

Developing the Cloud ERP Cybersecurity Assessment Framework (CECAF) for Evidence-Based Cybersecurity Capability Assessment in Cloud ERP Platforms

Staš Heric, Samo Bobek*

University of Maribor, Faculty of Economics and Business, Slovenia
 stas.heric@student.um.si, samo.bobek@um.si

ARTICLE INFO

Original Scientific Article

Article history:

Received July 2026

Revised August 2026

Accepted August 2026

JEL Classification

M10, M15, L86

Keywords:

Cloud ERP

Cybersecurity

Cybersecurity assessment framework

Cybersecurity capability assessment

Evidence-based assessment

Capability maturity

UDK: 004.056:004.4

DOI: 10.2478/ngoe-2026-0017

Cite this article as: Heric, S., & Bobek, S. (2026). Developing the Cloud ERP Cybersecurity Assessment Framework (CECAF) for Evidence-Based Cybersecurity Capability Assessment in Cloud ERP Platforms. Naše gospodarstvo/Our Economy, 72(3), 90-112. DOI: 10.2478/ngoe-2026-0017

©2026 The Authors. Published by the University of Maribor, Faculty of Economics and Business, Slovenia, in partnership with Paradigm Publishing Services. This is an open-access article under the CC BY-NC-ND 4.0 license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

Abstract

The purpose of this study is to develop the Cloud ERP Cybersecurity Assessment Framework (CECAF) to systematically evaluate cybersecurity capabilities in cloud ERP platforms. The framework was developed through the synthesis of academic literature, internationally recognised cybersecurity standards, cybersecurity capability maturity assessment principles, and cloud ERP-specific cybersecurity requirements, and demonstrated through an evidence-based assessment of Infor CloudSuite using publicly available official technical documentation. The findings demonstrate that CECAF enables a structured, transparent, and reproducible evaluation of cybersecurity capabilities across multiple assessment domains. The study contributes by introducing an analytical assessment framework tailored to cloud ERP platforms and by highlighting the methodological importance of documented technical evidence for objective cybersecurity capability assessment. The framework provides practical guidance for cybersecurity evaluation and comparative assessment of cloud ERP platforms.

*Corresponding author

Introduction

Digital transformation has fundamentally reshaped how organisations design, integrate, and manage business processes, making cloud Enterprise Resource Planning (ERP) platforms key enablers of organisational agility, scalability, and innovation (Ivanović & Marić, 2021; Lee et al., 2024). Organisations are replacing traditional on-premises ERP systems (Klaus et al., 2000) with cloud ERP platforms to improve operational efficiency, cross-functional integration, and data-driven decision-making (Lee et al., 2024; Llivisaca-Villazhañay et al., 2025). Their strategic value depends not only on their functional and technical capabilities but also on their successful organisational adoption and effective use within business processes (Sternad Zabukovšek & Bobek, 2025).

The widespread adoption of cloud ERP platforms has increased cybersecurity challenges. Unlike traditional ERP systems, cloud ERP platforms operate within highly interconnected digital ecosystems characterised by shared responsibility models, third-party integrations, cloud-native architectures, and continuous data exchange. Consequently, cybersecurity has evolved from a technical concern into a strategic organisational capability supporting business continuity, regulatory compliance, operational resilience, and organisational trust (Anica-Popa et al., 2024; Lee et al., 2024; NIST, 2024).

Despite the growing importance of cybersecurity in cloud ERP platforms, assessing cybersecurity capabilities remains a significant challenge. Existing cybersecurity standards and frameworks, including ISO/IEC 27001, the NIST Cybersecurity Framework (CSF 2.0), Zero Trust Architecture, and the Cloud Security Alliance Cloud Controls Matrix,

guide organisational cybersecurity management. However, these frameworks were developed primarily for cybersecurity governance and risk management rather than for evidence-based assessment of cybersecurity capabilities in cloud ERP platforms (Rose et al., 2020; Bertino, 2021; ISO/IEC, 2022; NIST, 2024; Cloud Security Alliance, 2024).

Furthermore, existing research has predominantly focused on cybersecurity risks, security controls, cloud ERP adoption, or individual technological solutions, while comparatively limited attention has been devoted to developing analytical approaches to cybersecurity capability assessment in cloud ERP platforms (Anica-Popa et al., 2024; Khokrale, 2025; Qazi et al., 2026). Although recent studies recognize the importance of assessing cybersecurity capability maturity, they offer limited methodological guidance on systematically, transparently, and reproducibly assessing cybersecurity capabilities using documented technical evidence (Brezavšček & Baggia, 2025; Liyanage et al., 2024). Consequently, a research gap exists regarding the availability of an analytical assessment framework specifically designed for evidence-based cybersecurity capability assessment in cloud ERP platforms.

