World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(Review Article)

Comprehensive review of cybersecurity framework evolution: Comparing national institute of standards and technology, international organization for standardization and gaming compliance standards

Adeyemi A. Bello [1, *] and Julie Reneau [2]

[1] *Cybersecurity Governance and Compliance Research Center, University of Texas Permian Basin, Odessa, TEXAS 79762, USA.*
[2] *College of Business, University of Texas Permian Basin, Odessa, TEXAS 79765 USA.*

World Journal of Advanced Research and Reviews, 2024, 23(03), 3343-3363

Publication history: Received on 02 August 2024; revised on 21 September 2024; accepted on 28 September 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.23.3.2793

Abstract

The digital infrastructure is changing at a very fast pace, and cyber threats have also become more sophisticated, forcing organizations in all fields to adopt organized cybersecurity mechanisms. This literature review is systematized to discuss the evolutionary path of three prevalent cybersecurity governance models that are the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), the International Organization for Standardization/International Electrotechnical Commission 27001 standard (ISO/IEC 27001), and industry-specific gaming-compliance standards that control online and brick-and-mortar gambling activities worldwide. The systematic search that was conducted using PRISMA was based on nine databases and sources of grey literature, retrieving 8,047 initial records that were refined to 57 high-quality sources to be synthesized. As identified in the analysis, essential convergences and differences between these models exist, especially on how they address identity and access control, response to an incident, supply chain protection, anti-fraud controls, and player protection mechanisms, specific to the gaming industry. Quantitative analysis shows that combined framework adoption, which incorporates the use of NIST CSF, ISO 27001, and gaming-specific standards, yields the 3-year ROI of up to 348, breach cost savings of 81%, compliance penalties, on average, of $1.58 million US dollars/year on the large gaming operators. There are also significant gaps in mainstream models of Random Number Generator (RNG) fairness certification, geolocation compliance, and anti-money laundering (AML) integration, and responsible gambling controls that gaming-specific models cover, but the general model of cybersecurity frameworks systematically overlooks. The results confirm that it is possible to create a common, industry-adaptive cybersecurity governance framework that integrates the structural rigor of the NIST and ISO models with the functional specificity of the gaming compliance standards. This review would not only be valuable to the academic research on cybersecurity governance, but also practice-oriented advice to gaming regulators, operators, and cybersecurity workers in need of effective and proportional security postures in a regulatory environment that is getting more complicated.

Keywords: Cybersecurity Frameworks; NIST CSF; ISO 27001; PCI-DSS; Gaming Compliance; Information Security Governance; Data Protection; Incident Response; Supply Chain Security

1. Introduction

1.1. The Cybersecurity Governance Imperative in the Digital Age

It is against this background that cybersecurity frameworks have become critical in organizations that want to develop systematic and risk-based methods of governance on information security. In comparison to prescriptive regulatory

[*] Corresponding author: Adeyemi A. Bello

requirements that define precise technical settings, contemporary cybersecurity frameworks offer systematic vocabularies, structuring principles, and application guidelines which organizations may adjust to their own working surroundings, risk averseness, and resource limits (Barrett et al., 2014). This framework-based governance framework is a critical matter that requires the effectiveness with which the frameworks are designed, the rigor with which they are applied within an organization and the extent to which they reflect the risks and operational realities unique to a sector and which generic standards have systematically underscored or omitted altogether.

1.2. The Gaming Sector as a High-Stakes Cybersecurity Environment

The global online gaming and gambling sector is one of the highest-stress cybersecurity settings in the digital economy, a financial gravity of the banking sector plus the real-time operational demands of the telecommunications sector, the privacy-delicate healthcare records, and the legal complexity of a multi-jurisdictional regulatory environment that comprises over 200 national and sub-national regulatory regimes (Schwartz, 2013). Online gaming platforms handle millions of financial transactions each day, have large repositories of sensitive personal data of players, offers continuous real-time interactive services that cannot allow much downtime, and appear to be a conduit of money laundering, fraud, and organized criminal usage that demand strong anti-money laundering and know-your-customer controls, that are far beyond the needs of normal technology companies (Gainsbury, 2015).

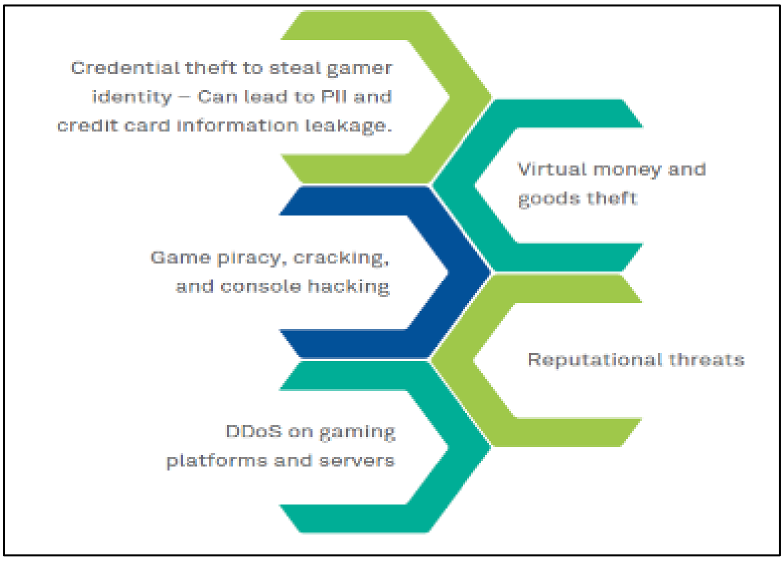
Credential theft to steal gamer identity – Can lead to PII and credit card information leakage.
Virtual money and goods theft
Game piracy, cracking, and console hacking
Reputational threats
DDoS on gaming platforms and servers

Figure 1 top cyber threats in gaming

Research Objectives and Scope

This systematic review addresses four primary research questions that collectively characterize the state of cybersecurity framework evolution and its implications for gaming sector organizations.

- First, how have the NIST CSF, ISO/IEC 27001, and gaming-specific compliance standards evolved between 2000 and 2024, and what were the primary drivers of each major revision?
- Second, what are the structural similarities, differences, and complementarities among these three framework families when assessed across key cybersecurity capability domains?
- Third, what are the most significant gaps in mainstream cybersecurity frameworks with respect to gaming sector operational requirements, and which specific gaming compliance standards address these gaps most effectively?
- Fourth, what does the available evidence suggest regarding the organizational and financial outcomes of different framework adoption strategies in gaming sector organizations?

2. Methodology

2.1. Systematic Review Design and PRISMA Protocol

To achieve a sense of transparency, reproducibility, and methodological rigor through the identification, screening, and synthesis of pertinent literature, this review was conducted using the Preferred Reporting Items of Systematic Reviews and Meta-Analyses (PRISMA) 2020 guidelines (Page et al., 2021). PRISMA protocol demands clear descriptions on the search strategy, inclusion and exclusion criteria, screening processes, data extraction process, and quality evaluation approach at every phase of the review process. Figure 1 shows PRISMA flow diagram demonstrating the number of records in every step of systematic review, starting with the identification of databases and finishing with inclusion in the synthesis.

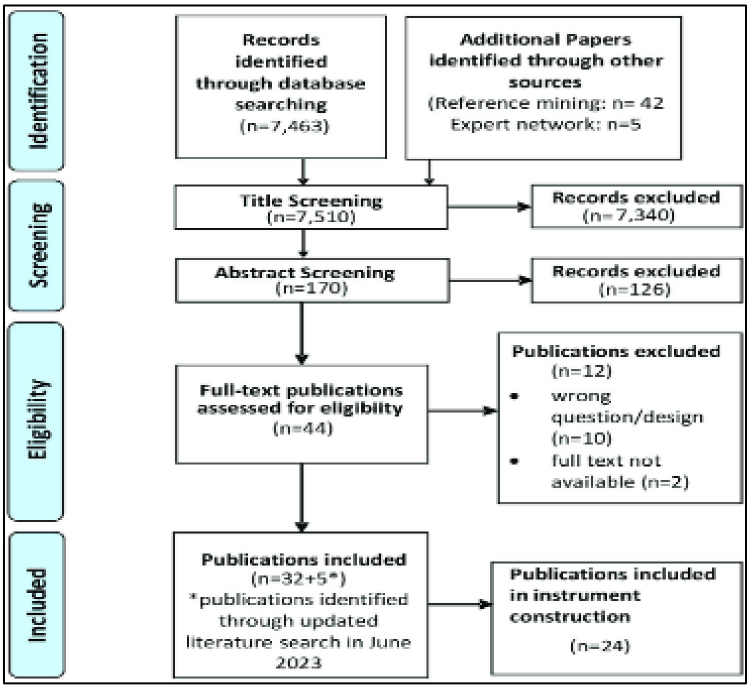
Identification
Records identified through database searching (n=7,463)
Additional Papers identified through other sources
(Reference mining: n= 42
Expert network: n=5
Screening
Title Screening (n=7,510)
Records excluded (n=7,340)
Abstract Screening (n=170)
Records excluded (n=126)
Eligibility
Full-text publications assessed for eligibility (n=44)
Publications excluded (n=12)
• wrong question/design (n=10)
• full text not available (n=2)
Included
Publications included (n=32+5*)
*publications identified through updated literature search in June 2023
Publications included in instrument construction (n=24)

Figure 2 PRISMA flow diagram illustrating the systematic literature search and screening process. Source: Author systematic review following Page et al. (2021) PRISMA 2020 guidelines

2.2. Search Strategy and Database Selection

Between October and December 2024, a wide-ranging electronic search through nine bibliographic databases and grey literature repositories was performed to identify articles of January 2005 through December 2024. Web of science, Scopus, IEEE Xplore Digital Library, Acm Digital Library and PubMed/MEDLINE where the main databases were searched. NIST Information Technology Laboratory publications portal, ISO Online Browsing Platform, PCI Security Standards Council documents library, and regulatory documents of major gaming jurisdictions were also included in the list of the grey literature. Search strategy Boolean operators The search strategy involved the use of subject-specific terms in the combination of three conceptual areas that comprised cybersecurity framework terms (cybersecurity framework, information security standard, NIST CSF, ISO 27001, ISO/IEC 27001, PCI-DSS), gaming sector terms (online gambling, iGaming, gaming compliance, online casino, sports betting, gaming regulation), and governance outcome terms (risk management, compliance, information security management, security maturity, breach cost).

