ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov619

Framework of Assessing Cybersecurity Maturity in Yemen Higher Education Institutions

Dr. Muneer Abduallh Saeed Hazaa[1]; Ali Mohammed Ali Al-Aomari[2]

[1]Associate Professor: Faculty of Computer and Information Systems –Thamar University, Thamar, Yemen
[2]Research Scholar: Network, Yemen Academy for Graduate Studies, Yemen, Sanaa

Publication Date: 2025/11/28

Abstract: The accelerating digital transformation of higher education has expanded institutions' exposure to cyber threats, a challenge that is particularly acute in resource-constrained settings where budgets, regulatory guidance, and security awareness remain limited. While international frameworks such as ISO/IEC 27001 and the NIST Cybersecurity Framework (CSF) are robust, their complexity, cost, and limited contextual fit often hinder effective adoption in low-resource environments. This study introduces ISOGMAF—an Institutional Security Governance Maturity Assessment Framework tailored to Yemeni higher-education institutions (HEIs). ISOGMAF is developed through a multi-stage methodology that integrates international best practices, local regulatory considerations, and sector-specific requirements, translating controls into measurable components spanning 34 governance/control domains. The framework is empirically validated via a survey administered across Yemeni HEIs using a six-point Likert scale maturity instrument to rate and classify cybersecurity governance levels. Findings reveal substantive gaps across governance, awareness, and technical preparedness, yet indicate tangible potential for phased improvement guided by a context-aware, scalable roadmap. The contribution is twofold: (i) it operationalizes the localization of global cybersecurity frameworks for developing-country HEI contexts, and (ii) it provides an objective self-assessment mechanism that supports benchmarking and targeted enhancement of institutional cyber resilience.

Keywords: *ISOGMAF; Cybersecurity Governance; Maturity; Higher Education; ISO/IEC 27001; NIST CSF; Readiness; Yemen.*

How to Cite: Dr. Muneer Abduallh Saeed Hazaa; Ali Mohammed Ali Al-Aomari (2025) Framework of Assessing Cybersecurity Maturity in Yemen Higher Education Institutions. *International Journal of Innovative Science and Research Technology*, 10(11), 1735-1756. https://doi.org/10.38124/ijisrt/25nov619

I. INTRODUCTION

Over the past decade, universities have adopted cloud services, online learning platforms, research data infrastructures, and campus-wide connectivity to improve access and performance. These developments have simultaneously broadened the attack surface and intensified the urgency of safeguarding critical information assets [1]–[2]. The core challenge is to balance the openness inherent to academic environments—essential for knowledge exchange and innovation—with the rigor required for effective cybersecurity governance and compliance [2], [3]. The problem is more pronounced in developing countries, where incidents are comparatively more frequent due to constrained resources, uneven awareness, and heterogeneous institutional capacities [4], [5]. In practice, cybersecurity maturity in HEIs reflects the interaction of technology, people, and organizational processes, yet many assessments remain qualitative, limiting consistent and comparable measurement across institutions [5], [6].

The higher-education context is structurally distinctive. Universities must protect sensitive assets—student records, research data, and administrative systems—while preserving open access for teaching and research [13], [14], [15]. Although Information Security Management Systems (ISMS) and global regulations/guidelines (e.g., GDPR, NIST) offer useful reference points, adoption barriers persist in low-resource HEIs due to complexity, cost, and process misalignment [5], [9]. Cross-institutional discrepancies in policy and control implementation signal a lack of common baselines and shared metrics, a pattern also reflected in the broader cybersecurity and cyber-insurance literature [11]–[17].

In Yemen, these hurdles are amplified by infrastructural limitations, gaps in security awareness and training, and the absence of comprehensive national guidance and shared terminology for security practices. As a result, coordinated incident response is weakened and the maturation of a robust security culture is impeded [11], [13]. This underscores the need for a unified, adaptable maturity framework designed for Yemeni HEIs—one that (a) enables systematic self-assessment of the current state, (b) identifies gaps relative to international good practice, and (c) supports prioritized, evidence-based improvement under resource constraints.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov619

➢ *Research Objectives. Building on this Need, the Paper Pursues Four Objectives:*

- RO(1): Define the essential components of an effective cybersecurity governance maturity framework tailored to higher education.
- RO(2): Assess the current state of cybersecurity across Yemeni HEIs, identifying gaps in policies, infrastructure, and practices.
- RO(3): Examine adoption barriers in resource-constrained environments and propose practical strategies to overcome them.
- RO(4): Evaluate alignment with international best practices and provide actionable recommendations for improvement.

- *Contribution*

The paper presents ISOGMAF, a context-aware maturity framework that harmonizes ISO/IEC 27001 and NIST CSF requirements with local regulatory considerations and HEI operational realities. The framework translates abstract controls into measurable elements across 34 domains, and is implemented via a six-point Likert instrument to support objective scoring, benchmarking, and phased capability development. By codifying a localization pathway from global standards to a developing-country HEI context, the study offers both a replicable methodology and a practical tool for enhancing cyber readiness and resilience.

II. LITERATURE REVIEW

➢ *Concepts of Cybersecurity Maturity in the Higher Education Context*

Cybersecurity maturity models are defined as staged approaches that transform security from disparate activities into a measurable governance system, through ascending levels that determine where the institution stands and what must be done to move to the next level [6], [16]. In universities, the picture becomes more complex for four interrelated reasons: (1) academic openness and the multiplicity of users (students/researchers/partners); (2) heterogeneity of capabilities across colleges and centers; (3) the dynamism of digital services (e-learning, cloud, research data); and (4) balancing the sensitivity between protecting intellectual assets and the requirements of open access. Therefore, sound maturity modeling requires blending three interrelated dimensions: governance (policies, roles, compliance), technology/operations (controls, engineering, incident management), and the human/awareness element (culture, training, behavior); and turning them into quantitative indicators and phased improvement bundles that facilitate adoption in resource-constrained environments. Here, the role emerges of standardized self-assessment tools and evidence lists to stabilize judgment and reduce variance among assessors, so that measurement serves benchmarking and decision-making.

➢ *General Global Reference Frameworks*

Global frameworks constitute an indispensable knowledge and practical base, but their usefulness in HEIs comes from adaptation rather than literal transfer. Most notably:

- ISO/IEC 27001: The cornerstone of ISMS via the PDCA cycle, evolving from 2005 and 2013 to 2022, which introduced 93 controls grouped into four themes (Organizational/People/Physical/Technological), with additions to address emerging risks (cloud/zero-day) [9], [18], [41]. Its strength lies in the comprehensive governance framework, and its challenge lies in cost and complexity in resource-limited environments.
- NIST CSF: Five core functions (Identify–Protect–Detect–Respond–Recover) form a flexible "common language" for sectoral adaptation [6], [24]. Its weakest point for HEIs is the absence of an embedded scoring system; a complementary maturity tool is therefore required for consistent measurement.
- COBIT: Goes beyond security to IT governance and management with 34 processes and six maturity levels (0–5) [42]. It provides a strong enterprise framework, but its complexity and linkage to large structures reduce its suitability for resource-poor universities [9].
- Supporting standards/references: ITIL, C2M2, PCI DSS, GDPR, CMMI, DSPT, BISM [9], [37], [34]. They complement gaps (services, readiness, privacy, process improvement) and frame compliance.

These frameworks provide the vocabulary of governance, lists of controls, and compliance boundaries, but they do not automatically yield a unified quantitative maturity metric suitable for universities with disparate capabilities. Accordingly, the HEI context—especially in developing countries—needs an adapted framework that links these foundations to a scoring/level mechanism and practical measurement evidence.

➢ *Adoption Challenges in Resource-Constrained Environments*

The literature shows that applying global frameworks in developing-country universities runs into recurring obstacles: the cost of certification and implementation [16], [18]; the shortage of technical and managerial competencies [19]; academic decentralization that complicates policy unification [6], [28]; weak technical infrastructures and monitoring/response tools [38]; and the absence of a unified national framework that defines responsibilities and guides compliance [38], [39]. In practice, this results in partial/unsustainable implementation or a gap between "paper policies" and "operational practice"—which undermines standard consistency and clouds benchmarking and improvement planning.

➢ *The State of Cybersecurity in Yemeni Higher-Education Institutions*

Higher education in Yemen is experiencing rapid digital expansion (internet and mobile), without a parallel institutional maturation in governance and policies. This has revealed a clear human-capital gap between rising demand for cybersecurity specialists and weak qualified output; estimates indicate that about 82% of entities require cybersecurity staff, while the limited number of qualified graduates drives 92% of

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov619

institutions to rely on external recruitment to fill the gap [40]. Institutional fragility is evident in the absence of dedicated security units or incident response teams, and in the persistence of outdated curricula detached from market needs [3].

Despite official initiatives (the 2021 Cybersecurity Conference and the 2022 Information Security Policy Guide/Decision 166), practical impact remains limited and has not risen to the level of systematic improvement in governance and response capabilities across Yemeni universities [40]. Consequently, there is a need for a local maturity tool that provides HEIs with a common language for policies and controls and a unified quantitative metric for staged diagnosis and improvement.

As the subsequent table (1) shows, an analytical summary of 28 studies on cybersecurity maturity models—their methodologies, scopes, and criteria—confirms the limited transferability of those models to the Yemeni context, reinforcing the rationale for developing a localized approach that responds to local regulatory and structural constraints [40].

- *Specialized Higher-Education Frameworks and Supporting International Comparisons*

The literature indicates that closing the "contextual fit" gap in universities requires shifting from the generality of global frameworks to sector-localized models that combine structured self-assessment with a staged improvement roadmap. In this vein, the HCYMAF in the United Kingdom stands out as a self-assessment tool that enables higher-education institutions to benchmark against best practices and align with privacy and compliance frameworks (GDPR, PCI DSS, DSPT) [6], [28]. HCYMAF builds on CMMI logic and offers a graduated structure across three interrelated functional areas—Identify, Protect & Detect, and Respond & Recover—and includes 15 requirements used for diagnosis and as a roadmap to raise institutional resilience. Although it originated in the UK, its structural flexibility allows adaptation in developing environments facing similar resource and governance constraints.

With a similar objective in a different context, SCMAF offers a Saudi-tailored framework that integrates NIST CSF, ISO/IEC 27001, and national compliance requirements, with a clear focus on security governance, awareness building, and resource allocation [28]. Alongside these two models, European/US schemes—such as ATC, eMM [31], and ICMM [33]—offer approaches that assess digital and institutional infrastructures under specific legislative contexts; in the United States many of them are tied to NIST and FERPA/HIPAA, while GDPR provides the governing legal foundation in Europe [4].

Additional specialized works and applied studies across Europe, Asia, and Africa (Gerl et al.; Makupi & Karume; Bondoc & Malawit; Bass; Suwito et al.; Aedah & Hoga; Ismail et al.; Appuhamilage & Rathnayake; De Ramos; Dwivedi & Vig; Li et al.; Yaokumah & Dawson; Al-Ghamdi et al.; Bilge et al.; Boughzala & De Vreede; etc.) collectively emphasize that maturity measurement must be evidence-based, context-sensitive, and capable of staged progression.

Section takeaway: shared principles (risk-based implementation, smart compliance, comparative measurement) require locally adaptable templates; hence the need for a localized framework such as ISOGMAF.