To address this gap, this study develops the Cloud ERP Cybersecurity Assessment Framework (CECAF) to provide an evidence-based assessment of cybersecurity capabilities in cloud ERP platforms. It demonstrates its application by assessing Infor CloudSuite using publicly available technical documentation. The study contributes by (1) developing an analytical assessment framework synthesising established cybersecurity standards, capability maturity principles, and cloud ERP requirements; (2) demonstrating its application to a

contemporary cloud ERP platform; and (3) highlighting the value of transparent technical documentation for objective and reproducible cybersecurity assessment. The remainder of the paper presents the theoretical background, methodology, assessment results, discussion, and conclusions.

Theoretical Background

Evolution of ERP Systems

ERP systems were originally developed to overcome organisational information silos by integrating fragmented business functions into a unified information system. Their primary objective was to standardise business processes, establish a single source of organisational data, and support information sharing across functional areas, enabling greater operational efficiency, reduced data redundancy, and coordinated decision-making (Klaus et al., 2000).

As organisations accelerated their digital transformation initiatives, ERP systems evolved from transactional systems into enterprise-wide digital platforms that support organisational agility, process innovation, data-driven decision-making, and integration with advanced digital technologies. Contemporary ERP solutions increasingly incorporate business intelligence, advanced analytics, artificial intelligence, robotic process automation, and the Internet of Things (IoT), extending their role beyond process integration to become key enablers of digital transformation and long-term business competitiveness (Ivanović & Marić, 2021; Khan et al., 2025; Sternad Zabukovšek & Bobek, 2025).

The transition to cloud computing represents the latest stage in this evolution. Cloud-native ERP platforms provide scalability, flexibility, accessibility, and continuous software innovation while reducing infrastructure management requirements. As components of broader digital ecosystems integrating cloud services, external partners, mobile technologies, artificial intelligence, and data-driven business processes, they fundamentally transform the architecture and operational context of ERP systems. However, their extensive connectivity also expands the cybersecurity attack surface, making cybersecurity a strategic prerequisite for organisational resilience and the successful operation of cloud ERP platforms (Lee et al., 2024).

Unlike traditional on-premises ERP systems, cloud ERP platforms operate within highly interconnected digital infrastructures characterised by distributed services, external integrations, mobile access, and shared cloud resources. These characteristics substantially increase cybersecurity complexity, making security an essential organisational capability rather than merely a technical requirement. Understanding these characteristics, therefore, provides the foundation for examining the cybersecurity challenges associated with cloud-based ERP platforms.

Cloud-Based ERP Systems

The evolution of cloud computing has transformed the architecture, deployment, and management of ERP systems. Unlike traditional on-premises solutions that require dedicated hardware and software infrastructure, cloud ERP platforms are primarily delivered via Software-as-a-Service (SaaS)

models, enabling organisations to access enterprise applications via cloud infrastructure maintained by external service providers. This deployment model offers scalability, flexibility, lower infrastructure costs, automatic software updates, rapid implementation, and improved accessibility, making cloud ERP an attractive option for organisations of all sizes (Demi & Haddara, 2018; Lee et al., 2024). Beyond a different deployment model, cloud ERP represents a fundamental shift in the role of enterprise systems within digital organisations. Cloud ERP platforms operate as cloud-native digital platforms that support continuous innovation and interoperability while integrating enterprise processes with customer relationship management, supply chain management, IoT, artificial intelligence, business analytics, and external digital services through standardised application programming interfaces (APIs) and cloud integration services. This connectivity enhances organisational agility, accelerates digital innovation, and supports data-driven decision-making (Lee et al., 2024; Llivisaca-Villazhañay et al., 2025).

However, the same characteristics that create business value also increase cybersecurity complexity. Compared with traditional ERP environments, cloud ERP platforms operate within distributed infrastructures characterised by shared cloud resources, external integrations, remote access, mobile connectivity, and continuous data exchange. Consequently, security responsibilities are shared between cloud service providers and customer organisations, introducing challenges related to identity and access management (IAM), multi-tenancy, third-party dependencies, cloud misconfigurations, APIs, and increasingly sophisticated cyberattacks. Cybersecurity, therefore, becomes a strategic organisational capability rather

than merely a technical requirement (Demi & Haddara, 2018; Lee et al., 2024).

These characteristics distinguish cloud ERP platforms from traditional enterprise applications and explain why conventional cybersecurity approaches are insufficient for cloud-native ERP environments. Understanding these characteristics provides the foundation for identifying appropriate cybersecurity mechanisms and assessment frameworks.

Cybersecurity Challenges in Cloud-Based ERP Platforms

The migration of ERP systems to cloud environments has transformed organisational cybersecurity requirements. Unlike traditional on-premises ERP systems operating within relatively isolated corporate infrastructures, cloud ERP platforms are embedded in highly interconnected digital ecosystems characterised by cloud services, mobile access, external APIs, third-party integrations, and distributed data processing. While these characteristics enhance organisational flexibility and digital innovation, they also expand the cybersecurity attack surface and increase exposure to sophisticated cyber threats (Anica-Popa et al., 2024; Lee et al., 2024).