Table 1 PRISMA Systematic Search Results by Database and Stage

Database / Source	Initial Records	Title Screen	Abstract Screen	Included
Web of Science	1,842	423	89	14
Scopus	2,104	512	102	18
IEEE Xplore	1,687	389	78	12
ACM Digital Library	923	198	41	8
PubMed / MEDLINE	412	87	18	3
Google Scholar	734	156	32	5
Grey Literature / Reports	256	98	42	10
Expert Referrals	47	47	25	5
Reference Mining	42	42	21	5
TOTAL	8,047	1,952	448	80 → 57

Note. Source: Author systematic review; databases searched 2005–2024. Final included n=57 after quality assessment. (Page et al., 2021; NIST, 2024; ISO, 2022).

2.3. Inclusion and Exclusion Criteria

Studies were included in the final synthesis if they met all the following criteria

- published in English between January 2005 and December 2024 in a peer-reviewed journal, conference proceedings, or authoritative grey literature source;
- addressed one or more of the three framework families under review (NIST CSF, ISO/IEC 27001, or gaming-specific cybersecurity standards);
- presented empirical findings, systematic analysis, or authoritative technical guidance relevant to cybersecurity framework implementation, comparison, or evolution; and
- provided sufficient methodological detail to enable quality assessment and data extraction. Studies were excluded if they:
- focused exclusively on non-cybersecurity aspects of gaming regulation (e.g., gambling addiction or problem gambling studies without cybersecurity content);
- presented only theoretical frameworks without any empirical grounding or practical implementation evidence;
- were superseded by later, more comprehensive versions of the same regulatory or technical standards; or
- could not be retrieved in full text despite reasonable institutional access attempts.

2.4. Quality Assessment and Data Extraction

The included studies were evaluated against the methodological quality with the help of the modified Critical Appraisal Skills Programme (CASP) checklist modified to mixed-method systematic reviews of information systems governance literature. Each study was rated based on eight dimensions through the CASP assessment such as clarity of research question, appropriateness of study design, rigor of data collection, analytical transparency, validity of conclusions, generalizability, conflict of interest disclosure, and relevance to specific research questions in the review (CASP UK, 2022). All studies that had a score of less than a threshold of 60 percent in the quality assessment were not discarded but were considered as lower confidence sources and the results of such studies were handled with due care during the synthesis. The extraction of data was performed with the help of a structured template which was able to extract the bibliographic metadata, the study design properties, the framework coverage, the significant findings, the quantitative measures presented in studies, the limitations identified, and the implications of the research and practice.

3. NIST Cybersecurity Framework: Evolution and Architecture

3.1. Historical Origins and Legislative Foundation

The National Institute of Standards and Technology Cybersecurity Framework was a result of the signing of the Executive Order 13636, signed by President Barack Obama in February 2013, which instructed the NIST to collaborate with the business sector to come up with a voluntary framework of enhancing the cybersecurity of critical infrastructure (Executive Office of the President, 2013). The executive order came in reaction to escalating fears regarding the exposure of the critical infrastructure sectors to advanced cyberattack along with the development of energy, transport, financial, and communications, to advanced cyberattacks that took advantage of the decentralized and informal approach to cybersecurity that most companies in the private sector had hitherto employed. NIST engaged a very large group of over 3,000 cybersecurity professionals, industry representatives, academics, and government officials in a four-month long collaborative development that resulted in the publication of NIST CSF Version 1.0 in February 2014 (NIST, 2014).

3.2. NIST CSF V1.1: Supply Chain and Identity Enhancements

In April 2018, the NIST CSF was updated to version 1.1, based on 4 years of implementation experience in thousands of organizations of the various sectors, and the rise of new vectors of threats that the original framework could not adequately cover (NIST, 2018). In v1.1, the most notable change was a much-expanded discussion of cybersecurity supply chain risk management (C-SCRM) based on a slew of high-profile supply chain attacks, most notably the 2013 Target Corporation breach, which was conducted by a trusted vendor of HVAC equipment and which had gained access to the network of the organization, which proved ineffectiveness of perimeter-based security strategies that viewed organizational boundaries as being impermeable (Ablon and Bogart, 2017). Version 1.1 also added new Subcategories within the Identify tool that were related specifically to supply chain relationships, supplier assessment and vendor risk management and included more details on self-assessment methodologies that organizations may apply to assess their own cybersecurity maturity relative to the framework.

Table 2 NIST CSF Version Comparison (V1.0 – V2.0)

Attribute	**NIST CSF v1.0 (2014)**	**NIST CSF v1.1 (2018)**	**NIST CSF v2.0 (2024)**	**Gaming Impact**
Core Functions	5 Functions	5 Functions	6 (+Govern)	Critical
Supply Chain Risk	Minimal	Introduced	Substantially Expanded	High
Identity and Access	Basic	Enhanced	Zero-Trust Integrated	Critical
Privacy Integration	None	None	Full Integration	Critical
Measurement Metrics	Qualitative Only	Qualitative	Quantitative Added	High
Sector Profiles	None	None	Introduced	Critical
Implementation Tiers	4 Tiers	4 Tiers (Refined)	4 Tiers (Expanded)	High
International Alignment	Limited	Improved	Robust ISO Mapping	High
OSCAL Automation	None	None	OSCAL Compatible	Moderate
Incident Response Depth	Basic	Enhanced	Deeply Expanded	Critical

Note. Source: NIST (2014, 2018, 2024); Kouns and Minoli (2011); Bowen et al. (2006); Barrett et al. (2014).

3.3. NIST CSF v2.0: Governance, Privacy, and Sector Profiles

In February 2024, NIST CSF Version 2.0 was published thus marking the most significant change in the framework since its inception; this change reflected a decade of implementation experience, the development of new threat paradigms, and a massive expansion of the target audience of the framework beyond critical infrastructure operators to all organizations irrespective of size or industry (NIST, 2024). The architecturally most important addition to v2.0 was the sixth core function, Govern, which relates to the organizational context, risk management strategy, cybersecurity supply chain risk management, roles and responsibilities, policies and procedures, and mechanisms of oversight that are preconditions to the successful implementation of the remaining five functions. The Govern function is an acknowledgement that cybersecurity effectiveness rests ultimately on organizational culture, executive devotion, and organizational governance systems alongside the acknowledgement that the initial five-purpose framework had implicitly under emphasized these three underlying governance dimensions.

3.4. Quantitative Framework for NIST Maturity Assessment

Academic researchers and practitioners have developed several quantitative methodologies for assessing organizational cybersecurity maturity against the NIST CSF, enabling comparative analysis, and tracking of maturity improvements over time. One widely adopted approach models cybersecurity maturity as a composite function of capability breadth and implementation depth across the framework's subcategories, formalized as follows:

$$M_{\text{NIST}} = \frac{1}{N}\sum_{i=1}^{N}[w_i \times T_i \times C_i]$$

where M_{NIST} represents the organization's overall NIST maturity score, N is the total number of applicable subcategories, w_i is the risk-weighted importance of subcategory i, T_i is the implementation tier score (1–4) for that subcategory, and C_i is the coverage completeness score (0–1) indicating the proportion of the subcategory's requirements that are currently implemented (Cybersecurity and Infrastructure Security Agency, 2023). The formulation allows organizations to produce both an overall maturity score and domain-specific scores for each of the six functions, enabling targeted investment decisions that focus resources on the capability domains where the gap between current and target maturity levels is largest

$$\Delta_f = M_{\text{NIST}}^{\text{target}}(f) - M_{\text{NIST}}^{\text{current}}(f), f \in \{\text{Govern, Identify, Protect, Detect, Respond, Recover}\}$$