Table 1 Comparative Analysis Among the Related Cybersecurity Framework

Author/Year	Research Methodology	Scope	Adopted Standards
Gerl et al., 2021 [21]	Case Study Analysis	IT Governance in Higher Education	COBIT 2019
Proença & Borbinha, 2018 [35]	Maturity Model Analysis	Information Security Management Systems	ISO/IEC 27001
Singh & Alshammari, 2020 [22]	Institutional Theory Perspective	Cybersecurity Legal Framework in Saudi Arabia	Saudi local standards
Almuhammadi & Alsaleh, 2017 [23]	Framework Development	Information Security in Various Industries	NIST Cybersecurity Framework
Makupi & Masese, 2019 [18]	Cybersecurity Maturity Level Assessment Based on ISO 27001	Higher Education Institutions	ISO 27001
Bass, 2011 [24]	ICT Maturity Model Analysis	Ethiopian Educational Institutions	ICT Standards
Suwito et al., 2016 [25]	IT Security Evaluation	Higher Education Institutions	Cybersecurity Maturity Model
Ismail et al., 2010 [19]	Framework for Cybersecurity Management in Malaysian Academia	Malaysian Academic Environment	Local ISMS
Aliyu et al., 2020 [6]	Comprehensive Cybersecurity Maturity Framework	Higher Education Institutions in the UK	NIST, PCI DSS, GDPR, DSPT

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov619

Author/Year	Research Methodology	Scope	Adopted Standards
Aedah & Hoga, 2020 [16]	ISO 27001 Maturity Framework Analysis in Indonesian Higher Education	Indonesian Higher Education Institutions	ISO 27001:2013
Ajmi et al., 2019 [26]	Proposed Cybersecurity Framework	Cybersecurity in Saudi SMEs	Custom Framework
Al Hamed & Alenezi, 2016 [27]	Capability Analysis	Business Continuity and Disaster Recovery	ISO 22301
Aziz & Shahzad, 2015 [28]	Quality Measurement Analysis	ITES in Saudi Arabia	Custom ITES Quality Framework
Altameem, 2013 [29]	Experimental Investigation	E-Learning in Saudi Arabia	E-Learning Standards
Alnatheer & Nelson, 2009 [30]	Cultural Framework Proposal	Information Security Culture in Saudi Arabia	Custom Framework
Nsamba, 2019 [31]	Digital Maturity Level Analysis	Open Distance Learning University	Digital Maturity Framework
Marshall, 2010 [36]	Continuous Quality Improvement Framework	E-Learning Environments	E-Learning Maturity Model
Peñafiel et al., 2017 [32]	Maturity Model Application	E-Learning in Higher Education	E-Learning Standards
Rizun & Pańkowska, 2022 [1]	Maturity Model for Educational Allocation	Higher Education in Poland	Unspecified
Appuhamilage & Rathnayake, 2023 [2]	Gap Analysis in Cybersecurity Management Systems	Higher Education Institutions in Sri Lanka	ISO 27001
De Ramos & II, 2022 [4]	Cybersecurity Program for Philippine Higher Education	Philippine Higher Education Institutions	Unspecified
Almekhlafi, 2023 [9]	Balanced Information Security Maturity Model	General Security in Yemen	ISO/IEC 27001:2013 and O-ISM3
Alariqy, 2024	Blockchain Adoption in Higher Education	Higher Education in Yemen	TOE Framework, DOI Model
Almomani et al., 2021 [20]	Cybersecurity Maturity Assessment Framework	Saudi Higher Education	SA's CRF, ECC, NIST, PCI DSS, GDPR, DSPT
Li, Xiao & Zhang, 2023 [5]	Model to Analyze Factors Affecting Data Breaches	Higher Education Institutions	Unspecified
Bolanio, Paredes & II, 2021 [7]	Network Security Policies Based on ISO Standards	Higher Education Institutions	ISO 27001
Dwivedi & Vig, 2024 [8]	Blockchain Adoption in Higher Education	Higher Education in India	Unspecified
Kenneally et al., 2018 [12]	Cyber Risk Economics Capability Gap Strategy	Public and Private Institutions	Unspecified
Proposed ISOGMAF	Cybersecurity Maturity Assessment Framework for Yemeni Higher Education Institutions	Yemeni Higher Education Institutions	ye ISPGOT, ye GISGA, NIST, PCI DSS, GDPR, DSPT, ISO 2022

➢ *Gaps in Current Models and the Need for Localization*

Global interest in raising the security of higher-education institutions is increasing, but the applicability of common maturity models (ISO/IEC 27001, NIST CSF, CMMI) in developing contexts such as Yemen remains limited. They were designed to operate in advanced environments with available infrastructure, governance, financing, and competencies, making full adoption impractical without local tailoring [6][9][16]. These models also lack suitable mechanisms for gradual scaling that reflect varying institutional sizes, resources, and maturity levels, and their technical language hampers non-specialists, highlighting the

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov619

need for flexible, locally simplified frameworks that support staged improvement rather than a binary comply/not-comply logic [6][9]. Cost is a decisive challenge: training, external assessments, and continuous monitoring exceed Yemeni universities' capacities, calling for low-cost, context-appropriate models that balance rigor and practicality [6][16]. Purely technical frameworks also overlook human and organizational factors (weak governance, absent leadership accountability, scarcity of roles such as CISO, low awareness), resulting in scattered practices. Thus, operational management, training, and cultural transformation must be integrated alongside technical controls, with repeated quantitative self-assessment tools to track progress instead of reliance on external qualitative evaluations [6][9][22]. Finally, regulatory and legal opacity in Yemen—despite national initiatives and agreements—complicates compliance due to the absence of higher-education-specific guidance and weak practical enforcement [9][72].

III. METHODOLOGY

The study adopts a quantitative perspective within a design-science approach to develop, evaluate, and validate the ISOGMAF framework for measuring the maturity of information-security governance in Yemeni higher-education institutions. The methodology proceeds through three phases: conceptual formulation; 2) standards integration and cross-mapping between international and national references; 3) empirical verification using standardized inquiry methods and tools.

The framework was aligned with ISO/IEC 27001, the NIST CSF, higher-education–specific frameworks (e.g., HCYMAF), and relevant national regulations and policies. For cross-institutional comparison, a structured questionnaire was developed from the normative integration (34 main and sub-requirements) and administered to IT directors, security officers, and faculty members involved in the digital infrastructure. Descriptive and comparative analyses were employed, and responses used a six-point Likert scale (1–6) that is translated into a diagnostic Cybersecurity Maturity Index (CMI).

A. Framework Development Procedure

The methodology starts by constructing a "controls map" that pairs ISO/IEC 27001:2022 with the NIST CSF and national/sectoral references (ISPGOT, GISGA, and higher-education guidelines), and then proceeds through an interlinked three-stage process:

- *Stage 1 — Extraction and Initial Alignment:*

The methodology begins with a "controls map" combining ISO/IEC 27001:2022 and the NIST CSF with national/sectoral references (ISPGOT, GISGA, and higher-education guidelines). At this stage, controls suitable for the higher-education context are selected, redundancies are removed, and terminology is unified within a normative glossary. This is followed by contextual sorting with explicit decisions: retain what aligns with operations, resources, and national policies; adjust linguistically/procedurally/technically where needed (e.g., P14 Email Usage Policy and P10.3 Wireless Network Policy); and exclude items outside the context. This step yields a measurable, semantically encoded list of controls methodically linked to the five NIST functions, with documentation of each control's origin and alignment rationale.

It is noted that the frameworks used encompassed most of the requirements in ISO/IEC 27001:2013, particularly those suitable for the higher-education environment. The new additions in ISO/IEC 27001:2022—eleven (11) requirements as shown in Table (3.1)—were adopted because they address contemporary challenges. Local policies were also derived from ISO/IEC ISO/IEC 27001:2013 and ISO/IEC 27002:2013. HCYMAF was used as a basis for comparison, integration, and re-harmonization. Where direct matches were absent, a consensus-based approach mindful of the local context was adopted. Table (2) also shows the alignment mechanism between Yemeni security policies and the referenced regional and international frameworks. This integration contributed to establishing the proposed ISOGMAF framework, which aims to measure cybersecurity maturity in Yemeni higher-education institutions in line with local challenges and available resources.

Table 2 Shows Direct Integration and Mapping of Controls and Policies

ISOGMAF Requirement	**Standards Mapping**
ISOGMSF: I1 Components for securing the operational environment: usage policy, configuration management, and threat	HCYMAF:I1 GISGA:NO ISPGOT:NO ISO2022:A9.8,A5.7
ISOGMSF: I2 Requirements for administrative assessment	HCYMAF:I2 GISGA:NO ISPGOT:NO ISO2022:NO
ISOGMSF: I**3** Requirements for a risk management strategy**..**	HCYMAF: I3 GISGA:NO ISPGOT:NO ISO2022:NO

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov619

ISOGMAF Requirement	Standards Mapping
ISOGMSF: I4 Ensuring the security of the risk management chain: contracting requirements and policy for external parties.	HCYMAF: I4 GISGA:3 ISPGOT:NO ISO2022:NO
ISOGMSF: P5 Securing services: protection policies, processes, and procedures for data privacy.	HCYMAF:P5 GISGA:9 ISPGOT:NO ISO2022:NO
ISOGMSF: P5.1 Compliance with GDPR.	HCYMAF:P5.1 GISGA:NO ISPGOT:NO ISO2022:NO
ISOGMSF: P6 Identity management and asset control requirements	HCYMAF:P6 GISGA:6 ISPGOT:NO ISO2022:: NO
ISOGMSF: P**6**.1 Management of equipment preparation and administrative purposes.	HCYMAF: P6.1 GISGA:NO ISPGOT:NO ISO2022:NO
ISOGMSF: P**6.2** Securing access control: access control policy and access management policy	HCYMAF: P6.2 GISGA:8 ISPGOT:7 ISO2022:NO
ISOGMSF: P**6.3** Verification mechanism..	HCYMAF: P6.3 GISGA:NO ISPGOT:NO ISO2022: NO
ISOGMSF: P7 Physical and environmental security requirements and configuration management: organization, monitoring, and control of changes.	HCYMAF: P7 GISGA:1 ISPGOT:4 ISO2022: A7.4
ISOGMSF: P8 Application security requirements: policy for malicious code, virus, and device protection.	HCYMAF: P8 GISGA:15 ISPGOT:NO ISO2022:NO
ISOGMSF: P8.1 System security requirements..	HCYMAF: P.8.1 GISGA:NO ISPGOT:NO ISO2022:NO
ISOGMSF: P8.2 Application security requirements.	HCYMAF: P8.2 GISGA:NO ISPGOT:NO ISO2022:NO
ISOGMSF: P8.3 Securing application development: system and application development and maintenance policy	HCYMAF: P8.3 GISGA:10 ISPGOT:NO ISO2022: NO
ISOGMSF: P9 Data security: data security requirements, deletion, masking, and leakage prevention.	HCYMAF: P9 GISGA:NO ISPGOT:NO ISO2022: A8.10, A8.11, A8.12
ISOGMSF: P9.1 Data security through encryption: encryption policy and secure coding..	HCYMAF: P9.1 GISGA:14 ISPGOT:NO ISO2022: A8.28