One of the principal cybersecurity challenges is the rapid expansion of potential attack vectors. Cloud ERP platforms continuously exchange data across organisational boundaries while supporting remote work, mobile devices, supplier integration, customer portals, and cloud-based applications. As a result, cyber attackers increasingly exploit vulnerabilities across cloud infrastructure, APIs, connected applications, and third-party services rather than targeting only the ERP application itself. Recent

studies identify ransomware, phishing attacks, cloud misconfigurations, supply chain attacks, and API vulnerabilities among the most critical threats affecting cloud ERP platforms (Anica-Popa et al., 2024; Khokrale, 2025).

Identity and access management (IAM) has therefore become one of the most critical security domains in cloud ERP platforms. Because these platforms support geographically distributed users, external partners, contractors, and mobile access, organisations require robust authentication, authorisation, and continuous identity verification. Traditional perimeter-based security models are increasingly insufficient, while identity-centric approaches based on multi-factor authentication, least-privilege access, privileged access management, and continuous verification have become essential for protecting enterprise resources against unauthorised access and insider threats (Rose et al., 2020; Bertino, 2021).

Cloud ERP has also changed organisational responsibility for cybersecurity. Under the shared responsibility model, cloud providers typically secure infrastructure and platform services. At the same time, customer organisations remain responsible for user management, access control, data governance, application configuration, regulatory compliance, and organisational security policies. Effective cloud ERP cybersecurity, therefore, requires coordinated governance rather than isolated technical controls (Singh & Sharma, 2021; NIST, 2024).

Beyond technical protection, contemporary literature increasingly recognises cybersecurity resilience as a strategic organisational capability. Organisations must continuously monitor security events, detect anomalies, respond rapidly to incidents, and recover critical business operations.

As cloud ERP platforms support mission-critical business processes, cybersecurity has evolved from an operational IT function into an essential component of organisational resilience and enterprise governance (Anica-Popa et al., 2024; NIST, 2024).

These challenges demonstrate that securing cloud ERP platforms requires more than isolated technical controls. Organisations need integrated cybersecurity frameworks combining governance, identity management, data protection, monitoring, incident response, and organisational resilience. The following section, therefore, reviews the principal cybersecurity frameworks that provide the theoretical foundation for assessing cybersecurity capabilities in cloud ERP platforms.

Cybersecurity Frameworks for Cloud-Based ERP Platforms

The increasing complexity of cloud ERP environments has stimulated the development of cybersecurity frameworks that provide organisations with structured guidance for managing cyber risks. Rather than relying on isolated technical controls, contemporary frameworks integrate governance, risk management, identity protection, continuous monitoring, incident response, and organisational resilience. Although they were not specifically developed for cloud ERP platforms, they provide a valuable theoretical foundation for assessing cybersecurity capabilities.

From a governance perspective, cybersecurity is regarded as an organisational capability requiring strategic management rather than merely a technical function. The NIST Cybersecurity Framework (CSF) 2.0 organises cybersecurity

activities into six interconnected functions—Govern, Identify, Protect, Detect, Respond, and Recover—supporting organisational cyber resilience throughout the cybersecurity lifecycle (NIST, 2024). Similarly, ISO/IEC 27001 defines requirements for implementing an Information Security Management System (ISMS) based on continuous risk assessment, governance, and improvement. Together, these frameworks emphasise that cybersecurity should be embedded within organisational governance structures and business processes rather than treated as an isolated technical responsibility (ISO/IEC, 2022).

The migration of enterprise systems to cloud environments has challenged traditional perimeter-based security models. As cloud ERP platforms support geographically distributed users, mobile devices, external partners, cloud services, and APIs, the assumption of trusted internal networks has become increasingly obsolete. Zero Trust Architecture (ZTA) addresses these challenges by continuously verifying the "never trust, always verify" principle (Rose et al., 2020). It emphasises identity and access management (IAM), multi-factor authentication (MFA), least-privilege access, privileged access management, and continuous authentication as key mechanisms for protecting enterprise resources against unauthorised access and insider threats (Bertino, 2021). Recent studies further highlight the growing importance of identity-centric security in cloud ERP environments (Mushtaq et al., 2025).

Contemporary cybersecurity extends beyond preventing cyberattacks to ensuring the continuous operation of organisational processes. This perspective emphasises continuous monitoring, threat detection, incident response, business continuity, and recovery capabilities. Modern cloud

ERP platforms, therefore, require security approaches capable of maintaining operational continuity during cybersecurity incidents. Security monitoring, security information and event management (SIEM), automated threat detection, vulnerability management, backup strategies, disaster recovery, and organisational learning are recognised as essential components of resilient cloud ERP platforms (NIST, 2024; Anica-Popa et al., 2024). Cybersecurity should therefore be evaluated not only by the technical controls implemented, but also by an organisation's ability to detect, respond to, and recover from cyber incidents.