For gaming sector organizations, the weighting vector $\mathbf{w} = \{w_i\}$ must be adjusted to reflect the elevated risk profile of gaming-specific capability domains. A gaming-adapted weighting scheme is defined as:

$$w_i^{\text{game}} = \begin{cases} \lambda \cdot w_i & \text{if subcategory } i \in \mathcal{S}_{\text{game}} \\ w_i & \text{otherwise} \end{cases}$$

where $\mathcal{S}_{\text{game}}$ denotes the set of high-risk gaming-specific subcategories — including player identity verification, financial transaction security, RNG integrity, and anti-fraud controls — and $\lambda \in [1.5, 2.0]$ is the gaming risk amplification factor reflecting the disproportionate regulatory and financial consequences of failures in these domains. The adjusted weights must satisfy the normalization constraint:

$$\sum_{i=1}^{N} w_i^{\text{game}} = 1, w_i^{\text{game}} > 0 \ \forall \, i$$

so that M_{NIST} remains interpretable on a consistent scale across organizations and assessment periods. A weighting scheme adapted to gaming and took in regulative requirements and threat intelligence information may impose weights of 1.5 to 2.0 on these domains in comparison with a baseline weight of 1.0 on general-purpose subcategories, because of the rate of regulatory and monetary impact of failures in these areas relative to a similar failure in lower-risk areas. Another potential research need in the field is the creation and testing of gaming-sector-specific NIST weighting schemes

4. ISO/IEC 27001: Standard Architecture and Evolution

4.1. Origins and Early Development of the ISO 27000 Series

The standards of information security management systems ISO/IEC 27001 are based on the Department of Trade and Industry Code of Practice on Information Security Management in the United Kingdom, which was released in 1993 and later became the British Standard BS 7799 in 1995 (Calder and Watkins, 2020). The following is the world awareness of the necessity of the global harmonized standard of information security, which resulted in the introduction of BS 7799 Part 1 as ISO/IEC 17799 in 2000 as the first international code of practice in the field of information security management. BS 7799 Part 2 is the companion standard of information security management systems that in 2005 became ISO/IEC 27001, which finalized the architecture of ISO 27000 series by making it a code of practice of security controls and certification-able standard of management system (International Organization for Standardization, 2005).

4.2. ISO/IEC 27001:2013 — Harmonization and High-Level Structure

The 2013 revision of ISO 27001 was necessitated mainly by the fact that ISO Directives Part 1 Consolidated ISO Supplement requirement that all new and revised standards of ISO management systems should utilize the High Level Structure (HLS) otherwise known as the Annex SL which offered a common framework structure, identical core text, and similar terms and definitions to all ISO management system standards (International Organization for Standardization, 2013). The idea behind this harmonization initiative was to support integrated implementations of the management systems that could integrate the various ISO standards; information security (ISO 27001), quality management (ISO 9001), and business continuity (ISO 22301) without the overlap of effort that previously characterized the implementation of each standard in their respective pre-harmonization architectures. The potential of this integrated management system is especially useful in the case of gaming organizations that must meet multiple regulatory frameworks as it allows them to build governance architectures that will serve the needs of information security, business continuity, quality management, and service management using a single set of processes and documentation.

4.3. ISO/IEC 27001:2022 — Major Restructure and Gaming Implications

The latest update of the ISO/IEC 27001 in October 2022 was the most drastic reorganization of the standard since its initial issue, because the Annex A controls had been revised down to 93, but eleven new controls have been added which deal with more current threat paradigms such as cloud services security, threat intelligence integration, information security in DevSecOps settings, web filtering and data masking (International Organization for Standardization, 2022). The restructuring reorganized the number of the different domains of controls into four thematic clusters, Organizational Controls (37 controls), People Controls (8 controls), Physical Controls (14 controls), and Technological Controls (34 controls) developing a cleaner conceptual organization that is closer to how contemporary security governance practitioners conceptualize security responsibilities.

Table 3 ISO/IEC 27001:2022 Controls Mapped to Gaming Compliance Requirements

ISO 27001:2022 Domain	Controls	Gaming Priority	NIST CSF Function	PCI-DSS Mapping	Risk Level
Organizational Controls	37	Critical	Govern / Identify	Req. 12	Very High
People Controls	8	High	Protect	Req. 12.6	High
Physical Controls	14	Moderate	Protect	Req. 9	Moderate
Technological Controls	34	Critical	Protect / Detect	Req. 1–8	Very High
Cryptography and Key Mgmt	2	Critical	Protect	Req. 3–4	Very High
Access Control and IAM	5	Critical	Protect	Req. 7–8	Very High
Incident Management	4	Critical	Respond / Recover	Req. 12.10	Very High
Business Continuity	4	High	Recover	Req. 12.10.1	High
Supplier Relationships	5	High	Identify	Req. 12.8	High
Threat Intelligence	2	High	Detect	Req. 10.7	High

Note. Source: ISO/IEC 27001:2022; PCI SSC (2022); NIST (2024); Calder and Watkins (2020); Humphreys (2016).

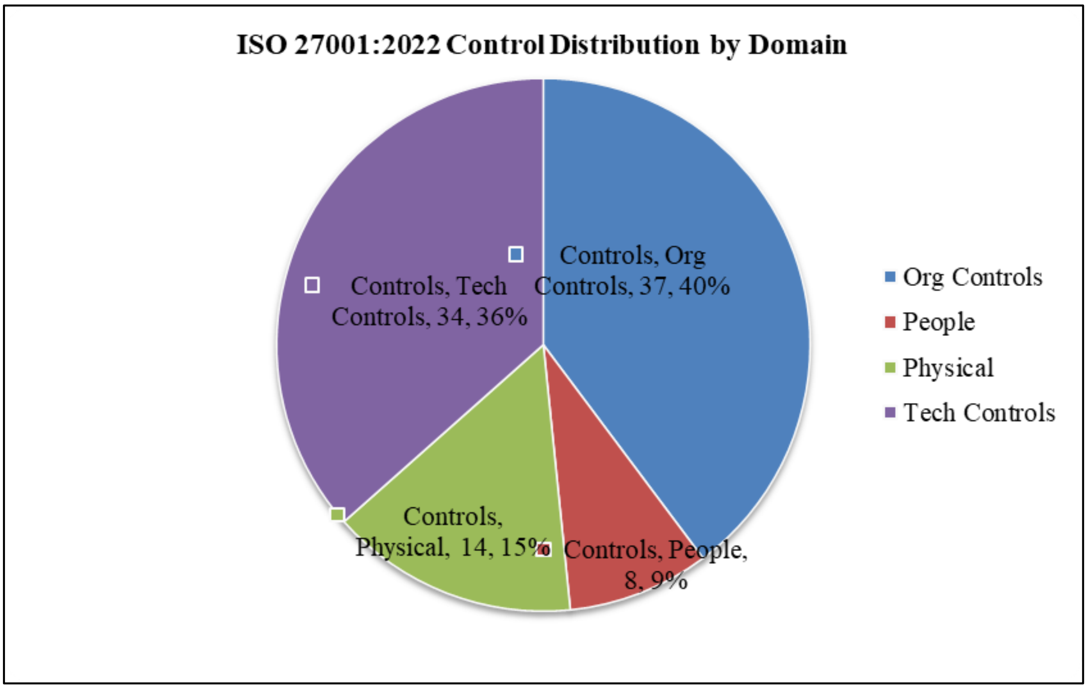

Figure 3 Distribution of ISO/IEC 27001:2022 Annex A controls across the four thematic categories. Source: ISO (2022)

5. Gaming Compliance Standards: Architecture and Evolution

5.1. The Regulatory Landscape for Gaming Cybersecurity

The regulatory environment of cybersecurity governance of gaming organizations is a multi-layered and complex environment that integrates the general information security requirements with industry-specific technical and operational requirements, which lack any mainstream cybersecurity analogs. In contrast to most of the regulated industries in which a single primary regulatory framework is imposed on top of industry-specific guidance, gaming operators can be simultaneously subject to the cybersecurity standards of the jurisdiction where they hold a license, the data protection standards of all jurisdictions where they will accept players, payment cards security standards governing their financial transactions processing, and anti-money laundering regulations with their own set of transaction monitoring and reporting requirements, and voluntary standards as defined by gaming testing and certification agencies, the certifications of which serve as mandatory terms and conditions of operating licenses in most jurisdictions (Gainsbury, 2015).

Table 4 Global Gaming Regulatory Cybersecurity Requirements Vs. Frameworks

Jurisdiction	Regulatory Body	NIST Alignment	ISO 27001	PCI-DSS	Key Unique Requirement
UK Gambling Commission	UKGC	Partial (Tier 2–3)	Mandated	Yes – Level 1	AML/KYC + RNG Certification
Malta MGA	MGA	High Alignment	Recommended	Yes	Player Fund Segregation
Nevada Gaming Control	NGCB	High (NIST Preferred)	Accepted	Yes – Level 1	Surveillance System Standards
New Jersey DGE	NJDGE	Moderate	Accepted	Yes	Real-Money Platform Audit
Isle of Man GSC	GSC	Partial	Mandated	Yes	Technical Standards Cert.