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov619

ISOGMAF Requirement	Standards Mapping
ISOGMSF: P9.2 Information security: classification, disclosure, and information sensitivity policy..	HCYMAF: P9.2 GISGA:5 ISPGOT:5 ISO2022:
ISOGMSF: P10 Security technology measurement requirements.	HCYMAF: P10 GISGA:NO ISPGOT:NO ISO2022:NO
ISOGMSF: P10.1 Securing security technologies: monitoring and measurement policies, log management.	HCYMAF: P10.1 GISGA:11,19 ISPGOT:NO ISO2022: A8.16
ISOGMSF: P10.2 System segregation	HCYMAF: P10.2 GISGA:NO ISPGOT:NO ISO2022:NO
ISOGMSF: P10.3 Wireless access network use policy	HCYMAF:NO GISGA:NO ISPGOT:12 ISO2022:NO
ISOGMSF: P11 Ensuring security systems readiness and testing requirements: ICT readiness and continuity	HCYMAF: P11 GISGA:NO ISPGOT:NO ISO2022: A5.3
ISOGMSF: P**11.1** System evaluation	HCYMAF: P11.1 GISGA:NO ISPGOT:NO ISO2022:NO
ISOGMSF: P**11**.2 Compliance testing	HCYMAF: P11.2 GISGA:4 ISPGOT:NO ISO2022:NO
ISOGMSF: P**11.3** Experimental environment policy	HCYMAF:NO GISGA:NO ISPGOT:11 ISO2022:NO
ISOGMSF: P**11.5** Internet use security: internet use policy and web filtering.	HCYMAF:NO GISGA:NO ISPGOT:NO ISO2022:A5.23
ISOGMSF: P**11.4** Cloud services security	HCYMAF:NO GISGA:11 ISPGOT:3 ISO2022:A8.32
ISOGMSF: P12 Change management policy	HCYMAF: P12 GISGA:7 ISPGOT:NO ISO2022:NO
ISOGMSF: P13 Awareness and employment security policy	HCYMAF: P13 GISGA:2 ISPGOT:NO ISO2022:NO
ISOGMSF: P14 Email use policy	HCYMAF: NO GISGA:NO ISPGOT:2 ISO2022:NO

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov619

ISOGMAF Requirement	Standards Mapping
ISOGMSF: P15 Acceptable use of SharePoint policy	HCYMAF: NO GISGA:NO ISPGOT:13 ISO2022:NO
ISOGMSF: R16 Incident response management and emergency plan for information security incidents**.**	HCYMAF: R14 GISGA:17 ISPGOT:NO ISO2022:NO
ISOGMSF: R17 Ensuring business continuity and disaster recovery: requirements for continuity management, backup, and disaster recovery	HCYMAF: P15 GISGA:16,18 ISPGOT:9 ISO2022:

➢ *Stage 2 — Functional Classification and Local Adaptation:*

Controls are re-packaged by the NIST functions into a simplified classification of three operational groups to facilitate adoption in resource-constrained environments: I (Identify), P (Protect & Detect), and R (Respond & Recover). Adaptation is governed by the Yemeni context to ensure consistency with ISPGOT/GISGA; all descriptions are fully Arabized; Likert (1–6) anchors and evidence-guidance are provided to reduce subjectivity. A visual/tabular map shows the distribution of 34 requirements across the three groups with unified coding (e.g., ISOGMAF: I1, P14, P10.3, R16).

ISOGMAF controls were organized into five groups per NIST, but, in the proposed framework, were combined into three groups to present the framework more neatly and lightly, facilitating comprehension and traceability of security requirements across all stages, as follows:

- Group 1: Identify requirements (I) — numbering starts at (I1) and extends to (I…N). This group covers requirements for risk identification, understanding potential security threats, establishing key policies that help protect the educational institution, and determining whether such policies have been effectively implemented.
- Group 2: Detection and protection requirements (P) numbering starts from (P…n+1) to (P…N). This group focuses on how the institution protects against cyber threats and includes the policies and procedures used to secure the institution's IT systems and technological infrastructure.
- Group 3: Response and recovery requirements (R) — numbering starts from (R…n+1) to (R…N). This group covers policies defining how the institution responds to security breaches and how it recovers promptly to maintain continuity of academic and operational activities, as shown in Figure (1), which depicts the distribution of requirements across the three groups.

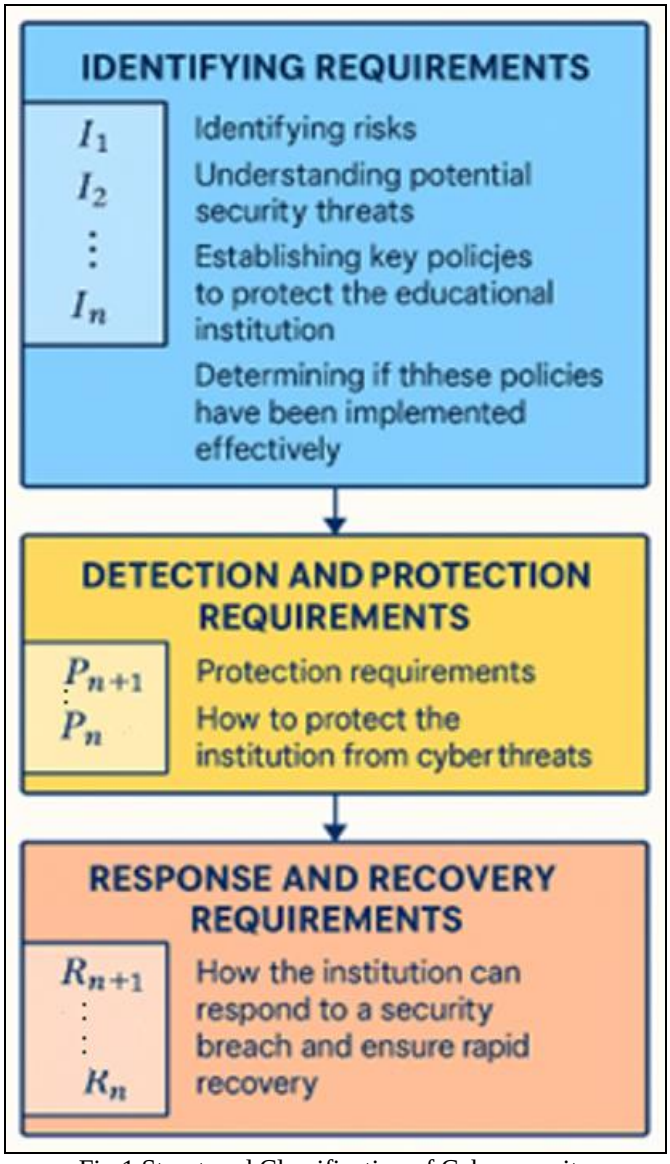

Fig 1 Structured Classification of Cybersecurity Requirements for Educational Institutions (Identification, Detection and Protection, Response and Recovery)

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov619

➢ *Stage 3 — Construction and Modeling*

The framework is completed in a hierarchical structure of Domains → Requirements → Controls comprising 34 measurable requirements, with a six-level maturity matrix (1 = Not Applied … 6 = Optimized) and differential weights for high-impact controls (e.g., R16), with equality assumed in the absence of a specific definition. Standard evidence is defined for each control (policies and review dates; training records; incident tickets and closure reports; monitoring/change logs) to ensure sufficiency and currency, while computation enables extracting indicators at the requirement, domain, and institutional levels with gap reports and priority-ordered recommendations.

For example, as shown in Table (3), one control associated with the Email Usage Policy (ISOGMAF: P14) was assessed through a set of detailed items designed to measure institutional compliance with email-security standards. The items include: use of the national domain (.ye), local data hosting, message encryption, prohibition of personal or commercial use of institutional email, and immediate reporting of device loss or intrusion attempts. The table measures these elements using a six-point Likert scale, with each level of compliance assigned a numerical score reflecting the extent of implementation. This assessment allows the institution to diagnose partial or full compliance and enables comparative analysis across different requirements or across institutions.

Table 3 Example of Assessment Items Under One Requirement (Email Usage Policy)

Requirement Questions (Email Usage Policy ISOGMSF: P14)	**Score**	**Likert Scale (0 to 5)**					
		Excellent "6"	**Very Good "5"**	**Good "4"**	**Moderate "3"**	**Weak "2"**	**Very Weak "1"**
Government entities dopting email communication must have their own email domain under (.ye), and the email system and its database must be hosted within the country.	4			√			
The email provided under the institutional domain (@ptc.gov.ye) is owned by the institution, and it reserves the right to suspend it temporarily or permanently if misused.	3				√		
Emails sent from the institutional account are considered official and the account holder is responsible for all correspondence.	1						√
It is prohibited to send highly confidential files or passwords through email, in compliance with the information classification and disclosure policy.	2					√	
Employees must not use institutional email for activities such as social media registration, sales, promotions, or personal use.	3				√		
Employees are responsible for any compromise of their institutional email account, regardless of the device or network used.	4			√			
Any loss of mobile phones or laptops containing institutional emails must be reported immediately to the information security department.	3				√		
Access to email records is restricted to the account owner and the information security officer, except for audit purposes.	2					√	
A clear mechanism must be in place for employees to report suspected email compromises to the security department promptly.	2					√	
Average Maturity Score:	2.7						

A pivotal component in this phase was the technical design of the maturity matrix, which constitutes the backbone of performance measurement within ISOGMAF. Drawing on staged maturity development as in models such as SSE-CMM and CMMI, a six-level matrix was built to evaluate each control across progressive stages of implementation and improvement [16]. Levels range from Level 1 (Incomplete process) to Level 6 (Optimized process), enabling institutions to recognize not only the existence of a control but also its integration, measurement, and continual improvement. The description of each maturity level was harmonized with the capabilities and constraints of higher-education institutions in resource-constrained environments such as Yemen. For example, moving from Level 3 (Managed) to Level 4 (Defined) requires not only implementing the control but also standardizing and documenting institutional procedures.

This example illustrates how adherence to controls can be translated into objective quantitative results that are subsequently used to determine the overall maturity level for each domain. To convert numerical averages into standardized maturity levels, a six-level maturity matrix was developed, as shown in Table (4). The matrix shows how the numerical average resulting from responses is translated into an equivalent maturity index ranging from Level (1)—no actual implementation—to Level (6), which reflects continual improvement and full integration of security practices.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov619

Table 4 Cybersecurity Maturity Levels and the Equivalent Maturity Index

Level	Description	Equivalent Maturity Index (Score Range)
1	Incomplete: The process is either not implemented or fails to achieve expected outcomes.	1.00 – 1.50
2	Initial: The process is implemented successfully and achieves its intended purpose.	1.51 – 2.50
3	Managed: The process is carried out systematically and its results are controlled.	2.51 – 3.50
4	Defined: The process follows formal guidelines and achieves consistent outcomes.	3.51 – 4.50
5	Quantitatively Managed: Process results are predictable based on predefined rules.	4.51 – 5.50
6	Optimized: Processes are regularly improved to achieve sustainable goals.	5.51 – 6.00

In line with the ISOGMAF development stages described above, Table (3) below present the final version of the framework after integrating methodological and design best practices.

This presentation shows how security requirements were classified into defined domains and distributed across the three core groups: Identify, Detect & Protect, and Respond & Recover, reflecting the framework's comprehensive philosophy of covering all stages of the cybersecurity lifecycle.

In this context, the visual figure highlights interactions among these domains and how each supports the others in building an integrated security system. The diagram shows the distribution of framework requirements across the circles associated with the reference model (ISOGMAF), with color coding for each group to ensure clear differentiation among assessment axes.