Although these frameworks provide complementary perspectives for managing organisational cybersecurity, none were specifically designed to evaluate cybersecurity capabilities in cloud ERP platforms. Cloud ERP environments introduce domain-specific characteristics, including enterprise process integration, cloud-native architectures, shared responsibility models, and extensive third-party connectivity. Consequently, assessing cybersecurity capabilities requires an analytical framework that integrates governance, identity-centric protection, and operational resilience into a unified assessment. Building on these complementary perspectives, this study develops the Cloud ERP Cybersecurity Assessment Framework (CECAF).

Key Cybersecurity Mechanisms for Cloud-Based ERP Platforms

The increasing complexity of cloud ERP environments has shifted organisational cybersecurity from isolated technical safeguards to integrated security mechanisms that collectively protect enterprise applications, business processes, and organisational data. Rather than relying on

individual security controls, cloud ERP cybersecurity combines complementary mechanisms to address identity protection, data security, continuous monitoring, governance, and organisational resilience, thereby establishing a multilayered security architecture for cloud-native enterprise environments.

Identity has become the primary security perimeter in cloud ERP environments. Unlike traditional on-premises systems protected by network boundaries, cloud ERP platforms support geographically distributed users, external partners, suppliers, mobile devices, and cloud services. Consequently, identity and access management (IAM) has become one of the most critical cybersecurity mechanisms for controlling access to enterprise resources. Multi-factor authentication (MFA), single sign-on (SSO), privileged access management (PAM), role-based access control (RBAC), and least-privilege principles provide continuous identity verification and reduce unauthorised access, identity theft, credential misuse, and insider threats (Rose et al., 2020; Bertino, 2021).

Protecting enterprise data remains a core objective of cloud ERP cybersecurity. As sensitive organisational information is exchanged across cloud services, applications, and external stakeholders, organisations must ensure data confidentiality, integrity, and availability throughout their lifecycle. Encryption of data at rest and in transit, cryptographic key management, secure backup strategies, data integrity verification, and secure cloud storage are widely recognised as fundamental mechanisms for protecting enterprise information. These controls are particularly important under shared responsibility models, where organisations remain responsible for

protecting business data despite outsourcing infrastructure management to cloud providers (NIST, 2024; ISO/IEC, 2022).

Cloud ERP cybersecurity also depends on continuous monitoring rather than periodic security assessments. Modern security architectures integrate logging, Security Information and Event Management (SIEM), vulnerability management, automated alerting, behavioural analytics, and AI-supported threat detection to identify suspicious activities, correlate security events, and accelerate incident detection (Anica-Popa et al., 2024; Dwivedi et al., 2021).

Effective cybersecurity also requires governance mechanisms integrating organisational policies, regulatory compliance, security auditing, risk management, and continuous security assessment. These mechanisms establish organisational responsibilities, support compliance, and provide the foundation for implementing technical security controls (NIST, 2024; ISO/IEC, 2022).

Finally, organisational resilience has become an essential component of cloud ERP cybersecurity. Preparedness, incident response, business continuity, disaster recovery, recovery testing, and organisational learning enable organisations to minimise operational disruption and restore critical ERP services following cybersecurity incidents, thereby strengthening organisational resilience (NIST, 2024; Anica-Popa et al., 2024).

Collectively, these complementary cybersecurity mechanisms provide the theoretical foundation for developing the Cloud ERP Cybersecurity Assessment Framework (CECAF), which synthesises governance, identity protection, data security,

monitoring, and resilience into a structured analytical approach for assessing cybersecurity capabilities in cloud ERP platforms.

Research Methodology

Research Design

This study employs a qualitative case research design to assess cybersecurity capabilities in a Cloud ERP environment systematically. A qualitative case research is appropriate because cybersecurity represents a complex, context-dependent phenomenon shaped by technological architecture, governance mechanisms, security controls, and organisational practices. Rather than examining individual security features or testing causal relationships, the study evaluates cybersecurity capabilities within a real-world Cloud ERP platform by applying the proposed CECAF to the Infor CloudSuite case research.

Building on the identified research gap, the CECAF was developed by synthesising academic literature, internationally recognised cybersecurity standards, and industry best practices. The framework provides a structured approach for evaluating cybersecurity capabilities across predefined assessment domains using documented technical evidence and a capability maturity model. This enables a consistent evaluation from organisational, technical, and operational perspectives (Becker et al., 2009; ISO/IEC, 2022; NIST, 2024).

A case research design is particularly appropriate because cybersecurity capabilities cannot be adequately evaluated outside their technological context. Cloud ERP platforms integrate interconnected security mechanisms, including

application security, security monitoring, incident response, and governance (Yin, 2018).

The research followed a four-phase process. First, the literature was reviewed to identify cybersecurity requirements and assessment domains relevant to Cloud ERP platforms. Second, these findings were synthesised into the CECAF. Third, the framework was applied to the selected case through systematic evidence collection and capability assessment. Finally, the results were analysed to identify cybersecurity strengths, potential vulnerabilities, and opportunities for improvement. This process establishes a connection between the theoretical foundations, the analytical framework, and the empirical evaluation, enhancing the methodological rigour and reproducibility of the study.