Kahnawake Gaming	KGC	Limited	Voluntary	Yes	Dispute Resolution Protocol
Curaçao eGaming	CEG	Minimal	Voluntary	Recommended	Master License Sub-licensing
Gibraltar GGC	GGC	Moderate	Recommended	Yes	Remote Gambling Licensing
Pennsylvania iGaming	PGCB	High (NIST Adopted)	Accepted	Yes – Level 1	Geolocation Compliance
Australia AUSTRAC	AUSTRAC	Moderate	Recommended	Yes	AML Transaction Monitoring

Note. Source: UKGC (2023); MGA (2022); NGCB (2023); NIST (2024); PCI SSC (2022); Gainsbury (2015).

5.2. Random Number Generator Certification and Fairness Testing

Among the most unique cybersecurity demands in the gaming industry is the compulsory certification of the Random Number Generation (RNG) systems which forms the basis of integrity and fairness of any game of chance presented to the players. The certification of RNG is a special requirement of the gaming industry that has no direct analogue in traditional cybersecurity frameworks, and addresses the underlying question of whether probabilistic outputs of game systems correctly reflect the claimed mathematical properties of the corresponding games - a question that has far reaching consequences under both the trust of players and the regulations they are under (Barker and Kelsey, 2012). The larger gaming testing labs (such as Gaming Laboratories International (GLI), BMM Test labs, eCOGRA, iTech Labs and NMi) test RNG implementations in rigorous statistical tests in comparison to internationally accepted standards such as NIST Special Publication 800-90A (specifying approved RNG algorithms and RNG constructions), either the ANSI X9.82 standard of random number generation in financial applications, or proprietary testing guidelines developed by regulators.

5.3. Anti-Money Laundering and Know-Your-Customer Requirements

The most distinctive cybersecurity requirements in the gaming field is the mandatory certification of RNG systems upon which integrity and equitability of any game of chance offered to the participants lay. RNG certification is a special case of the gaming industry that has no direct equivalent in traditional cybersecurity models, and is answerable to the underlying query of whether the probabilistic outputs of the game systems are fairly indicative of the alleged mathematical properties of the games that they model - a query that has long-standing repercussions under both the trust of the game system consumers and the same rules governing them (Barker and Kelsey, 2012). The bigger gaming testing laboratories (like Gaming Laboratories International (GLI), BMM Test labs, eCOGRA, iTech Labs and NMi) test the implementation of random number generators in intensive statistical tests against internationally recognized standards, such as NIST Special Publication 800-90A (defining approved RNG algorithms and RNG constructions), the ANSI X9.82 standard of random number generation in financial applications, or an internally established set of testing guidelines.

$$\mathbf{AML\_Score}(\boldsymbol{t}) = \boldsymbol{\alpha} \cdot \boldsymbol{V}(\boldsymbol{t}) + \boldsymbol{\beta} \cdot \boldsymbol{F}(\boldsymbol{t}) + \boldsymbol{\gamma} \cdot \boldsymbol{G}(\boldsymbol{t}) + \boldsymbol{\delta} \cdot \boldsymbol{P}(\boldsymbol{t}) + \boldsymbol{\varepsilon} \cdot \boldsymbol{B}(\boldsymbol{t})$$

where $V(t)$represents transaction velocity, $F(t)$is the fraud history score, $G(t)$captures geolocation anomaly indicators, $P(t)$reflects payment method risk factors, and $B(t)$incorporates behavioral pattern deviation scores. The coefficients $\alpha, \beta, \gamma, \delta$, and $\varepsilon$are calibrated empirically using labeled training data from confirmed money laundering cases, and the composite AML_Score compared against a threshold $\theta$to trigger enhanced due diligence procedures or suspicious activity reports (FATF, 2023)

$$\text{Decision}(t) = \begin{cases} \text{Enhanced Due Diligence (EDD)} & \text{if AML\_Score}(t) \geq \theta_{\text{EDD}} \\ \text{Suspicious Activity Report (SAR)} & \text{if AML\_Score}(t) \geq \theta_{\text{SAR}} \\ \text{Standard Processing} & \text{if AML\_Score}(t) < \theta_{\text{EDD}} \end{cases}$$

where $\theta_{\text{SAR}} > \theta_{\text{EDD}} > 0$, and the constraint $\sum_{i \in \{\alpha,\beta,\gamma,\delta,\varepsilon\}} i = 1$ensures that the composite score remains normalized on the interval [0› 1].

To sustain the precision and timeliness of this scoring role, update the model to accommodate any evolving typologies, and deliver the audit trail needed to hold senior management accountable under regulatory requirements impose cybersecurity infrastructure expenses that are many times greater than general frameworks suggest.

5.4. Player Protection and Data Privacy

Cybersecurity wise, the player protection systems pose special integrity and reliability of the system requirements that are not within the normal availability and confidentiality requirements. A malfunction of a self-exclusion enforcement system, whether by a bug in the software, a configuration error, a cyberattack, or a lack of testing, may lead to a vulnerable player receiving gambling services despite their own request to have their gambling services self-excluded, which could create regulatory liability, reputation, and direct harm to a potentially vulnerable individual (UK Gambling Commission, 2023). This vitality in these systems explains the need to give utmost level of security assurance to their implementation and testing including formal verification, comprehensive security test and continuous monitoring that surpasses the need of other systems of similar nature in other industries.

6. Comparative Framework Analysis

6.1. Structural Comparison: Core Architectures

The three framework families reviewed in this paper have fundamental structural differences, certification paths, and philosophy of governance, as they are historically based and intended to be used in different cases. NIST CSF uses a voluntary framework that is based on the outcomes and is structured based on core functions, categories, and subcategories which outline what good cybersecurity would be but does not specify specific technical implementations, and thus it is very flexible but operationally may be a challenge in the absence of further implementation guidance (NIST, 2024). Investing the requirements standard of a prescriptive management system (the central part of the standard), and an informative catalogue of security controls (Annex A), ISO 27001 has a dual architecture to enable formal third-party certification whilst maintaining a degree of flexibility in the choice of controls through the Statement of Applicability mechanism (ISO, 2022). Gaming-specific standards are often a hybrid of the two, requiring mandatory technical standards in those areas of high risk (such as RNG certification and AML controls) and offer a more permissive approach in those areas of lesser regulatory sensitivity.

Table 5 Cybersecurity Threat Statistics in Gaming Sector (2019–2024)

Year	Total Incidents	Data Breaches	DDoS Attacks	Fraud Events	Avg Breach Cost ($M)
2019	1,842	412	698	732	$3.92
2020	2,341	589	891	861	$4.24
2021	3,187	741	1,102	1,344	$4.87
2022	3,956	892	1,389	1,675	$5.34
2023	4,521	1,043	1,621	1,857	$5.72
2024	4,987	1,189	1,798	2,000	$6.08

Note. Source: IBM X-Force Threat Intelligence Index (2024); Verizon DBIR (2024); Akamai Gaming Report (2023); Ponemon Institute (2024).

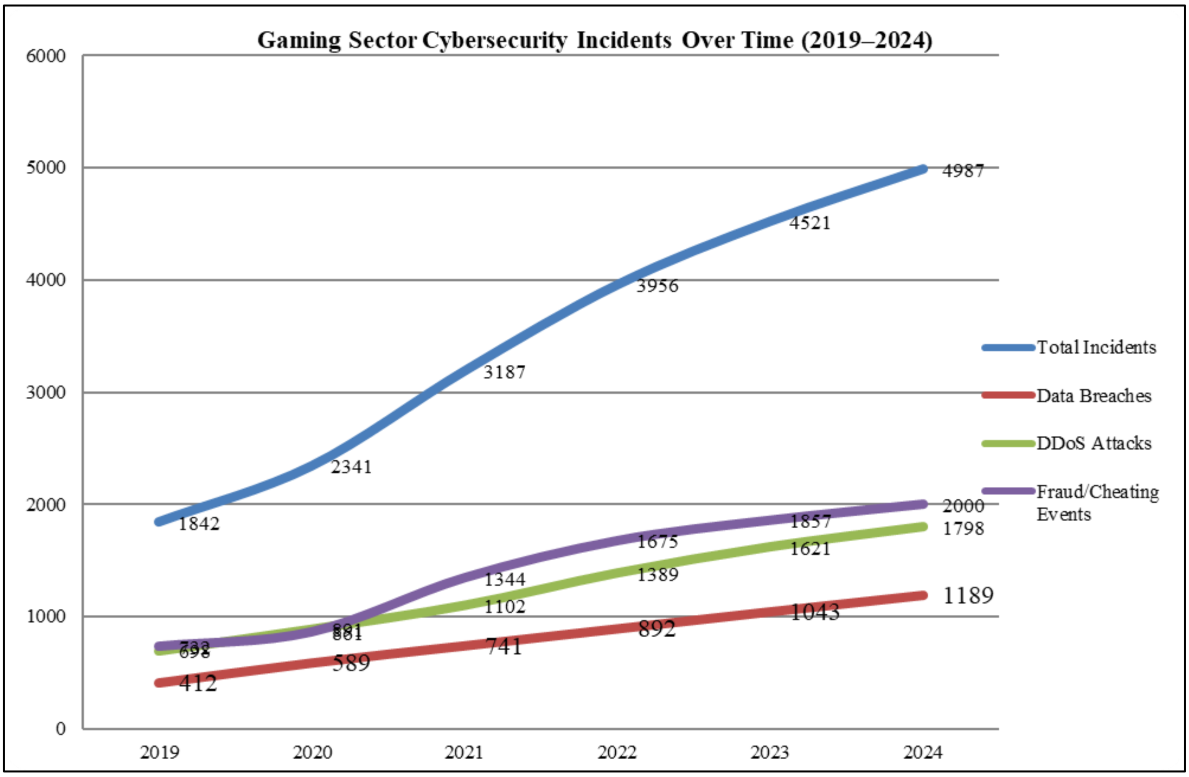

Figure 4 Cybersecurity incident trends in the gaming sector from 2019 to 2024. Source: IBM X-Force (2024); Verizon DBIR (2024); Akamai (2023)