Table 5 ISOGMAF Security Requirements and Sub-Requirements Categorized by Domain in its Final Form

No.	Group	ISOGMAF Requirement	ISOGMAF SUB REQUIRMENT
	IDENTIFY	ISOGMAF :I1 Components of Operational Security: Usage Policy, Configuration Management, and Threat Information.	
		ISOGMAF :I2 Access Management Requirements.	
		ISOGMAF :I3 Risk Management Strategy Requirements.	
		ISOGMAF I4 Risk Chain Integrity: Contracting and External Party Policy	
	DETECT & PROTECT	ISOGMA P5 Service Security: Protection Policies, Operations, Procedures, and Data Privacy	ISOGMAF: P5.1 GDPR Compliance
		ISOGMAF: P6 Identity and Asset Control Requirements	ISOGMAF: P6.1 IT Equipment Management for Security and Administration ISOGMAF: P6.2 Secure Access Control: Access Control and Access Management Policy ISOGMAF: P6.3 Verification Mechanism
		ISOGMAF: P7 Physical and Environmental Security Monitoring and Configuration Management Requirements	
		ISOGMAF: P8 Application Security Requirements: Security Requirements and Policy for Protection Against Malware, Viruses, and Devices	ISOGMAF: P8.1 System Security Requirements ISOGMAF: P8.2 Application Security Requirements ISOGMAF P8.3 Securing Application Development: Security Requirements and Policy for System and Application Development
		ISOGMAF: P9 Data Security: Data Protection, Deletion, Concealment, and Prevention	ISOGMAF: P9.1 Data Encryption: Encryption and Secure Coding Policy ISOGMAF: P9.2 Information Security: Classification, Disclosure, and Sensitivity Policy
		ISOGMAF: P10 Security Technology Measurement Requirements: Network Service Security.	ISOGMAF: P10.1 Security Monitoring and Event Management ISOGMAF: P10.2 System Segregation ISOGMAF: P10.3 Wireless Network Access Policy

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov619

No.	Group	ISOGMAF Requirement	ISOGMAF SUB REQUIRMENT
		I SOGMSF: P11 Security System Readiness and Testing: Security System Requirements, IT Readiness, and Business Continuity	ISOGMAF: P11.1 Security Assessments The organization must conduct regular security assessments ISOGMAF: P11.2 Compliance Audits The organization must regularly verify compliance with the recognized regulations and standards in the Republic of Yemen ISOGMAF: P11.3 Experimental Environment Policy ISOGMAF: P11.4 Information Security for Cloud Services ISOGMAF: P11.5 Internet Security: Internet Usage Policy and Web Filtering
		ISOGMAF: P12 Change Management Policy	
		ISOGMAF: P13 Employee Security Awareness Policy The organization must ensure that employees are well-trained to confront security threats	
		ISOGMAF: P14 Email Usage Policy	
		ISOGMAF: P15 Acceptable Use Policy for SharePoint Platform	
	RESPOND & RECOVER	ISOGMAF: R16 Security Incident Response and Management: Security Incident Response Policy and Emergency Plan.	
		ISOGMAF: R17 Business Continuity and Disaster Recovery: Business Management, Recovery lanning, and Backup & Restoration	

This constitutes detailed documentation of ISOGMAF requirements, presenting each main requirement with a brief definition and its scope—Identify, Detect & Protect, or Respond & Recover. The table also includes sub-requirements linked to some main requirements, providing a higher degree of precision and flexibility in assessment by allowing examination of implementation particulars for each policy or procedure. This breakdown helps academic institutions align each element with operational capabilities and set phased implementation priorities.

B. Tool Development

A bilingual self-assessment instrument was developed within ISOGMAF comprising 113 indicators distributed across 34 requirements and using a six-point Likert scale (1–6). Items were organized by control impact (Low 1–2, Medium 3–4, High up to 5), and requirement identifiers (e.g., ISOGMAF: P14) were unified to facilitate traceability and analysis. The questionnaire is evidence-based and consistent with the five ISOGMAF domains—Identify, Detect, Protect, Respond, and Recover—featuring usability for resource-constrained environments and methodological rigor for reliable, actionable results.

The study population includes all accredited Yemeni higher-education institutions (public and private). A purposive sample of 120 participants (IT directors, information-security officers, system administrators, and digitally involved faculty) was used to ensure balanced managerial–technical coverage.

- *Instrument Distribution, Channels, and Collection Window:*

Offline mode via an Excel workbook with integrated formulas and export capability; secure online mode via Google/Microsoft Forms for centralized collection. Official institutional email and protected limited-circulation links were used. Collection lasted four weeks with two reminders and a formal support letter from the Ministry of Higher Education to enhance credibility, in addition to a technical support line for low-connectivity institutions.

- *Statistical Analysis:*

Processing was conducted using Microsoft Excel and IBM SPSS Statistics for cleaning, coding, and analysis. Descriptive analysis used means, standard deviations, frequencies, and percentages to describe sample characteristics and cybersecurity practices, with average performance evaluated across the five ISOGMAF domains.

C. Measurement and Indexing Model (CMI)

ISOGMAF's cybersecurity maturity assessment relies on a precise hierarchical coding methodology that enables tracing institutional performance from the micro level (individual requirements) to the macro level (overall institutional performance). This stepwise approach not only provides a holistic evaluation but also allows educational institutions to understand strengths and weaknesses in their security controls through detailed, extensible analysis. At the start of the assessment, each security requirement is treated as an independent entity measured via a number of items (one to five) according to the requirement's importance and impact. Each item is scored from 1 to 6 per the Likert scale, providing fine-grained discrimination among implementation levels. After collecting scores for items associated with a given requirement, an arithmetic mean is computed to represent that requirement's "maturity score," calculated as follows.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov619

$$Q_{ij} \sum_{j=1}^{n} \frac{1}{n} = R_i$$

R: Requirement score
Q_ij: Score of item j within requirement i
n: Number of items under the requirement

➢ *Example:*

"Identity and Asset Management" has 4 items scored as: 4, 5, 3, 4

R = (4 + 5 + 3 + 4) / 4 = 4.0

Once requirement scores are obtained, assessment proceeds to the domain level. Related requirements are grouped under five main domains—Identify, Detect and Protect, Respond and Recover—each representing a strategic pillar of institutional cybersecurity. A domain's final score is the mean of the constituent requirements' scores.

$$R_i \sum_{i=1}^{m} \frac{1}{m} = D_k$$

D: Domain score
R_i: Score of each requirement
m: Number of requirements

➢ *Example:*

"Protect" domain has 3 requirements scored: 4.0, 3.5, 2.5

D = (4.0 + 3.5 + 2.5) / 3 = 3.33

Finally, the overall institutional maturity index is derived by averaging the five domains' scores, after which the average is mapped to the nearest maturity level on a six-level scale from Level 1 (Not Applied) to Level 6 (Continuously Optimized). This final classification is used to characterize institutional readiness holistically and serves as a benchmark for cross-institutional comparisons in higher education.

$$D_K \sum_{k=1}^{k} \frac{1}{k} = M$$

M: Institutional maturity score
D_k: Score of each domain
K: Number of domains

➢ *Example:*

If domain scores are: 3.0, 3.33, 2.67

M = (3.0 + 3.33 + 2.67) / 3 = 3.0

The final result of the assessment indicates that the institution obtained an overall maturity score of 3.0 on the ISOGMAF scale. Under this scale, the score falls within Level 3: "Good — Defined," reflecting the presence of clear policies and procedures that have not yet been rolled out or implemented comprehensively. This indicates that the institution has begun adopting security controls and practices and has partially documented them, with initial implementation in some departments or units—a transitional stage toward more mature, integrated institutional application. The hierarchical model enables institutions to analyze performance in both detailed and comprehensive ways and supports cross-institutional comparison. Similar models have been adopted in the United Kingdom, the Kingdom of Saudi Arabia, and Sri Lanka to assess cybersecurity readiness in higher education [6][28][2].

D. Verification and Quality Assurance

To ensure the questionnaire's validity and reliability prior to deployment, a two-stage verification process was conducted: expert review and field piloting in the local research environment. The process aimed to examine content accuracy, cultural suitability, participant clarity, and consistency with international cybersecurity frameworks.

➢ *First: Expert Review*

The questionnaire was reviewed by specialists with academic and professional expertise in ISO/IEC 27001, the NIST CSF, and information-security governance in higher-education institutions. The review focused on:

- Accuracy and consistency of technical terminology.
- Alignment of each item with the corresponding ISOGMAF control indicator.
- Clarity of statements and absence of ambiguity or duplication.
- Structural soundness reflecting objectively ascending maturity levels.
- Suitability of the instrument for practical application in the Yemeni context.

To enhance diversity and credibility, reviewers included academics and practitioners from multiple universities and official institutions.

➢ *Second: Field Piloting*

A pilot version was administered to a limited sample of Yemeni higher-education institutions—IT directors, administrative officials, technical staff, and academics—allowing the instrument's interaction to be gauged at different organizational levels. Key indicators: language/terminology clarity, completion time, engagement and comprehension levels, and informal participant feedback. Outputs included:

- Technical content review: identify ambiguous terms → update and phrase per established literature.
- Structural consistency: detect duplication or weak linkage → reorder and renumber items within the five domains.
- Limited field trial: difficulty/length of some items → simplify phrasing and split compound items.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov619

- Response analysis: varied understanding of certain technical indicators → include selective illustrative examples.
- Final review: produce an integrated, user-friendly version → unify the instrument's visual format.

These steps yielded tangible improvements in content accuracy, structural coherence, and language clarity, producing a reliable final version of the ISOGMAF questionnaire that reduces bias and misinterpretation and conforms to methodological recommendations in the literature on cybersecurity-maturity assessment in higher education [2][1].

➢ *Third: Ethical Considerations*

The study obtained approval from the Research Ethics Committee at the Yemeni Academy for Graduate Studies. Participation was voluntary with informed consent (electronic/paper) clarifying objectives, participation nature, and the right to withdraw. Anonymity was observed by removing identifiers and replacing them with non-traceable codes, with encrypted storage and strong passwords, researcher-only access, and use restricted to academic purposes, consistent with ISO/IEC 27001 practices [28].

IV. FRAMEWORK DESIGN (ISOGMAF)

The study employs a cross-sectional survey design integrated with the design-science paradigm. This coupling brings together the construction of the ISOGMAF model on clear methodological foundations and its field testing in actual university environments, thereby enabling, at the same time, (1) development of the framework architecture and its controls and (2) estimation of maturity levels as they exist on the ground under universities' operational constraints.

To translate the framework into a practicable instrument, a self-assessment tool was developed consisting of 113 items covering 34 requirements, providing higher-education institutions with an independent mechanism to diagnose maturity level, identify gaps, and track progress periodically. The tool was designed to align with international best practices and local contextual demands.

A. Technical Aspects of the Design

ISOGMAF rests on technical foundations that structure the measurement process and ensure consistency and comparability of results through:

- Unified coding for items and requirements: Each item is assigned an alphanumeric identifier indicating its domain and sequence. The Identify (I) domain includes requirements such as I1 (Components of operational security); the Protect/Detect (P) domain includes, for example, P6 (Identity and asset management); and the Respond/Recover (R) domain includes R17 (Disaster recovery). This coding facilitates traceability and reporting.
- Predefined criticality weights: Relative weights are applied to certain control elements to reflect their impact, set in consultation with experts and aligned with ISO/IEC 27001 and the NIST CSF, as well as frameworks suitable for higher education such as HCYMAF/SCMAF [16][6][28].
- A six-point Likert scale (1–6): This converts qualitative responses into quantitative maturity indicators, where a score of (1) represents absence of implementation and (6) denotes fully documented, integrated implementation. This enables fine-grained discrimination among implementation levels.

This approach provides flexibility for institutions with varying levels of technical infrastructure and supports both online and offline assessment scenarios. Processing and analysis are managed via a client/server-logic model: local applications (desktop or browser-based) perform the initial computation of scores and means, after which results are transmitted to central repositories for visualization, analysis, and longitudinal tracking. The computation engine applies a complexity model of O(N×K), where N denotes the number of participating institutions and K the number of assessed controls, ensuring performance efficiency even when scaling the framework up to nationwide assessments. These technical foundations support the framework's capacity to serve not only as a maturity-assessment tool but also as a strategic cybersecurity-management instrument, enabling institutions to (identify maturity gaps – benchmark performance against peer institutions – align practices with – international standards such as ISO/IEC 27001 and the NIST CSF – track progress through periodic assessments).