Research Context: Infor CloudSuite Industrial

The selected case is Infor CloudSuite Industrial (Infor CSI), a cloud-native ERP platform primarily designed for manufacturing organisations. It integrates core business processes, including production planning, procurement, inventory management, supply chain management, finance, customer relationship management, and quality management, within a unified cloud environment. As a SaaS solution, Infor CSI incorporates embedded cybersecurity mechanisms supporting secure data management, user authentication, access control, regulatory compliance, and continuous service availability.

Infor CSI was selected for three reasons. First, it represents a contemporary Cloud ERP platform with cybersecurity capabilities aligned with internationally recognised security standards and current cloud security practices. Second, its

architecture integrates multiple layers of cybersecurity controls, including IAM, encryption, application security, infrastructure protection, security monitoring, and governance, providing an appropriate environment for cybersecurity assessment. Third, the platform is widely adopted in manufacturing organisations, making the findings relevant to comparable Cloud ERP implementations.

The assessment focuses on cybersecurity capabilities embedded within the platform rather than organisation-specific security policies or implementation practices. Accordingly, the CECAF was applied to evaluate documented cybersecurity mechanisms while minimising the influence of organisation-specific factors that may differ across individual implementations.

The unit of analysis is the cybersecurity capability of the selected Cloud ERP platform. Rather than evaluating individual security features in isolation, the assessment examines how governance mechanisms, technical safeguards, operational controls, and compliance measures collectively contribute to overall cybersecurity capability. This holistic perspective enables a consistent assessment across the six CECAF domains.

Cloud ERP Cybersecurity Assessment Framework (CECAF)

The cybersecurity assessment was conducted using the CECAF. Developed through the synthesis of academic literature, internationally recognised cybersecurity standards, and industry best practices, the CECAF provides a structured instrument for evaluating cybersecurity capabilities

in Cloud ERP platforms. Rather than proposing a new cybersecurity framework, it operationalises established cybersecurity principles into a consistent analytical assessment methodology. Its development was informed by ISO/IEC 27001:2022, the NIST Cybersecurity Framework (CSF 2.0), the Cloud Security Alliance Cloud Controls Matrix (CCM), and recent research on cybersecurity challenges and maturity assessment in Cloud ERP platforms (ISO/IEC, 2022; NIST, 2024; Cloud Security Alliance, 2024; Anica-Popa et al., 2024; Qazi et al., 2026).

The CECAF translates cybersecurity requirements identified in the literature into six complementary assessment domains representing the principal organisational, technical, and operational dimensions of Cloud ERP cybersecurity. By organising predefined domains and representative assessment criteria, it supports a systematic, transparent, and repeatable evaluation while enabling cybersecurity capabilities to be assessed holistically rather than as isolated security controls. This multidimensional perspective is consistent with previous research advocating structured cybersecurity assessments in cloud environments (Almorsy et al., 2016; Sunyaev, 2020).

Unlike recent approaches that focus primarily on benchmarking or ranking ERP platforms, the CECAF emphasises an evidence-based assessment of cybersecurity capabilities within a selected Cloud ERP environment. It supports the evaluation of governance mechanisms, technical safeguards, operational controls, and compliance practices through a consistent analytical methodology (Qazi et al., 2026). The structure of the CECAF is presented in Table 1.

Table 1
CECAF: Assessment Domains, Representative Assessment Criteria, Evidence Sources, and Capability Assessment

Assessment Domain	Representative Assessment Criteria	Typical Evidence	Capability Assessment
Identity and Access Management (IAM)	User authentication, Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC), Single Sign-On (SSO), privileged access management, password policies	System configuration, security settings, vendor documentation, and administration guides	Level 1–5
Data Protection and Privacy	Encryption at rest, encryption in transit, key management, backup and recovery, data retention, privacy controls	Encryption documentation, backup policies, compliance reports, and technical documentation	Level 1–5
Infrastructure and Network Security	Network segmentation, firewalls, secure cloud infrastructure, vulnerability management, endpoint protection, and infrastructure hardening	Infrastructure documentation, security architecture, vulnerability reports, cloud configuration	Level 1–5
Application Security	Secure software development, patch management, API security, application configuration, security testing, and secure integrations	Release notes, patch documentation, API documentation, security configuration	Level 1–5
Security Monitoring and Incident Response	Logging, audit trails, security monitoring, alerting, incident response procedures, threat detection	Audit logs, monitoring dashboards, incident response documentation, and security reports	Level 1–5
Governance, Risk, and Compliance	Security governance, risk management, compliance certifications, security policies, third-party assurance, and audit support	Security policies, compliance certificates, audit documentation, governance reports	Level 1–5

Source: Developed by the authors based on ISO/IEC (2022), NIST (2024), Cloud Security Alliance (2024), Anica-Popa et al. (2024), and Qazi et al. (2026).