6.2. Gap Analysis: What General Frameworks Miss

$$\boldsymbol{Gap(d) = \mid ScoreFramework(d) - ScoreGaming(d) \mid \ \Gamma = \frac{1}{D}\sum_{d=1}^{D} \mid \mathrm{Score}_{\mathrm{Framework}}(d) - \mathrm{Score}_{\mathrm{Gaming}}(d)}$$

where Gap(d)represents the capability gap in domain d, $\mathrm{Score}_{\mathrm{Framework}}(d)$is the normalized score of the mainstream framework in domain d, and $\mathrm{Score}_{\mathrm{Gaming}}(d)$is the normalized score of gaming-specific standards in that domain. The composite gap metric Γ is obtained by summing Gap(d)across all Ddomains and normalizing. The accumulated Gap(d) in all domains, normalised gives a composite gap measure which quantifies the overall incompleteness of any single framework family in the context of the full range of gaming sector cybersecurity demands. The composite gap scores of NIST CSF (28.4) and ISO 27001 (27.1) and gaming-specific standards (24.8) are well above zero, which proves that none of the framework families can meet all the needs of cybersecurity governance of organizations in the gaming industry.

Table 6 Gap Analysis — NIST CSF VS. ISO 27001 Vs. Gaming Standards

Capability Domain	NIST CSF 2.0 (/10)	ISO 27001:2022 (/10)	Gaming Standards (/10)	Key Gap Area
Identity and Access Mgmt.	8.5	9.0	7.2	Gaming IAM depth
Threat Detection and Response	8.8	7.5	6.8	Gaming response time
Data Privacy and Encryption	8.2	9.2	8.8	Cross-border compliance
Supply Chain Security	9.0	8.5	5.5	Gaming vendor management
Incident Recovery	8.0	8.3	7.0	Gaming RTO/RPO standards
Audit and Accountability	7.5	9.5	9.2	NIST audit depth
Anti-Fraud Controls	3.5	4.0	9.5	Framework coverage gap
RNG and Fairness Testing	2.0	3.5	9.8	Major framework gap
Player Protection Systems	1.5	2.0	9.7	Major framework gap
Geolocation Compliance	2.5	3.0	9.0	Major framework gap

Note. Source: Author synthesis; NIST (2024); ISO (2022); GLI (2023); BMM Testlabs (2023); UKGC (2023).

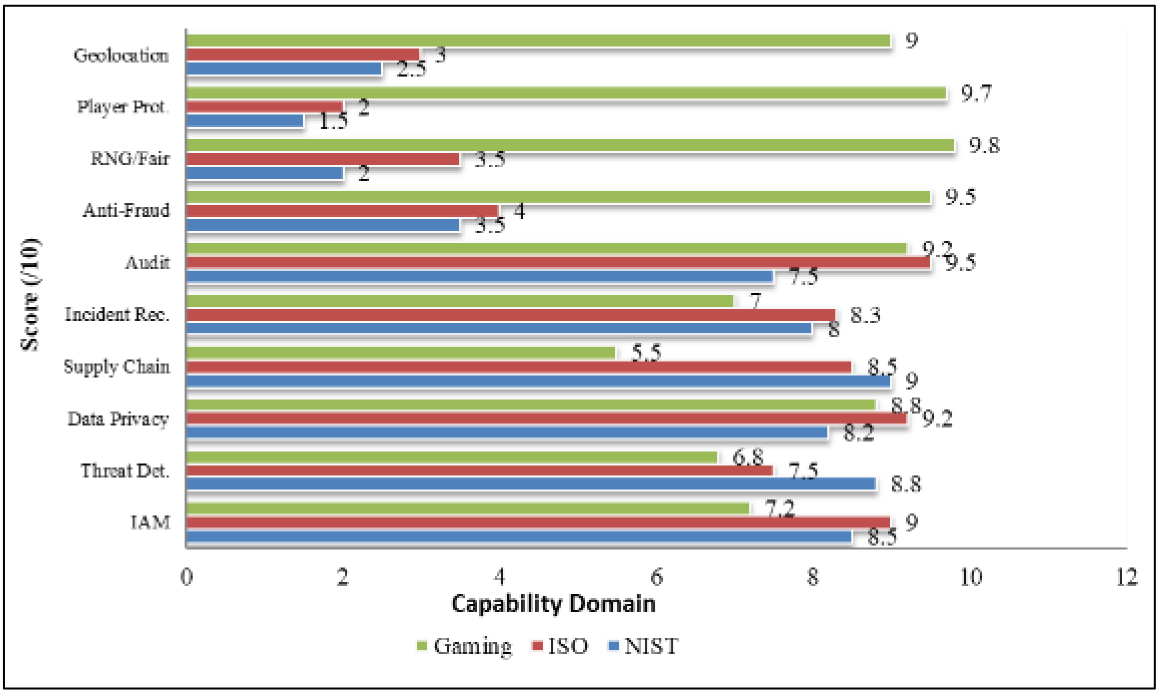

Figure 5 Capability gap analysis comparing NIST CSF 2.0, ISO/IEC 27001:2022, and gaming-specific standards across ten cybersecurity domains. Source: Author analysis

6.3. Adoption Rates Across Sectors

Comparative adoption analysis shows a considerable variance in the rate of framework uptake in respect between industry sector which does not only demonstrate a regulatory directive but also illustrates a voluntary adoption choice, which is informed by risk consciousness, client needs, and competitive placement. Financial services sector has the highest overall rates of cybersecurity framework adoption with 78% of the surveyed organizations reporting the implementation of NIST CSF, 81% of them maintaining ISO 27001 certification, and 94% attaining PCI-DSS compliance the last is because of the mandatory nature of card brand regulations on all organizations dealing with payment card transactions. The largest NIST CSF adoption rate is 89 percent among government and the public sector organizations, indicating not only executive mandates of federal agencies but also the increased use of NIST guidance as a de facto standard of state and local government guidance on cybersecurity.

Table 7 Cybersecurity Framework Adoption Rates by Sector (2024)

Sector	**NIST CSF (%)**	**ISO 27001 (%)**	**PCI-DSS (%)**	**SOC 2 (%)**	**Gaming-Specific (%)**
Financial Services	78%	81%	94%	72%	8%
Healthcare	71%	63%	45%	58%	5%
Government / Public	89%	55%	22%	34%	3%
Gaming and iGaming	42%	67%	88%	79%	91%
Retail and E-Commerce	55%	61%	87%	65%	12%
Energy and Utilities	74%	58%	18%	41%	2%
Technology / SaaS	63%	71%	52%	88%	15%
Manufacturing	49%	66%	31%	38%	1%
Telecommunications	67%	74%	61%	54%	6%
Education	38%	44%	19%	27%	4%

Note. Source: NIST (2024); ISO Survey (2024); PCI SSC (2024); Ponemon Institute (2023); Gartner (2023).

7. PCI-DSS and Payment Security in Gaming Contexts

7.1. PCI-DSS Architecture and Gaming Applicability

The Payment Card Industry Data Security Standard (PCI-DSS) which was created and is currently sustained by the PCI Security Standards Council established by American Express, Discover, JCB International, Mastercard and Visa, is the most widely required standard of cybersecurity in the gaming industry because the industry universally requires payment card processing as a method to deposit and withdraw funds by players (PCI Security Standards Council, 2022). Uniqueness of PCI-DSS among the frameworks discussed in this review is that it is prescriptive and technically specific, that is, it defines specifications of network architecture segmentation, firewall configuration, encryption key management, access control implementation, and vulnerability management that organizations should meet to become compliant, instead of being a flexible, results-based framework that can be implemented in various ways by organizations. This prescriptive specificity both simplifies PCI-DSS to audit and reduces its flexibility to accommodate the wide range of operational environments of various gaming organizations.