B. Operational Workflow

➢ *Documenting the Institutional File (Context, Governance, Digital Footprint).*

- Institutional profile module. Figure (2) presents an interactive digital interface designed to record higher-education assessment information in an organized and clear manner. The interface is divided into three primary sections: institutional data, assessment-entity information, and assessor details. Each section contains carefully arranged input fields, including assessment date, institutional location, relevant department, email, phone number, and additional notes.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov619

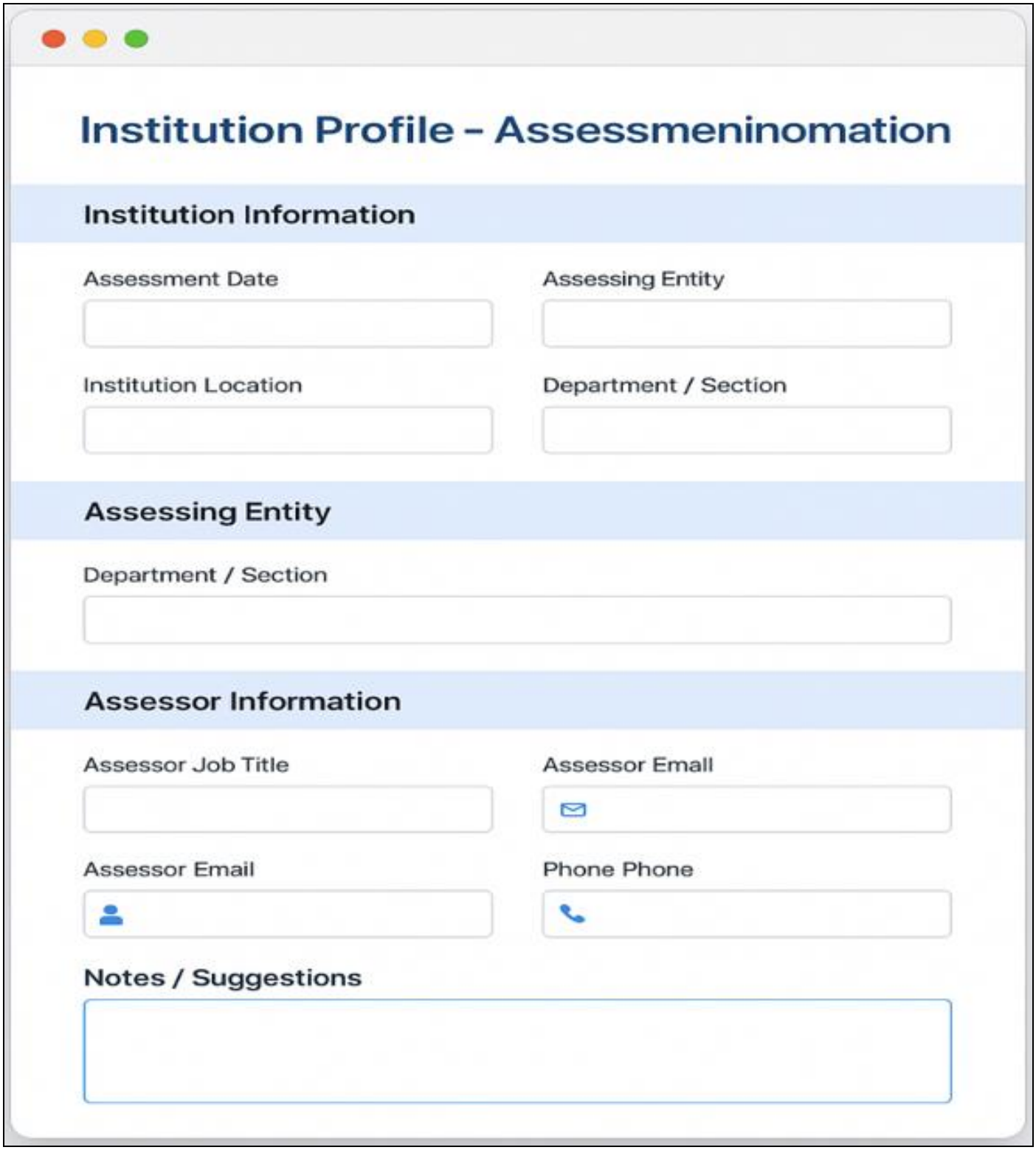

Fig 2 Institution Profile and Assessment Information Interface

- The tool provides flexible assessment-mode options, supporting both online assessment and offline data collection using structured Excel forms. This dual capability meets the needs of institutions with weak internet connectivity, ensuring inclusive and flexible application across urban and rural environments.
- The assessment interface classifies items by the core ISOGMAF domains and uses unified identifiers (e.g., P9.1 for data-encryption controls) to facilitate navigation and clearly link responses to framework requirements. Figure (3) displays three example interactive interfaces designed to assess cybersecurity controls within ISOGMAF.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov619

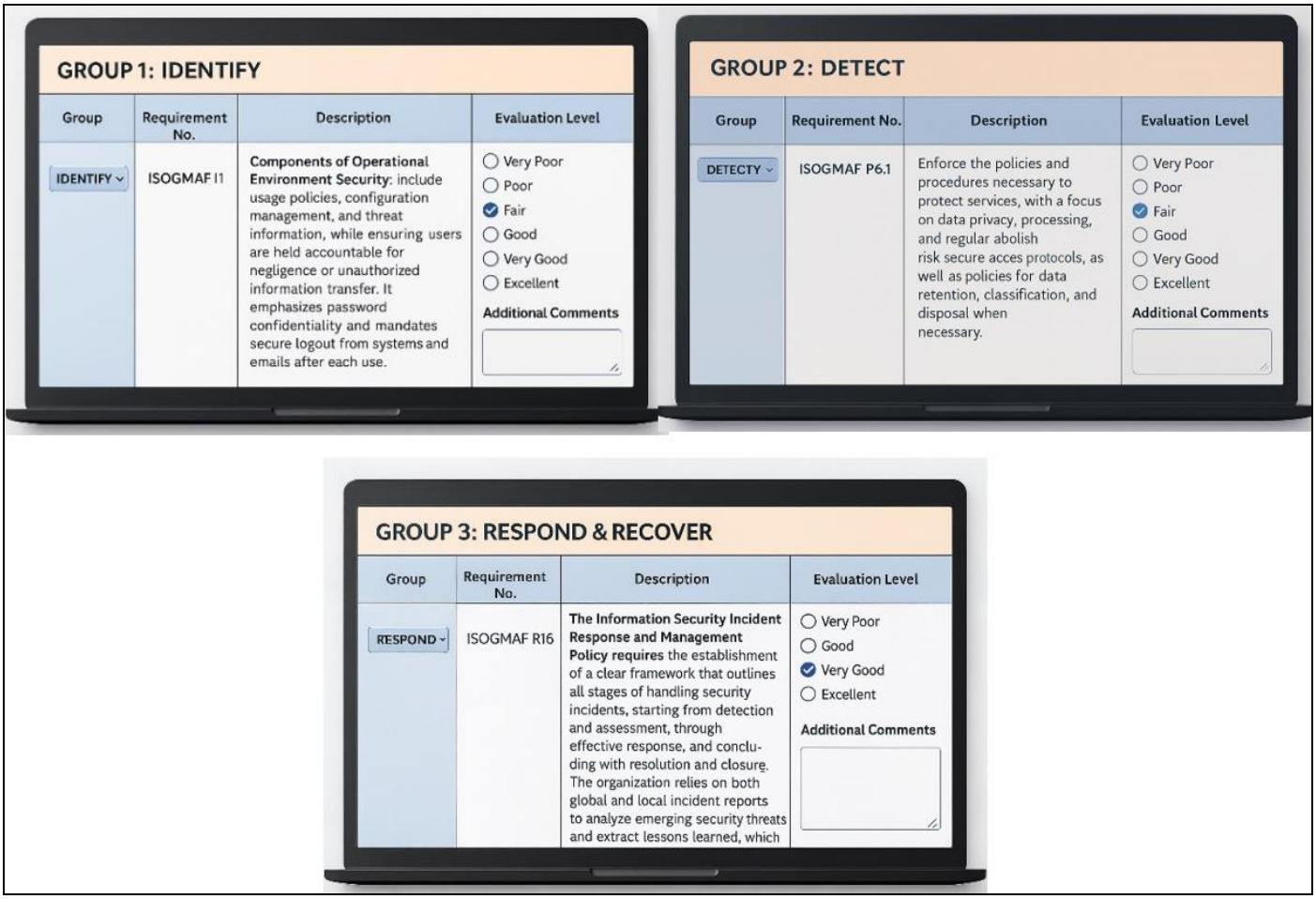

Fig 3 ISOGMAF Cybersecurity Assessment Interactive Interfaces

- *Regarding Tool Outputs, a Comprehensive Set of Visualization and Reporting Capabilities is Provided, Including:*

- Bar charts that display maturity levels across domains. Fig (4) shows a bar chart depicting maturity across three principal domains: Identify, Detect & Protect, and Respond & Recover. Each column represents a domain with distinct blue gradients, clearly showing differences in maturity levels, with Protect attaining the highest level. The title is prominent at the top and states the chart's purpose, with a simple, easy-to-read design;

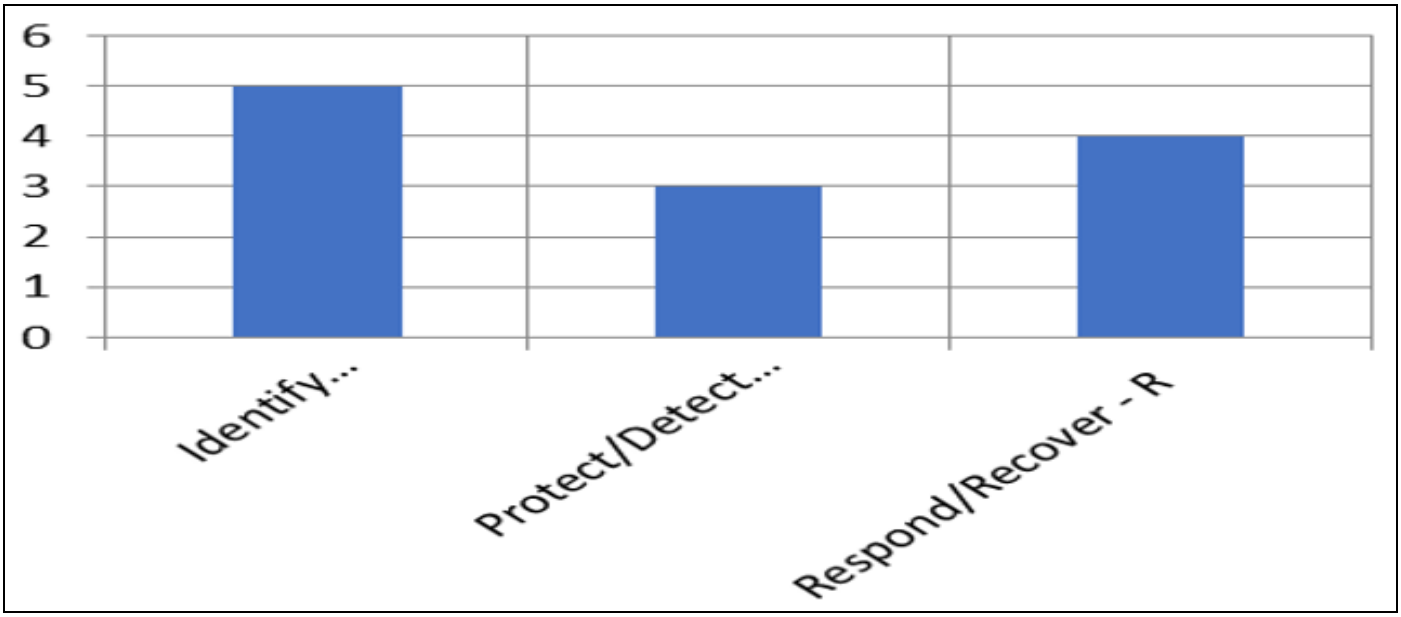

Fig 4 Maturity Levels Across Framework Domains

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov619

- Spider (radar) charts that illustrate sub-requirement performance. Fig (5) contains a circular radar chart exemplifying the performance of 17 principal ISOGMAF requirements distributed around the circumference. Performance appears as a transparent blue polygon extending along the axes to reflect maturity levels for each element.