Each representative assessment criterion was evaluated using a five-level Capability Maturity Model (CMM). The CMM assesses the extent to which cybersecurity capabilities are implemented, formalised, monitored, measured, and continuously improved. Applying a common maturity scale ensures consistency across assessment domains and facilitates comparison of cybersecurity capabilities. The use of maturity-based assessment is consistent with established maturity model research (Paulk et al., 1993; Becker et al., 2009) and recent cybersecurity assessment approaches for Cloud ERP systems (Qazi et al., 2026). The capability maturity levels are presented in Table 2.

Table 2

Capability Maturity Levels Used in the CECAF Assessment

Capability Level	Description
Level 1 – Initial	Cybersecurity practices are informal, limited, and primarily reactive. Security controls are implemented inconsistently or only after security incidents occur.
Level 2 – Managed	Basic cybersecurity controls have been implemented and are managed, although processes remain only partially standardised and are applied inconsistently across the platform.
Level 3 – Defined	Cybersecurity policies, procedures, and technical controls are formally documented, standardised, and consistently implemented throughout the platform.
Level 4 – Managed and measured	Cybersecurity capabilities are continuously monitored, measured, and periodically reviewed using defined security metrics and performance indicators to support proactive management.
Level 5 – Optimized	Cybersecurity capabilities are continuously improved through automation, advanced monitoring, proactive risk management, and the systematic adoption of security best practices.

Source: Adapted from Paulk et al. (1993), Becker et al. (2009), and Qazi et al. (2026).

Each capability rating was supported by documented evidence, including observable security features, system configuration settings, vendor technical documentation, compliance documentation, administrative guides, audit reports, and other verifiable sources. This evidence-based approach reduces evaluator subjectivity, strengthens consistency, and improves assessment repeatability (Yin, 2018; ISO/IEC, 2022).

The CECAF integrates governance mechanisms, technical safeguards, operational controls, and compliance practices into a single analytical framework for evaluating cybersecurity capabilities. The resulting capability profile provides a structured basis for identifying cybersecurity strengths, potential vulnerabilities, and opportunities for improvement.

Data Collection, Assessment Procedure, and Research Quality

The cybersecurity assessment was based on multiple sources of evidence to ensure a comprehensive evaluation of the selected cloud ERP platform. Consistent with evidence-based case research, information was collected from publicly available vendor documentation, technical implementation guides, security configuration documentation, compliance reports, official knowledge base articles, product release documentation, and other official information describing the cybersecurity capabilities of Infor CSI (Yin, 2018).

Using multiple evidence sources enabled methodological triangulation by verifying cybersecurity capabilities through different types of documentation rather than relying on a single source. Whenever possible, individual assessment criteria were supported by multiple sources of evidence. The collected evidence was organised according to the six assessment domains of the CECAF before the capability assessment.

The assessment followed a four-stage procedure. First, the collected evidence was reviewed and classified according to the six CECAF assessment

domains. Relevant security mechanisms, governance practices, technical safeguards, and compliance features were identified for each assessment criterion. Second, the documented evidence was evaluated against the representative assessment criteria presented in Table 1. Third, each assessment criterion was assigned a capability maturity level using the five-level CMM presented in Table 2. Capability ratings were based exclusively on documented evidence. Finally, the individual assessments were synthesised into an overall cybersecurity capability profile identifying cybersecurity strengths, potential weaknesses, and opportunities for improvement.

The collected evidence was analysed qualitatively using the CECAF. Cybersecurity capabilities were evaluated against predefined assessment criteria and maturity levels, with a focus on their presence, completeness, and maturity across the six assessment domains. Particular attention was given to aligning governance mechanisms, technical controls, operational security practices, and compliance measures to provide an integrated assessment of cybersecurity capability. The findings were synthesised into domain-level assessments and an overall cybersecurity capability profile.

Several measures enhanced the quality and credibility of the assessment. First, the CECAF provided predefined assessment domains, representative criteria, evidence requirements, and the CMM, ensuring consistency throughout the evaluation. Second, each capability rating was supported by documented, verifiable evidence from multiple official sources, thereby strengthening methodological triangulation and reducing subjective interpretation (Yin, 2018). Third, the

predefined capability maturity levels enabled consistent evaluation across all assessment domains and facilitated comparison of cybersecurity capabilities (Becker et al., 2009; Paulk et al., 1993). Finally, the explicit documentation of the assessment procedure, evaluation criteria, and evidence sources supports replication of the methodology and application of the CECAF to other Cloud ERP platforms. Although based on a single case research, the framework provides a structured and transferable approach for future cybersecurity assessments.

Results

To achieve the research objective, the CECAF was applied to assess Infor CSI's cybersecurity capabilities across six assessment domains. The assessment was based exclusively on documented technical evidence obtained from official vendor documentation, security administration guides, API documentation, compliance documentation, and the Infor Trust Center. Capability maturity levels were assigned solely on documented evidence rather than vendor claims.