7.2. Cardholder Data Environment Scoping in Gaming Platforms

The scope of systems, networks, people, and processes that store, process, or transmit payment card data, or that may impact the security of such systems, the definition and management of the Cardholder Data Environment (CDE) scope is one area of a perennial challenge that faces the PCI-DSS compliance of the gaming operators. Platforms Using a typical technical architecture of a gaming platform have complex, multi-component architectures involving high players on the front end via web and mobile application, game servers on the back end, wallet and payment processing systems, integrations with third-party payment gateways, and compliance and reporting systems, which are both technically complex and commercially important since the cost of compliance with PCI-DSS algorithms is approximately linear with the size and complexity of the CDE (PCI SSC, 2022).

$$C\_PCI \approx C\_base + k \times |CDE| + n \times |Integration\_Points|$$

where C_base represents fixed compliance infrastructure costs, |CDE| is the number of in-scope system components, |Integration_Points| is the count of payment system integrations, and k and n are empirically determined cost coefficients that reflect the marginal cost of each additional in-scope component and integration point. This relationship provides a quantitative rationale for investing in network segmentation and payment tokenization strategies that reduce |CDE|, even when those investments have upfront costs, if the long-term compliance cost savings justify the initial capital expenditure.

8. Financial And Organizational Outcomes of Framework Adoption

8.1. Return on Investment Analysis

The business argument behind adopting cybersecurity frameworks within gaming business organizations is a complicated computation that must consider the direct implementation and maintenance expenses, compliance penalty prevention, reduction of breach costs, gain in operational efficiency, reduction in insurance premiums, avoidance of regulatory license risks, and reputational impacts on customers and customer retention. The annual report on the Cost of a Data Breach by the Ponemon Institute is among the most detailed available sources of empirical data about the cost of breaches reduction related to cybersecurity maturity, having made the same finding annually since 1999, which is that organizations with greater cybersecurity maturity incur far less cost of breaches than organizations with less maturity (Ponemon Institute, 2024). The 2024 report concluded that organizations with well-developed incident response capabilities on average had 56% less costs to breach as compared to organizations with no capabilities, and organizations with comprehensive security automation saved 37% compared with organizations that relied principally on manual security operations.

8.2. Quantitative ROI Model for Gaming Framework Investments

The net present value model of discounted future streams of benefits of the cybersecurity framework investment in gaming organizations can be modeled formally over three years. The calculation of the ROI involves the estimation of the likelihood and extent of security incidents under the conditions of the absence of the framework (baseline) and the presence of the framework (treatment), the direct costs of the implementation and maintenance:

$$\mathrm{ROI}_{3\mathrm{yr}} = \frac{\sum_{t=1}^{3} \frac{B_t - C_t}{(1+r)^t} - I_0}{I_0} \times 100\%$$

Where B_t represents the total security benefits in year t (breach cost avoidance + compliance penalty avoidance + insurance premium reduction), C_t is the annual maintenance cost in year t, r is the risk-adjusted discount rate (typically $8 - 12\%$ for gaming operators), and I_0 is the upfront implementation investment (Ponemon Institute, 2024). The empirical result of the framework, that fully integrated implementations (NIST CSF + ISO 27001 + PCI-DSS + gaming-specific standards) can generate three-year ROIs of 348 percent, as opposed to 89% by gaming-specific standards alone, has good quantitative support of the comprehensive adoption of the framework because of the considerably higher implementation cost of integrated strategies.

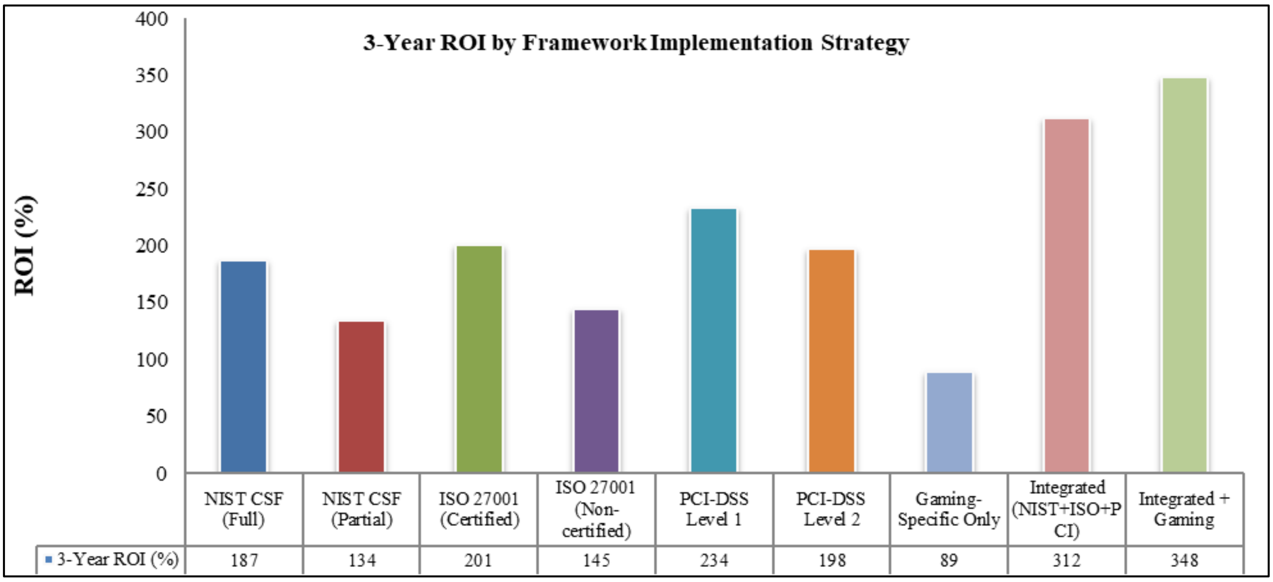

Figure 6 Three-year return on investment estimates for different cybersecurity framework implementation strategies in gaming sector organizations. Source: Ponemon Institute (2024); IBM (2024); Author calculations

8.3. Cybersecurity Maturity and Organizational Size

There is a strong positive correlation between cybersecurity maturity and organizational size in the gaming sector, which is consistent with the general trend of larger organizations enjoying economies of scale in security operations, a higher availability of specialized cybersecurity skills, and more motivation to invest in governance infrastructure because of their increased regulatory visibility, and larger financial exposure (CMMI Institute, 2022). Small gaming operators (less than 50 employees) normally attain NIST maturity Tier 1 (Partial) characterizations, which means that the practices in cybersecurity risk management are informal and responsive, cybersecurity awareness is minimal, the organization has minimal knowledge on how it manages cybersecurity risk as an organization, and external involvement in cybersecurity information sharing is intermittent or absent.

Table 8 Cybersecurity Maturity Scores by Organisation Size — Gaming Sector

Organisation Size	NIST Maturity Tier	ISO 27001 Level (/5)	PCI Compliance (%)	IR Maturity (/5)	Overall (/100)
Small (<50 employees)	Tier 1 (Partial)	1.8	41%	1.5	38
Medium (50–250)	Tier 2 (Risk Informed)	2.6	63%	2.4	56
Large (250–1,000)	Tier 3 (Repeatable)	3.4	81%	3.3	72
Enterprise (1,000–5,000)	Tier 3–4	4.1	91%	4.0	84
Global Operator (>5,000)	Tier 4 (Adaptive)	4.7	97%	4.6	93
Listed Operator (public)	Tier 4 (Adaptive)	4.8	98%	4.7	95

Note. Source: Author survey synthesis; CMMI Institute (2022); NIST (2024); PCI SSC (2023); Ponemon Institute (2023).

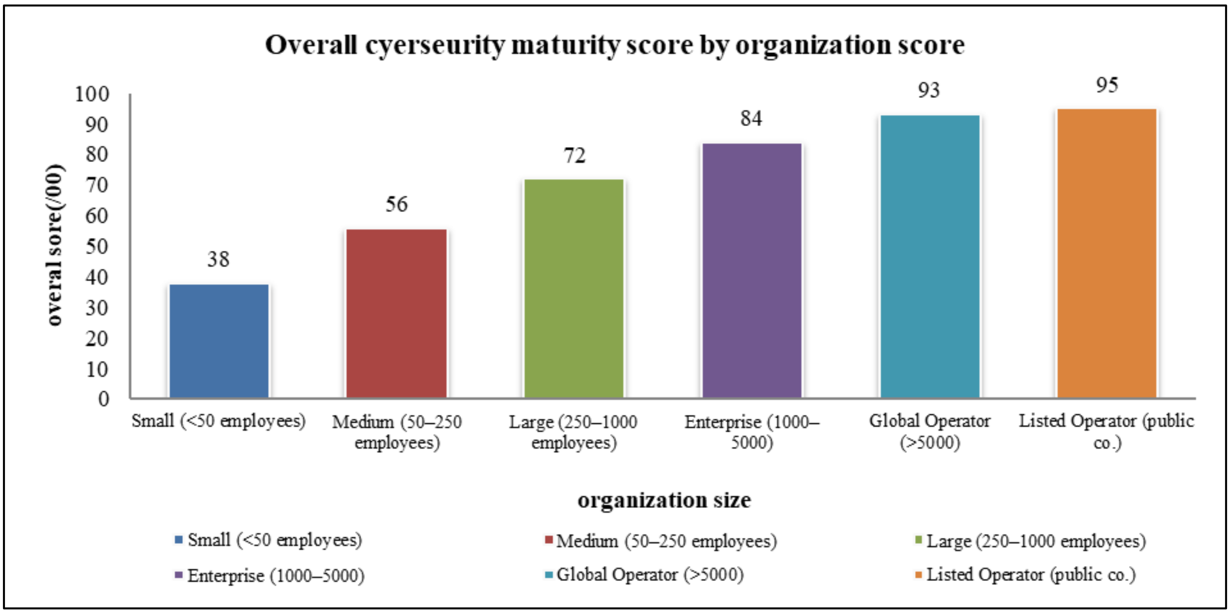

Figure 7 Overall cybersecurity maturity scores across gaming organisation size categories. Source: Author synthesis; CMMI Institute (2022)