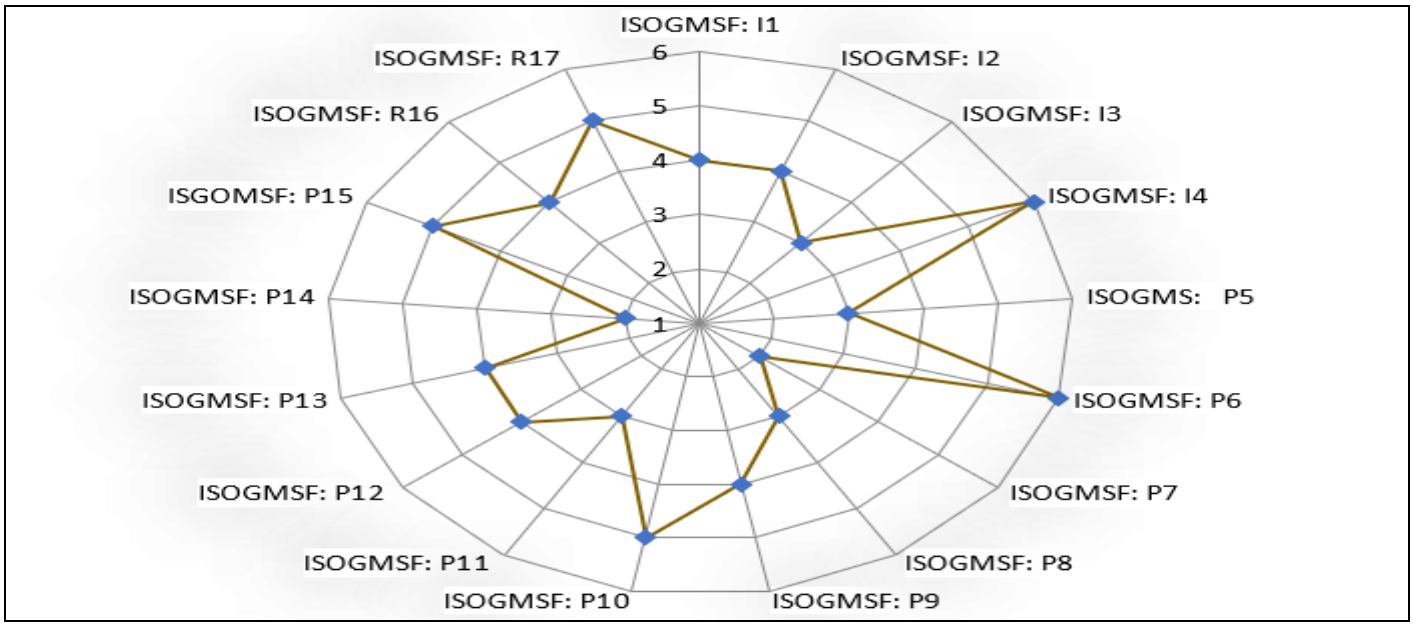

Fig 5 Requirement and Sub-Requirement Performance Radar Chart

Executive summary reports to support strategic decision-making and resource management. Fig (6) shows an executive-summary interface presenting the overall maturity level (2.3) with a green print button. Below it is a list of actionable recommendations for improving cybersecurity—such as developing a risk-management framework and enhancing user awareness. The final section describes system performance and explains the client/server architecture with O(N×K) complexity, demonstrating processing efficiency.

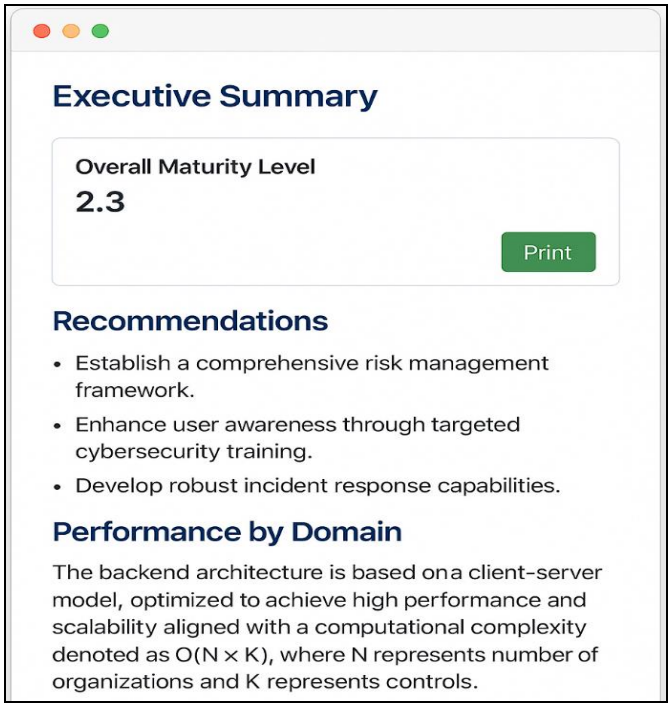

Fig 6 Executive Summary and Recommendations Report

By translating ISOGMAF into a practical, user-centered self-assessment system, this tool constitutes a core component supporting continuous cybersecurity improvement. It enables institutions to identify gaps, prioritize strategic investment, and demonstrate progress over time. In this way, the self-assessment tool helps bridge the gap between theoretical framework design and effective, real-world cybersecurity management, reinforcing a culture of proactive cybersecurity governance in Yemen's higher-education sector.

C. Use and Impact

Adopting this model delivers a set of strategic benefits for Yemeni higher-education institutions:

- Establishing a clear baseline for evaluating cybersecurity capabilities relative to peer institutions and prior performance.
- Supporting improvement priorities by pinpointing the weakest controls and domains.
- Aligning institutional practices with international standards such as ISO 27001 and the NIST Cybersecurity Framework.
- Providing objective data to justify funding requests, policy updates, and documentation of continuous-improvement efforts.

By combining quantitative measurement, visual analytics, and contextual assessment, ISOGMAF offers an integrated and flexible tool to support decision-making across academic-governance levels. This approach is a natural extension of prior efforts to develop the framework, laying a solid foundation for sustainable improvement and sound governance.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov619

D. Flowchart and Algorithm for the Assessment Tool

The ISOGMAF tool was developed to be domain-centric and flexible, guiding the user from entering institutional data to automatically generating results (scores, reports, and gaps). Fig (7) shows the workflow in five essential steps:

- Log in and enter the institutional profile.
- Load controls according to the selected domain.
- Respond using the six-point Likert scale (1–6).
- Compute maturity scores for each requirement, then for each domain, culminating in the institution-wide level.
- Issue a detailed report presenting maturity gaps in graphical form.

- *Execution options:* Download a template for manual assessment, use the interactive in-system version, or operate in offline mode. In all cases, the process follows the same assessment logic.

➢ *Assessment Logic (Flow/Algorithm):*

- Each requirement is presented to the user to determine whether it is met.
  - ✓ If not met: the tool proceeds directly to the reporting stage with current readiness scores.
  - ✓ If met: the user selects a readiness level from six levels (Very Weak, Weak, Acceptable, Good, Very Good, Excellent).

- After fixing the requirement's level, the tool automatically proceeds to the next requirement, while allowing manual navigation and confirmation.
- Upon completion of all requirements, the tool generates a final report containing readiness levels for each requirement, enabling management to analyze results and prioritize improvements, with an output format suitable for sharing and archiving.

This flow (Fig 7) aims to standardize procedures, enhance transparency, and ensure consistency with international best practices, while maintaining ease of use in low-connectivity environments.

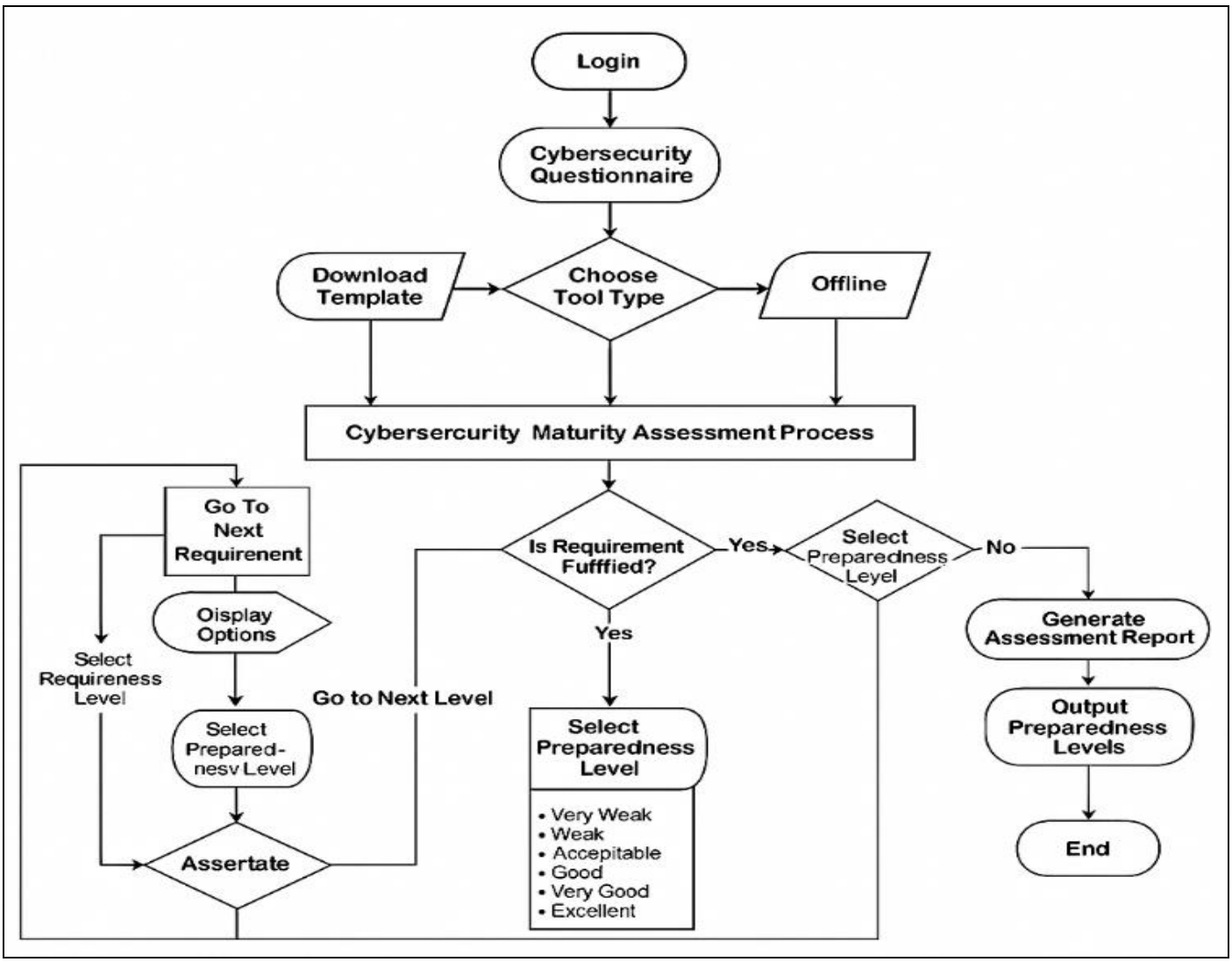

Fig 7 Cybersecurity Maturity Assessment Flowchart

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov619

Text heads organize the topics on a relational, hierarchical basis. For example, the paper title is the primary text head because all subsequent material relates and elaborates on this one topic. If there are two or more sub-topics, the next level head (uppercase Roman numerals) should be used and, conversely, if there are not at least two sub-topics, then no subheads should be introduced. Styles named "Heading 1," "Heading 2," "Heading 3," and "Heading 4" are prescribed.