The assessment indicates that Infor CSI demonstrates a high level of cybersecurity capability. Four of the six assessment domains achieved Capability Maturity Level 4 (Managed), while two achieved Level 3 (Defined). These findings indicate that cybersecurity is systematically supported through technical controls, centralised administration, and governance mechanisms. The lower maturity levels reflect limitations in publicly available technical evidence rather than deficiencies in cybersecurity capabilities. Consequently, Level 3 assessments should be interpreted as evidence limitations within the

CECAF rather than lower security maturity.

Table 3 summarises the cybersecurity capability profile produced by the CECAF. The strongest capabilities were identified in IAM, Application and Platform Security, Integration and API Security, and Compliance, Governance and Resilience, where extensive technical documentation supports mature

security controls. Lower maturity levels were assigned to Data Protection and Privacy and Monitoring, Logging, and Auditability because several advanced capabilities could not be fully verified using publicly available documentation. Consequently, the assessment reflects both implemented cybersecurity controls and the availability of documented technical evidence.

Table 3

Cybersecurity Capability Profile of Infor CSI Based on the CECAF Assessment

CECAF Assessment Domain	Assessment Dimensions	Key Technical Evidence	CMM Level
Identity and Access Management (IAM)	Authentication; Authorisation; Identity Federation; Access Governance	MFA, RBAC, SAML federation, centralized identity administration	Level 4 – Managed
Application and Platform Security	Infrastructure Security; Secure Configuration; Vulnerability Management; Platform Protection	Secure cloud infrastructure, centralized security configuration, vulnerability management, and platform protection	Level 4 – Managed
Data Protection and Privacy	Data Encryption; Data Lifecycle Protection; Backup and Recovery; Privacy Protection	Data protection controls, backup and recovery processes, privacy framework, and GDPR compliance	Level 3 – Defined
Integration and API Security	API Authentication; Secure Communication; API Management; Integration Security	OAuth 2.0 authentication, API Gateway, HTTPS communication, secure system integration	Level 4 – Managed
Monitoring, Logging and Auditability	Audit Logging; Security Monitoring; Event Traceability; Incident Support	Audit logging, event traceability, operational monitoring, vulnerability reporting	Level 3 – Defined
Compliance, Governance and Resilience	Regulatory Compliance; Security Governance; Business Continuity; Risk Management	ISO certifications, SOC assurance reports, business continuity planning, security governance	Level 4 – Managed

Source: Authors' assessment based on Infor (2020, 2023, 2024, n.d.).

Identity and Access Management

The IAM domain achieved Level 4 (Managed), indicating a mature approach to authentication, authorisation, and identity administration. The assessment identified comprehensive support for enterprise authentication mechanisms, including

multi-factor authentication (MFA), role-based access control (RBAC), centralised identity administration, and federated identity management based on Security Assertion Markup Language (SAML). Together, these capabilities provide a robust foundation for controlling user access to cloud ERP resources while reducing the risk of

unauthorised access (Infor OS Security Administration Guide, n.d.; Infor Federated Security, n.d.).

The assessment also confirmed support for configurable authentication policies, delegated administration, service account management, and integration with external identity providers. These capabilities support centralised identity management consistent with the principle of least privilege and strengthen identity protection by enabling federated authentication through enterprise identity providers (Infor OS User Administration Guide, n.d.).

Although authentication, authorisation, and identity federation demonstrated mature, well-documented capabilities, the available documentation provides limited evidence of advanced identity governance mechanisms, including automated access recertification, segregation-of-duties (SoD) analysis, privileged access management (PAM), and continuous identity risk assessment. While these capabilities may exist within broader enterprise security ecosystems, they cannot be verified from publicly available technical documentation.

The findings indicate that Infor CSI provides mature identity protection capabilities supported by documented technical controls. However, the available evidence was insufficient to justify the highest maturity level.

Application and Platform Security

The Application and Platform Security domain achieved Level 4 (Managed), reflecting a mature implementation of technical and organisational security controls. The assessment covered four

dimensions: infrastructure security, secure configuration, vulnerability management, and platform protection, demonstrating that security is embedded throughout the design, deployment, and operation of the cloud ERP platform (Infor Trust Center, n.d.).

The assessment identified substantial evidence of secure cloud infrastructure management, including documented security controls, centralised security administration, and internationally recognised compliance certifications. Secure configuration is supported by documented administrative procedures enabling organisations to configure authentication policies, security domains, session management, and other platform security settings in a controlled and consistent manner (Infor OS Security Administration Guide, n.d.; Infor Information Security Plan, 2023).

The vulnerability management dimension also demonstrated a high level of maturity. Official documentation outlines coordinated vulnerability disclosure procedures, structured security assessments, and regular maintenance processes to identify and mitigate security weaknesses throughout the platform lifecycle. Secure cloud architecture, encrypted communications, tenant isolation, and layered infrastructure protection further support platform protection.