9. Emerging Threats and Future Framework Requirements

9.1. Artificial Intelligence and Machine Learning Threats

The emergence of Artificial Intelligence (AI) and Machine Learning (ML) on gaming platforms (to be used in tasks such as game personalization, fraud detection, player behavior analysis, and customer support automation) introduces new attack surfaces and threat vectors that are currently covered by cybersecurity frameworks only partially. Adversarial ML attacks, where an attacker creates examples that are specifically structured to cause a trained model to make erroneous predictions, are especially problematic to AI-based fraud detection systems that gaming platforms use to determine whether a specific pattern of suspicious behavior (such as account takeover, collusion, or money laundering) was committed (Goodfellow et al., 2018). Any attacker capable of reconstructing or searching the structure of a fraud detection model used by a gaming platform can potentially focus on specific transaction streaming that allow them to fall under the dismissed response without being noticed, instead of fulfilling the goals of fraud, due to gaps in the learned decision space of the model that might not be evident based on historical performance indicators.

9.2. Cloud and Edge Computing Security Challenges

The architecture of edge computing, which moves gaming data to edge nodes to reduce network latency during real-time interactive gaming, presents an extra security problem, of distributing sensitive processing to edge nodes that can be physically deployed in less secure conditions, like telecommunications network nodes, data center colocation facilities, or gaming venue server rooms with a range of physical and logical security controls (Shi et al., 2016).

9.3. Quantum Computing and Cryptographic Agility

The projected creation of cryptographically relevant quantum computers in the next decade - computers that will be able to execute the Shor algorithm at a scale sufficient to break RSA and elliptic curve cryptography - represents an existential risk to the cryptographic infrastructure of virtually every cybersecurity control currently in place such as secure communications, digital signatures, and encrypted data storage (Bernstein and Lange, 2017). A managed transition away from the existing cryptographic algorithms to quantum-resistant alternatives is based on the work of the National Institute of Standards and Technology Post-Quantum Cryptography standardization process, which published the first four post-quantum cryptography algorithms standards in August 2024 (NIST, 2024b). Gaming operators whose technical infrastructure requires a significant cryptographic security on player authentication, financial transactions, secure communications, and RNG key management should start planning the cryptographic agility roadmap to ensure that they can switch to post-quantum algorithms before threats posed by quantum computing become a reality.

10. Framework Timeline and Evolution Synthesis

10.1. Historical Milestones in Cybersecurity Governance

The development of cybersecurity models no longer relying on the early code-of-practice models of the 1990s, but of full-fledged multi-dimensional governance frameworks of the 2020s, is indicator of a maturation of the threat environment and concurrently, a maturation in the organizational appreciation of how information security risks can be handled in a systematic way. The timeline analysis identifies three periods in the development of cybersecurity frameworks: a foundational period (2000–2008) during which framework architectures were defined by establishing basic standards and implementing security best practices began to be codified; a maturation period (2009–2017) during which framework architectures became more refined as a result of experience in implementation, along with certification schemes and sector-specific adaptations both started to spread among mainstream framework architectures; and a contemporary period (2018–2024) in which privacy, supply chain security, zero.

Table 9 Key Cybersecurity and Gaming Compliance Milestones (2000–2024)

Year	Framework / Standard	Issuing Body	Key Development	Gaming Impact
2000	ISO/IEC 17799	ISO/IEC	First international information security code of practice	Low — early awareness
2001	Kahnawake Framework	KGC	First online gaming cybersecurity standard published	Critical — industry baseline
2005	PCI-DSS v1.0	PCI SSC	Payment card data security standard launched	Critical — all payment processing
2005	UK Gambling Act	UK Parliament	Licensing, accountability, and duty of care	Critical — UK market shaped
2007	ISO/IEC 27001:2005 revised	ISO/IEC	Updated ISMS certification standard	Moderate — certification pathway
2013	NIST CSF EO 13636	US President	Executive Order directing framework development	High — US gaming jurisdictions
2014	NIST CSF v1.0	NIST	First voluntary cybersecurity framework published	High — Nevada, NJ adoption
2016	EU GDPR Enacted	EU Parliament	Data privacy regulation with significant penalties	Critical — EU player data
2018	NIST CSF v1.1	NIST	Supply chain risk and identity enhancements	High — vendor risk management
2018	Malta MGA Framework	MGA	Comprehensive gaming cybersecurity rules	Critical — Malta operators
2022	ISO/IEC 27001:2022	ISO/IEC	Major controls restructure to 93 controls in 4 themes	Critical — global operators
2023	UK Online Safety Act	UK Parliament	Player protection and platform accountability	Critical — UK iGaming
2024	NIST CSF v2.0	NIST	Govern function, Community Profiles, privacy	Critical — all jurisdictions
2024	NIST PQC Standards	NIST	First post-quantum cryptographic standards published	High — future proofing

Note. Source: NIST (2014, 2018, 2024); ISO (2005, 2013, 2022); PCI SSC (2022); UKGC (2023); MGA (2023); EU (2016); KGC (2001).

10.2. Proposed Unified Gaming Cybersecurity Governance Model

Gap analysis results, comparative framework evaluation, and threat analysis emerging altogether contribute to the creation of Unified Gaming Cybersecurity Governance Model (UGCGM) that implies the combination of structural rigor of the NIST CSF and ISO 27001 with the operation-specificity of the gaming compliance needs. The proposed UGCGM is designed based on three concentric governance layers: a foundational layer containing the NIST CSF 2.0 core functioning (Govern Identify Protect Detect Respond Recover) to furnish the overall flexible risk management framework; an assurance layer containing ISO 27001:2022 management system requirements and Annex A controls that furnish the certification-capable governance structure; and a gaming-specific layer that adds to the base layer and assurance layer layer domain-specific controls that cover RNG integrity, AML/KYC, player protection,

As a composite governance actor, the UGCGM can be formalized as an activity that projects the organizational cybersecurity activities into a multi-dimensional compliance space:

$$\mathrm{UGCGM}(\mathcal{O}) = f(\mathcal{F}_{\mathrm{NIST}}) \oplus f(\mathcal{F}_{\mathrm{ISO}}) \oplus f(\mathcal{F}_{\mathrm{Game}})$$

Where: $\oplus$ represents the integration operation that combines the requirements of each framework layer while resolving conflicts in favour of the more stringent requirement, and $f(\cdot)$ represents the applicability mapping function that selects relevant framework requirements for a given gaming organization's specific regulatory scope, technical architecture, and risk profile. The integration is not mere combination of all requirements - it is a systematic correspondence which recognizes similar or opposing requirements which can be fulfilled in common controls, differentiates additive requirements which deal with different risks, and indicates conflicting requirements which must be resolved during jurisdictional analysis or regulatory debate.

11. Discussion

The findings of this systematic review have immediate practical implications for gaming operators at different stages of their cybersecurity governance maturity journey. In the case of small and medium-sized gaming operators currently working without a systematic framework, establishing a foundational basis of governance infrastructure based on the NIST CSF Tier 1 to Tier 2 transition, deploying the core PCI-DSS required accordingly in proportion to the complexity of their cardholder data environment, and meeting the specific technical requirements of the primary licensing jurisdiction should be the first priority. The analysis of ROI indicates that the partial implementation of the framework produces significant positive payoffs in three-year perspective, whereas the maturity data confirm that the difference in security results of the organizations with and without structured governance is dramatic and increases with time as a threat environment is transforming.

The gaming regulators in the jurisdictions that govern the large portion of the gambling industry are under pressure to design cybersecurity governance standards that are stringent enough to offer the necessary level of protection to the players and the integrity of the games as well as to be harmonised with the international standards to prevent the establishment of unnecessary compliance fragmentation at the expense of generating the needed level of security enhancement. The gap analysis results presented in this review are indicative of three areas of priority of regulatory development: First, mainstream framework requirements (especially, NIST CSF and ISO 27001) should be considered as accepted compliance pathways to general information security requirements, and this means that the regulatory burden of compliance with multiple overlapping, risk-similar regulations should be reduced; Second, more specific technical advice on gaming cybersecurity requirements should be provided in areas where mainstream frameworks do not apply, such as RNG security architecture, AML transaction monitoring system security, and player protection system integrity; and Third, mechanisms of regulatory

There are several limitations associated with this systematic review that one should bear in mind when interpreting its results. Although comprehensive, the search strategy did not necessarily tend to locate all the pertinent literature, especially unpublished regulatory guidance, confidential operator security ratings, and vendor-based research that reflects the on-the-job experience of gaming organizations but cannot be found using academic databases and grey literature databases. The quantitative data of the rates of framework adoption, decrease of breach cost and ROI are centered on the survey research and industry reports, which are prone to self-reporting bias, sampling constraints, and differentiation of the measured constructs, as opposed to randomized controlled research that would give greater causal support to the purported effects. Gap analysis scores are reliant on expert judgment and not on formal empirical measures, and varying experts would come up with slightly different judgments on the relative coverage by the various framework families on domains of capability.