V. RESULTS AND ANALYSIS (PUBLICATION-READY, REFEREED FORMULATION)

A. Sample Description

The characteristics of the participants (n=54) reveal a composition that permits a reliable reading of cybersecurity governance in higher-education institutions: the majority hold a Bachelor's degree (63.0%), followed by Master's (20.4%), then PhD (14.8%) and Diploma (1.9%). Functionally, leadership roles prevail (Director-General 33.3% and Department Director 33.3%; Heads of Departments 7.4%; Staff 25.9%). Experience is distributed as follows: less than 5 years (20.4%), 5–10 (35.2%), 10–15 (27.8%), and more than 15 (16.7%). Institutionally: universities (44.4%) and "others" including hybrid centers/entities (31.5%), with institutes (5.6%), academic entities (11.1%), and organizations (7.4%). By sector: private (35.2%), governmental (33.3%), and hybrid/other (31.5%).

B. Hierarchical Maturity Results

The assessment uses a six-point scale (1.00–6.00) and is built on data from 54 institutions within the ISOGMAF framework, with emphasis on the mean (M) and standard deviation (SD).

➢ *Stronger Indicators:*

- I2 (Supply chain/third party): M=4.10, SD=1.18
- P6 (Identity and asset management): M=4.05, SD=1.32.
- P14 (Email policy): M=3.94, SD=1.50

There were also good levels in P10 (M=3.74, SD=1.54), P11.4 (Cloud security: M=3.72, SD=1.42), and P6.2 (Access control: M=3.73, SD=1.30).

➢ *Weaker Indicators:*

- P6.1 (Equipment provisioning/management): M=3.24
- P8.2 (Application security): M=3.21
- P11.3 (Testing environment): M=3.26

Within Identify, I3 (Risk-management strategy) recorded the lowest relative mean, M=3.52.

➢ *Inter-Institutional Variance:*

High SD values in P15 (1.61), P14 (1.50), and P10 (1.54) indicate notable disparities in implementation. Overall, the picture reflects a moderate level of implementation: relative strength in identity controls, email, and network/cloud technologies, versus gaps in application security, testing environments, and collaborative use.

Table 6 shows the detailed distributions, and the accompanying chart provides a visual reading of differences in means and deviations.

Table 6 Descriptive Analysis

ISOGMAF Framework	Institutions	Mean	Std. Deviation
ISOGMSF :I1	54	3.60	1.20
ISOGMSF :I2	54	4.10	1.18
ISOGMSF :I3	54	3.52	1.19
ISOGMSF :I4	54	3.80	1.25
ISOGMS :P5	54	3.44	1.28
ISOGMSF :P5.1	54	3.65	1.34
ISOGMSF :P6	54	4.05	1.32
ISOGMSF :P6.1	54	3.24	1.32
ISOGMSF :P6.2	54	3.73	1.30
ISOGMSF :P6.3	54	3.48	1.42
ISOGMSF :P7	54	3.69	1.34
ISOGMSF :P8	54	3.72	1.35
ISOGMSF :P8.1	54	3.46	1.24
ISOGMSF :P8.2	54	3.21	1.38
ISOGMSF :P8.3	54	3.53	1.28
ISOGMSF :P9	54	3.60	1.37
ISOGMSF :P9.1	54	3.40	1.39
ISOGMSF :P9.2	54	3.45	1.43
ISOGMSF :P10	54	3.74	1.54
ISOGMSF :P10.1	54	3.54	1.32
ISOGMSF :P10.2	54	3.57	1.26
ISOGMSF :P10.3	54	3.66	1.41
ISOGMSF :P11	54	3.46	1.44

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov619

ISOGMAF Framework	Institutions	Mean	Std. Deviation
ISOGMSF :P11.1	54	3.41	1.50
ISOGMSF :P11.2	54	3.63	1.44
ISOGMSF :P11.3	54	3.26	1.37
ISOGMSF :P11.4	54	3.72	1.42
ISOGMSF :P11.5	54	3.64	1.36
ISOGMSF :P12	54	3.57	1.26
ISOGMSF :P13	54	3.66	1.39
ISOGMSF :P14	54	3.94	1.50
ISGMSF :P15	54	3.37	1.61
ISOGMSF :R16	54	3.41	1.46
ISOGMSF :R17	54	3.78	1.38

C. Comparisons Across Participating Groups (U / A / O / I / Others)

This section provides a systematic comparison of cybersecurity-maturity levels across higher-education institution types (Universities/U, Academic/A, Organizations/O, Institutes/I, Others) using the ISOGMAF framework. The results show a clear gradient in readiness: universities and organizations tend toward a moderate-to-high range, while technical institutes lag behind; academic institutions and the "other" category exhibit wide variability tied to governance and resources. This pattern is consistent with literature linking maturity to clarity of governance, funding, and expertise, versus setbacks in resource-limited settings—especially in real-time monitoring and application security.

D. Highlighting the Findings and Linking them to the Research Objectives

- Maturity distribution: Most entities cluster between Levels 2–4 (partial implementation), with a smaller segment at Level 5 (proactive governance).
- *By Institutional Type:*

✓ U: ≈ 3.5–6.0 (moderate–high) with evident internal variance.
✓ A: ≈ 2.0–5.7 (low–high) with variability in automation and governance.
✓ O: ≈ 3.0–5.3 (moderate–high) driven by structural/financial support.
✓ I: 1.0–4.7 (low–moderate) with gaps in monitoring and response.
✓ Others: 2.3–6.0 depending on structural and capability differences.

These findings reinforce prior literature on persistent challenges facing higher-education institutions in attaining advanced capability to counter cyber threats. Salient contributing factors include limited funding, lack of technical competencies, and inconsistent policy implementation. Addressing these challenges requires targeted investments in cybersecurity education, automation of security processes, and alignment of institutional practices with international standards to bolster resilience. Fig 8 shows cybersecurity-maturity score ranges by institution type.

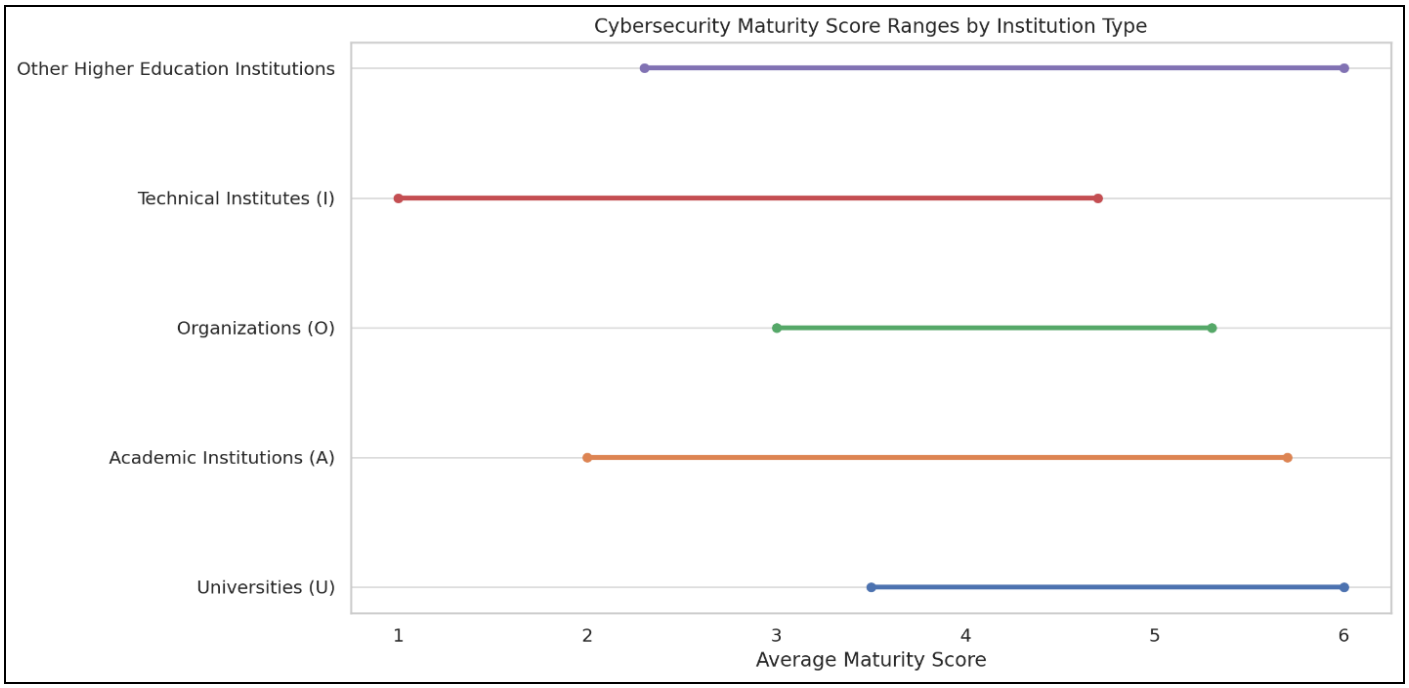

Fig 8 Cybersecurity Score Ranges by Institution Type

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov619

E. Scientific Value and Knowledge Contribution

- A precise comparative framework: The framework provides a differential maturity map across multiple institutional types, enriching the literature on readiness measurement in resource-constrained environments.
- Alignment with the literature: The observed patterns accord with prior studies that relate maturity to clarity of governance, funding, and experience, and underscore the impact of insufficient automation on real-time monitoring and incident response.

F. Cybersecurity-Maturity Analysis by Domains

This section tracks institutional performance across the three ISOGMAF domains: Identify (governance and risk recognition), Protect & Detect (protection and monitoring), and Respond & Recover (response and recovery). The results underscore an urgent need for targeted capacity-building investments, especially among low-maturity entities. It is evident that strengthening institutional governance, aligning with international standards, and embedding an awareness culture are pillars for enhancing cybersecurity resilience in higher education. Table 7 presents the key results by domain and examples of institutional average maturity with brief applied notes.

Table 7 Key Results by Domain

Domain	High Maturity Institutions	Moderate Maturity Institutions	Low Maturity Institutions
Risk Management (Identify)	A1, U1, O1	U6, U10, I2	A3, I3, Other14
Detection & Monitoring	U1, O1, A6	U3, I2, Other9	A3, U17, Other2
Protection	U5, U8, O3	U12, I1, Other6	A3, U17, Other14
Response	U4, A1, O1	U10, I2, Other12	A3, U7, Other14
Recovery	U2, U5, Other4	U12, I1, Other7	A3, U9, Other10

Domain High Maturity (examples) Moderate Maturity (examples) Low Maturity (examples) Brief applied notes Identify (risk management and recognition) A1, U1, O1 U6, U10, I2 A3, I3, Other14 Need to automate risk assessments, third-party assurance, and strengthen executive accountability.

Detection & Monitoring U1, O1, A6 U3, I2, Other9 A3, U17, Other2 Centralized logging, threat intelligence, and real-time alerts reduce time to detection.

Protection U5, U8, O3 U12, I1, Other6 A3, U17, Other14 Defense-in-depth (encryption, secure cloud, continuous compliance assessment) versus gaps in IAM and configuration.

