risk introduced by partners and suppliers.
Security Strategy and Advisory	Security strategy and advice for leaders	What: Strategic planning and executive security advice; How: roadmaps, investment cases, board briefings and risk prioritization; Who: executives, business leaders, board; Why: to align security with business goals and guide decisions.
Security Operations Center Monitoring	24/7 threat monitoring and alerting	What: Continuous monitoring for threats and suspicious activity; How: telemetry collection, alert triage and escalation to owners; Who: all operational teams and incident responders; Why: to detect attacks early and reduce impact.
Incident Response and Recovery	Respond to and recover from security incidents	What: Contain, investigate and restore after security incidents; How: playbooks, forensics, coordination with IT and business and postincident reviews; Who: affected teams, executives, customers as needed; Why: to minimize disruption and restore normal operations quickly.
Vulnerability Management	Find and fix security weaknesses	What: Discover and prioritize software and configuration weaknesses; How: automated scanning, risk scoring and remediation tracking with owners; Who: system owners, developers, IT ops; Why: to reduce exploitable weaknesses before attackers find them.
Identity and Access Management Services	Manage user access and privileges	What: Provision and control user identities and access rights; How: onboarding/offboarding, single signon, multifactor authentication and privileged access controls; Who: employees, contractors, partners; Why: to ensure only authorized users access resources.

Traditional name	Service oriented name	Service description
Threat Intelligence and Threat Hunting	Provide threat insights and proactive hunting	What: Deliver context about threats and proactively search for intrusions; How: curated intelligence feeds, analyst reports and hunting playbooks executed against telemetry; Who: SOC, incident responders, risk teams; Why: to anticipate threats and find hidden compromises.
Endpoint Detection and Response Operations	Protect and remediate endpoints	What: Detect and respond to threats on laptops, servers and devices; How: endpoint monitoring, containment actions and remediation guidance; Who: device owners, IT support, SOC; Why: to stop malware and lateral movement on endpoints.
Application Security	Secure application design and testing	What: Reduce vulnerabilities in software and services; How: threat modelling, secure code reviews, automated scanning and remediation guidance; Who: developers, product owners, QA; Why: to prevent applicationlevel breaches and protect customers.
Cloud Security and DevSecOps	Secure cloud services and development	What: Ensure cloud workloads and development pipelines are secure; How: infrastructure as code checks, cloud posture reviews, runtime protections and CI/CD gates; Who: cloud engineers, platform teams, developers; Why: to enable safe cloud adoption and fast, secure delivery.
Network and Perimeter Security	Design and protect network boundaries	What: Protect and segment network traffic and external connections; How: secure network design, firewall and segmentation controls and monitoring; Who: network engineers, IT ops, application owners; Why: to limit attack paths and protect critical systems.
Cryptography and Key Management	Manage encryption and keys	What: Provide and operate encryption, certificates and key lifecycle; How: PKI, hardware security modules, secrets stores and automated rotation; Who: application teams, platform owners, compliance; Why: to protect sensitive data and meet regulatory requirements.
Adversarial Security Testing	Simulate attacks to test defences	What: Validate defences by simulating real attacks; How: scheduled penetration tests, red team exercises and purple teaming with remediation tracking; Who: security teams, system owners, executives for assurance; Why: to reveal gaps and improve detection and response.
Secure Architecture and Design Reviews	Review and approve secure system designs	What: Ensure new systems are designed securely before build; How: architecture reviews, threat modelling and approval gates; Who: architects, project teams, product owners; Why: to prevent costly redesigns and embed security early.
Security Engineering and Automation	Automate security tasks and integrations	What: Build automation to scale security operations and controls; How: playbooks, orchestration, telemetry pipelines and CI/CD integrations; Who: security engineers, SREs, SOC; Why: to reduce manual work, speed response and improve consistency.

Traditional name	Service oriented name	Service description
Security Awareness and Training Programs	Train staff on security and phishing	What: Educate employees to reduce human risk; How: rolebased training, simulated phishing and targeted campaigns; Who: all employees, contractors and privileged users; Why: to lower incidents caused by human error and social engineering.
Data Protection and Privacy Services	Protect sensitive data and privacy	What: Classify, protect and manage sensitive data and privacy obligations; How: data classification, encryption, access controls and privacy impact assessments; Who: data owners, legal, product teams; Why: to prevent data loss and meet privacy laws.
Business Continuity and Resilience	Plan for business continuity and recovery	What: Prepare for and recover from major disruptions; How: disaster recovery plans, tabletop exercises and recovery runbooks; Who: business continuity owners, IT, executives; Why: to ensure critical services continue and recover quickly after incidents.
Security Advisory and Virtual CISO	Ondemand security advice for teams	What: Provide expert security guidance and temporary leadership; How: advisory sessions, project support and strategic reviews; Who: business units, small teams, executives without full security leadership; Why: to make informed security decisions and accelerate initiatives.
Security Reporting and Metrics	Security reporting and performance metrics	What: Provide visibility into security posture and service performance; How: dashboards, regular reports, KPIs and executive summaries; Who: executives, risk committees, service owners; Why: to inform decisions, track progress and demonstrate compliance.

Source: created by the author.

Cybersecurity Services: Definition and Relationship with Risk & Control Frameworks

Abstract

This conceptual paper examines cybersecurity services and their relationship with organizational risk and control (R&C) frameworks. Addressing terminological inconsistencies and the lack of internal service-oriented perspectives in the existing literature, the study synthesizes current knowledge to propose a unified definition of cybersecurity services and analyzes how such services integrate with governance and operational mechanisms. A structured literature synthesis was conducted across cybersecurity, information systems, management science and organizational security publications. The qualitative synthesis identified recurring themes, definitions and service taxonomies. A structured coding scheme classified cybersecurity services and mapped them to R&C artefacts, including policies, procedures and technical controls from ISO 27001 Annex A and NIST.

The study defines cybersecurity services as business-facing, outcome-oriented organizational offerings that safeguard assets in cyberspace whilst managing specialized costs,

complexity and risks. A four-domain service taxonomy is introduced: governance, operations, engineering and cross-cutting services. The analysis demonstrates how these services operate within layered risk-mitigation ecosystems, where policies provide strategic direction, procedures ensure consistent implementation, and controls deliver operational safeguards.

Cybersecurity services form an integrative mechanism linking managerial and technical dimensions of organizational security. The framework proposed here enhances conceptual clarity, positions cybersecurity as a value-enabling capability, and strengthens resilience in threat-intensive environments. This study contributes one of the first structured mappings between cybersecurity services and R&C frameworks, offering practical guidance for improving secure digital operations.

Keywords: cybersecurity services, risk management, governance, incident response, value co-creation

Author Contributions
Arkadiusz Rokicki: Conceptualization, Methodology, Formal analysis, Investigation, Resources, Visualization, Writing – original draft, Writing – review & editing.

Supplementary Materials
Not applicable.

Funding
This research received no external funding.

Ethics Approval Statement
Not applicable.

Informed Consent Statement
Not applicable.

Data Availability Statement
The data analysed in this study came from publically avaialble academic and industry publications.

Declaration of Generative AI Use
No artificial intelligence tools were used in the preparation of this manuscript.

Acknowledgments
Not applicable.

Conflict of Interest
Arkadiusz Rokicki declares no conflict of interest.