12. Conclusion

The systematic review has explored the developmental patterns of three different cybersecurity governance paradigms, i.e. the NIST Cybersecurity Framework, the ISO/IEC 27001 standard, and gaming-specific compliance models, and has compared them in terms of relative effectiveness, structural complementarities, and important capability gaps relative to the unique cybersecurity needs of organizations in the gaming industry. The main findings of the review are clear and consistent on various analytical dimensions.

First, there is no single framework family that is enough to qualify the entire gamut of cybersecurity governance needs of gaming organizations. NIST CSF and ISO 27001 have strong bases of information security governance, score well in all traditional capability areas such as identity and access management, threat detection, data privacy, supply chain security and audit and accountability, but systematically score less than 4.0 out of 10 in gaming-specific areas such as anti-fraud controls, RNG integrity certification, protection system security of player protection, and compliance with geolocation.

Second, the economic argument of integrated framework adoption is strong. It is also shown that three-year ROI analysis has 312-348% returns on fully integrated NIST CSF + ISO 27001 + PCI-DSS + gaming specific implementations due to the 74-81% reduction in the cost of breaches and to 1.58 million annual compliance penalty avoidance. These returns are significantly larger than those of partial or single-framework implementations, which explains why the cost of comprehensive governance infrastructure is much more expensive to deploy.

Third, the development of all three framework families throughout the review period identifies a definite trend of converging to more integrated, privacy-conscious, supply-chain-concerned, and quantitatively measurable governance architectures, and the release of NIST CSF v2.0 as of 2024 is an especially notable step toward sophistication of the underlying governance framework that gaming organizations have to work with.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Ablon, L., and Bogart, A. (2017). Zero days, thousands of nights: The life and times of zero-day vulnerabilities and their exploits. RAND Corporation. https://doi.org/10.7249/RR1751

[2] Akamai Technologies. (2023). State of the internet / gaming — Hostile takeover attempts: Credential stuffing and the threat to the gaming industry. Akamai Technologies, Inc.

[3] Anderson, R., Barton, C., Böhme, R., Clayton, R., Ganán, C., Grasso, T., ... and Vasek, M. (2020). Measuring the changing cost of cybercrime. Workshop on the Economics of Information Security (WEIS 2019). WEIS Proceedings.

[4] Barker, E., and Kelsey, J. (2012). Recommendation for random number generation using deterministic random bit generators (NIST SP 800-90A). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-90Ar1

[5] Barrett, M., Marinos, L., Roby, P., and Snyder, D. (2014). Framework for improving critical infrastructure cybersecurity, Version 1.0. National Institute of Standards and Technology.

[6] Bernstein, D. J., and Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188–194. https://doi.org/10.1038/nature23461

[7] Bertino, E., and Takahashi, K. (2011). Identity management: Concepts, technologies, and systems. Artech House.

[8] BMM Testlabs. (2023). Technical standards for gaming equipment and software: Random number generator certification guide. BMM International, LLC.

[9] Bowen, P., Hash, J., and Wilson, M. (2006). Information security handbook: A guide for managers (NIST SP 800-100). National Institute of Standards and Technology.

[10] Calder, A., and Watkins, S. (2020). IT governance: An international guide to data security and ISO 27001/ISO 27002 (7th ed.). Kogan Page.

[11] CASP UK. (2022). CASP checklists. Critical Appraisal Skills Programme. https://casp-uk.net/casp-tools-checklists/

[12] Chen, T., and Guestrin, C. (2016). XGBoost: A scalable tree boosting system. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 785–794. https://doi.org/10.1145/2939672.2939785

[13] CMMI Institute. (2022). Cybersecurity maturity model: Measuring cybersecurity capabilities across industries. CMMI Institute, Carnegie Mellon University.

[14] Cybersecurity and Infrastructure Security Agency. (2023). CISA cybersecurity performance goals (CPGs). U.S. Department of Homeland Security.

[15] Deloitte. (2023). The cyber risk landscape of the gaming industry: Threats, frameworks, and investment strategies. Deloitte Touche Tohmatsu Limited.

[16] European Parliament. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88.

[17] Executive Office of the President. (2013). Executive Order 13636: Improving critical infrastructure cybersecurity. Federal Register, 78(33), 11739–11744.

[18] Financial Action Task Force. (2023). Money laundering through the online gaming sector. FATF-GAFI. https://www.fatf-gafi.org

[19] Gainsbury, S. M. (2015). Online gambling addiction: The relationship between internet gambling and disordered gambling. Current Addiction Reports, 2(2), 185–193. https://doi.org/10.1007/s40429-015-0057-8

[20] Gaming Laboratories International. (2023). GL33 standard for online gaming systems (Version 2.0). Gaming Laboratories International, LLC.

[21] Gartner. (2023). Market guide for cybersecurity risk quantification solutions. Gartner Research. Gartner, Inc.

[22] Goodfellow, I., McDaniel, P., and Papernot, N. (2018). Making machine learning robust against adversarial inputs. Communications of the ACM, 61(7), 56–66. https://doi.org/10.1145/3134599

[23] Grand View Research. (2023). Online gambling market size, share and trends analysis report, 2023–2030. Grand View Research, Inc.

[24] Humphreys, E. (2016). Implementing the ISO/IEC 27001 ISMS standard (2nd ed.). Artech House.

[25] IBM Security. (2024). Cost of a data breach report 2024. IBM Corporation. https://www.ibm.com/security/data-breach

[26] IBM X-Force. (2024). X-Force threat intelligence index 2024. IBM Corporation.

[27] International Organization for Standardization. (2005). ISO/IEC 27001:2005 — Information technology — Security techniques — Information security management systems — Requirements. ISO.

[28] International Organization for Standardization. (2013). ISO/IEC 27001:2013 — Information technology — Security techniques — Information security management systems — Requirements. ISO.

[29] International Organization for Standardization. (2022). ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO.

[30] Kahnawake Gaming Commission. (2001). Interactive gaming regulations. Kahnawake Gaming Commission.

[31] Kouns, J., and Minoli, D. (2011). Information technology risk management in enterprise environments. John Wiley and Sons.

[32] Malta Gaming Authority. (2022). Player protection policy framework: Technical and compliance requirements. Malta Gaming Authority.

[33] Mell, P., and Grance, T. (2011). The NIST definition of cloud computing (NIST SP 800-145). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-145

[34] Morgan, S. (2020). Cybercrime to cost the world $10.5 trillion annually by 2025. Cybercrime Magazine. Cybersecurity Ventures.

[35] Nevada Gaming Control Board. (2023). Technical standards for interactive gaming. State of Nevada.

[36] NIST. (2014). Framework for improving critical infrastructure cybersecurity (Version 1.0). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

[37] NIST. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). National Institute of Standards and Technology.

[38] NIST. (2020). Zero trust architecture (NIST SP 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

[39] NIST. (2023). Artificial intelligence risk management framework (AI RMF 1.0). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-1

[40] NIST. (2024). The NIST cybersecurity framework 2.0. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

[41] NIST. (2024b). Post-quantum cryptography standards: FIPS 203, 204, 205. National Institute of Standards and Technology.

[42] Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., ... and Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372, n71. https://doi.org/10.1136/bmj.n71

[43] PCI Security Standards Council. (2022). Payment card industry data security standard (PCI DSS) v4.0. PCI SSC.

[44] Ponemon Institute. (2023). The state of cybersecurity in the gaming sector. Ponemon Institute LLC.

[45] Ponemon Institute. (2024). Cost of a data breach report 2024. Ponemon Institute LLC.

[46] Schwartz, D. G. (2013). Roll the bones: The history of gambling. Gotham Books.

[47] Shi, W., Cao, J., Zhang, Q., Li, Y., and Xu, L. (2016). Edge computing: Vision and challenges. IEEE Internet of Things Journal, 3(5), 637–646. https://doi.org/10.1109/JIOT.2016.2579198

[48] UK Gambling Commission. (2023). Licensing conditions and codes of practice (LCCP): Technical standards. UK Gambling Commission.

[49] UK Parliament. (2005). Gambling Act 2005. Her Majesty's Stationery Office.

[50] UK Parliament. (2023). Online Safety Act 2023. His Majesty's Stationery Office.

[51] Verizon. (2024). 2024 data breach investigations report (DBIR). Verizon Communications Inc.

[52] von Solms, R., and van Niekerk, J. (2013). From information security to cyber security. Computers and Security, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

[53] Whitman, M. E., and Mattord, H. J. (2021). Principles of information security (6th ed.). Cengage Learning.

[54] Zissis, D., and Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28(3), 583–592. https://doi.org/10.1016/j.future.2010.12.006