Response U4, A1, O1 U10, I2, Other12 A3, U7, Other14 Plans/teams/simulations improve response speed and quality. Recovery U2, U5, Other4 U12, I1, Other7 A3, U9, Other10 Distributed backups and automated restoration reduce downtime and ensure business continuity.

G. Primary Gap Analysis

- Critical gaps appear in governance, risk management, and incident response, with shortcomings in application security (P8.2), testing environments (P11.3), and collaboration platforms (P15); variability is also evident in network monitoring (P10) and cloud readiness (P11.4).
- Institutions below 3.0 (e.g., A3, I3, Other14) lack governance frameworks and dedicated security teams and rely on traditional, non-automated architectures, increasing exposure to ransomware/phishing/data-leak attacks.
- Weak awareness and training; insufficient third-party/cloud risk scrutiny; absence of a clear leadership role (e.g., CISO); in addition to funding constraints, sector-level regulatory ambiguity, and weak threat-intelligence sharing among institutions.

➢ *The Results Recommend Two Integrated Tracks:*

- Rapid improvements: updated policies, training, access control, and procedure documentation.
- Structural investments: monitoring automation, real-time analytics, infrastructure enhancement, simulations, and business-continuity exercises.

VI. DISCUSSION AND RECOMMENDATIONS

The study achieves its primary objective by designing, releasing, applying, and validating the ISOGMAF framework in Yemen's higher-education environment. A unified reading of the findings shows that the overall maturity mean ≈ 2.3/6 reflects a status between "weak" and "moderate," with relative strength in Identify and recurring weaknesses in Respond/Recover (response plans, recovery, and business continuity). This pattern accords with the higher-education literature in resource-limited settings, which documents a structural gap between preventive and reactive measures [6][4][10][3], and simultaneously explains how ISOGMAF could function as both a "diagnostic lens" and an "execution road-map."

A. Recommendations

➢ *For National Policy:*

- Adopt a national policy framing annual maturity assessments using ISOGMAF or its equivalent to enable benchmarking and targeted interventions.
- Fund staged capacity-building tracks by maturity level and incorporate security indicators into accreditation criteria.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov619

➢ *For Institutions:*

- Conduct a systematic annual assessment across the five domains and establish a security unit led by a CISO or equivalent.
- Budget prioritization guided by framework data and a focus on digital behaviors/awareness as a primary human-risk factor.

➢ *For Researchers:*

- Benchmarking studies across institutions/regions; incident/indicator data to increase transparency.
- Maintain the framework by incorporating emerging threats, regulations, and technological evolution.

VII. FUTURE WORK

- Convert the framework into a web application with interactive analytics, longitudinal tracking, and peer comparison.
- Expand geographic representation to build a national database.
- A dedicated area for human factors (awareness/phishing/ compliance) to capture the cultural dimension.
- Employ predictive analytics/AI for proactive risk measurement and tailored improvement plans.

VIII. CONCLUSION

The study shows that ISOGMAF, as a localized and validated framework, provides diagnostic and practical value for elevating cybersecurity readiness in resource-constrained HEIs. The results align with the literature in terms of strength/weakness trends, with an applied knowledge contribution confirming that systematic localization of global standards can yield measurable improvement over short implementation cycles. Leading into the conclusion, this discussion guides policies, institutions, and researchers toward high-return interventions that close response/recovery gaps and support a sustainable security culture.

REFERENCES

[1]. 1M. Rizun and M. Pankowska, “Maturity model for assessment of personalization of higher education,” in Proc. KDIR, 2022, pp. 43–53.
[2]. S. P. Don Appuhamilage and R. M. D. U. Rathnayake, “Gap analysis of information security management systems in Sri Lankan higher education institutes,” unpublished, 2023.
[3]. B. Ulven and G. Wangen, “A systematic review of cybersecurity risks in higher education,” Future Internet, vol. 13, art. 39, 2021.
[4]. N. M. De Ramos and F. D. E. II, “Cybersecurity program for Philippine higher education institutions: A multiple-case study,” International Journal of Evaluation and Research in Education, 2022, p. 1199.
[5]. J. Li, W. Xiao, and C. Zhang, “Data security crisis in universities: Identification of key factors affecting data breach incidents,” Humanities and Social Sciences Communications, vol. 10, no. 1, pp. 1–18, 2023.
[6]. A. Aliyu, L. Maglaras, Y. He, I. Yevseyeva, E. Boiten, A. Cook, and H. Janicke, “A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom,” Applied Sciences, vol. 10, no. 10, 3660, 2020.
[7]. J. B. Bolanio, R. K. Paredes, and R. E. II, “Network security policy for higher education institutions based on ISO standards,” Mediterranean Journal of Basic and Applied Sciences, 2021.
[8]. S. Dwivedi and S. Vig, “Blockchain adoption in higher-education institutions in India: Identifying the main challenges,” Cogent Education, vol. 11, no. 1, 2292887, 2024.
[9]. M. S. A. A. Almekhlafi, Balanced information security maturity model based on ISO/IEC 27001:2013 and O-ISM3. Sana’a, Yemen: Yemen Academy for Graduate Studies, 2023.
[10]. A. B. Nassoura, “Cybersecurity technologies and practices in higher education institutions: A systematic review,” Webology, vol. 19, no. 3, 2022.
[11]. W. H. Hayes, Cyber insurance and small community banks: A mixed-methods exploration. Capitol Technology University, 2022.
[12]. E. Kenneally, L. Randazzese, and D. Balenson, “Cyber risk economics capability gaps research strategy,” in 2018 Int. Conf. on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA), 2018, pp. 1–6. IEEE.
[13]. J. Wolff and W. Lehr, “Roles for policy-makers in emerging cyber insurance industry partnerships,” in TPRC, Mar. 2018.
[14]. P. W. Coopers, Insurance 2020 & beyond: Reaping the dividends of cyber resilience. Price Waterhouse Cooper Insurance, 2015.
[15]. F. H. Katz, “The effect of a university information security survey on instruction methods in information security,” in Proc. 2nd Annu. Conf. on Information Security Curriculum Development, 2005, pp. 43–48.
[16]. A. R. Aedah and S. Hoga, “Maturity framework analysis ISO 27001:2013 on Indonesian higher education,” International Journal of Engineering & Technology, vol. 9, no. 2, pp. 429–436, 2020.
[17]. C. Biener, M. Eling, and J. H. Wirfs, “Insurability of cyber risk: An empirical analysis,” The Geneva Papers on Risk and Insurance—Issues and Practice, vol. 40, pp. 131–158, 2015.
[18]. D. Makupi and N. Masese, “Determining information security maturity level of an organization based on ISO 27001,” unpublished, 2019.
[19]. Z. Ismail, M. Masrom, Z. Sidek, and D. Hamzah, “Framework to manage information security for Malaysian academic environment,” Information Assurance & Cybersecurity, 2010, pp. 1–16.
[20]. I. Almomani, M. Ahmed, and L. Maglaras, “Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia,” PeerJ Computer Science, vol. 7, e703, 2021.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov619

[21]. A. Gerl, M. von der Heyde, R. Groß, R. Seck, and L. Watkowski, "Applying COBIT 2019 to IT governance in higher education," in INFORMATIK 2020, 2021, pp. 517–530. Gesellschaft für Informatik, Bonn.
[22]. H. P. Singh and T. S. Alshammari, "An institutional theory perspective on developing a cyber security legal framework: A case of Saudi Arabia," Beijing Law Review, vol. 11, p. 637, 2020.
[23]. S. Almuhammadi and M. Alsaleh, "Information security maturity model for NIST cyber security framework," Computer Science & Information Technology (CS & IT), vol. 7, no. 3, pp. 51–62, 2017.
[24]. J. Bass, "An early-stage ICT maturity model derived from Ethiopian education institutions," International Journal of Education and Development using ICT, vol. 7, no. 1, pp. 5–25, 2011.
[25]. M. H. Suwito, S. Matsumoto, J. Kawamoto, D. Gollmann, and K. Sakurai, "An analysis of IT assessment security maturity in higher education institution," in Information Science and Applications (ICISA) 2016, Springer Singapore, 2016, pp. 701–713.
[26]. L. Ajmi, N. Alqahtani, A. U. Rahman, and M. Mahmud, "A novel cybersecurity framework for countermeasure of SMEs in Saudi Arabia," in 2019 2nd Int. Conf. on Computer Applications & Information Security (ICCAIS), IEEE, 2019, pp. 1–9.
[27]. T. Al Hamed and M. Alenezi, "Business continuity management & disaster recovery capabilities in Saudi Arabia ICT businesses," International Journal of Hybrid Information Technology, vol. 9, no. 11, pp. 99–126, 2016.
[28]. R. Aziz and B. Shahzad, "Factors for measurement of ITES quality for higher education institutions in Saudi Arabia," Global Journal of Computer Science and Technology, vol. 15, no. 3, pp. 1–11, 2015.
[29]. A. Y. M. A. N. Altameem, "What drives successful e-learning? An empirical investigation of the key technical issues in Saudi Arabian universities," Journal of Theoretical & Applied Information Technology, vol. 53, no. 1, 2013.
[30]. M. Alnatheer and K. Nelson, "Proposed framework for understanding information security culture and practices in the Saudi context," unpublished, 2009.
[31]. A. Nsamba, "Maturity levels of student support e-services within an open distance e-learning university," International Review of Research in Open and Distributed Learning, vol. 20, no. 4, pp. 60–78, 2019.
[32]. M. Peñafiel, S. Luján-Mora, S. Vásquez, J. Zaldumbide, A. Cevallos, and D. Vásquez, "Application of e-learning maturity model in higher education," in EDULEARN17 Proc., 2017, pp. 4396–4404.
[33]. G. Secundo, S. Elena-Perez, Ž. Martinaitis, and K. H. Leitner, "An intellectual capital maturity model (ICMM) to improve strategic management in European universities: A dynamic approach," Journal of Intellectual Capital, vol. 16, no. 2, pp. 419–442, 2015.
[34]. Payment Card Industry, Data Security Standard: Requirements and Security Assessment, ver. 3, 2010.
[35]. D. Proença and J. Borbinha, "Information security management systems—a maturity model based on ISO/IEC 27001," in Business Information Systems—BIS 2018, Proc. 21, Springer, 2018, pp. 102–114.
[36]. S. Marshall, "A quality framework for continuous improvement of e-learning: The e-learning maturity model," International Journal of E-Learning & Distance Education / Revue internationale du e-learning et la formation à distance, vol. 24, no. 1, pp. 143–166, 2010.
[37]. McCuen, T. L., & MSCS, M. (2008). Building information modeling and the interactive capability maturity model. Associated Schools of Construction, 1–10.
[38]. Nazar, S., & Abbasi, E. (2008, April). CMMI and OPM3: Are they compatible? In International Multi Topic Conference (pp. 235–242). Berlin, Heidelberg: Springer.
[39]. Li, S., Liu, C., Xi, X., Zhao, C., Tian, Y., & Liu, C. (2019, August). Diagnosis platform development of partial discharge data based on CMMI model. In IOP Conference Series: Materials Science and Engineering, 605(1), 012006. IOP Publishing.
[40]. I. A. Humied, "Cybersecurity as emerging challenge to Yemen security," International Journal of Information Security and Cybercrime, vol. 11, no. 2, pp. 35–44, 2022. [Online]. Available: https://www.ijisc.com
[41]. Revaclier, A. R. (2021). SOC-AM: An Accessible Maturity Model for Security Operation Centers (Master's thesis, Eindhoven University of Technology, Netherlands). Retrieved from https://pure.tue.nl/ws/portalfiles/portal/198120514/Revaclier_A. R..pdf
[42]. NHS Digital. (n.d.). Data Security and Protection Toolkit: Help – Attachment 851. Retrieved June 13, 2025, from https://www.dsptoolkit.nhs.uk/Help/Attachment/851