Although all four assessment dimensions demonstrated mature capabilities, the publicly available documentation provides limited evidence of advanced infrastructure hardening techniques, autonomous threat-prevention mechanisms, and internal security engineering practices. Consequently, the available evidence supports a managed cybersecurity environment but is

insufficient to justify the highest maturity level.

The findings indicate that Application and Platform Security is one of the strongest cybersecurity domains of the evaluated platform. Comprehensive documentation of security controls, centralised administration, and vulnerability management demonstrates a mature and well-managed security environment.

Data Protection and Privacy

The Data Protection and Privacy domain achieved Level 3 (Defined). The assessment covered four dimensions: data encryption, data lifecycle protection, backup and recovery, and privacy protection. While it identified a comprehensive organisational framework supporting data protection and privacy, the publicly available documentation provided less detailed evidence for several advanced technical controls than in other assessment domains (Infor Data Privacy, 2024).

The privacy protection dimension demonstrated the highest level of maturity. Official documentation describes established privacy governance practices, compliance with the General Data Protection Regulation (GDPR), and policies governing the processing, protection, and management of customer data. These measures indicate that privacy management is formally integrated into the platform's governance framework (Infor Information Security Plan, 2023; Infor Trust Center, n.d.).

The documentation also describes administrative, technical, and physical safeguards for protecting customer information throughout its lifecycle. In addition, backup and recovery mechanisms are incorporated into the SaaS operating model to

support service availability and organisational resilience.

However, publicly available documentation provides limited evidence for several important aspects of data protection, including encryption key management, secure data deletion procedures, product-specific data retention mechanisms, and recovery objectives for individual ERP services. Because the CECAF assigns capability levels solely on verifiable, documented evidence, these limitations influenced the assessment.

The findings indicate mature organisational privacy governance and well-established data protection practices. However, the available evidence was insufficient to verify several advanced technical capabilities. Consequently, the assessment reflects the availability of documented technical evidence rather than deficiencies in the platform's overall approach to data protection and privacy.

Integration and API Security

The Integration and API Security domain achieved Level 4 (Managed), demonstrating a mature approach to securing the platform's integration architecture. The assessment covered four dimensions: API authentication, secure communication, API management, and integration security. Together, these dimensions indicate that Infor CSI provides a robust framework for secure communication between the ERP platform and external applications, services, and enterprise systems (Infor ION API Administration Guide, n.d.; Infor OS API Gateway Administration Guide, n.d.).

The strongest evidence was identified in the API authentication and API management dimensions.

Official documentation describes the implementation of OAuth 2.0 authentication, bearer token authorisation, centralised management of authorised applications, and secure client registration through the API Gateway. These mechanisms provide standardised authentication and authorisation procedures widely recognised as best practices for protecting APIs (Infor ION API Administration Guide, n.d.).

The secure communication dimension further demonstrates platform maturity by enabling encrypted communication via HTTPS and Transport Layer Security (TLS). Together with centralised API administration and secure integration mechanisms, these controls help ensure the confidentiality, integrity, and authenticity of information exchanged between interconnected systems.

The integration security dimension supports secure system-to-system communication through standardised authentication flows, controlled API access, and secure integration services. These capabilities enable organisations to integrate Infor CSI with heterogeneous enterprise environments while maintaining consistent security controls across multiple integration points.

Overall, the available evidence demonstrates a mature integration security architecture supported by well-documented technical controls. However, publicly available documentation provides limited evidence of advanced API threat detection, adaptive protection mechanisms, behavioural analytics, and automated protection against API abuse. Consequently, the findings support a mature integration security capability, although the available evidence was insufficient to justify the highest maturity level.

Monitoring, Logging and Auditability

The Monitoring, Logging, and Auditability domain achieved Level 3 (Defined). The assessment covered four dimensions: audit logging, security monitoring, event traceability, and incident support. Although comprehensive capabilities supporting auditability and operational transparency were identified, the available documentation provides limited evidence regarding advanced security monitoring and automated incident response capabilities (Infor Audit Logging Documentation, n.d.).

Among the four assessment dimensions, audit logging and event traceability demonstrated the highest level of maturity. Official documentation describes configurable audit logs for user activities, administrative actions, authentication events, and system operations. These capabilities establish comprehensive traceability of critical activities within the cloud ERP environment and provide a strong foundation for internal controls, compliance verification, and digital forensic investigations (Infor ION API Administration Guide, n.d.; Infor Trust Center, n.d.).

The documentation also describes monitoring capabilities for operational processes, API transactions, and administrative activities. In addition, Infor maintains a structured vulnerability reporting programme enabling security researchers and customers to report suspected vulnerabilities through established disclosure procedures. These processes contribute to continuous platform security improvement and strengthen accountability throughout the security lifecycle.

However, the available evidence provides limited insight into capabilities typically associated with

highly mature security operations, including integrated SIEM, automated threat detection, security orchestration, behavioural anomaly detection, and automated incident response. As these capabilities could not be verified through publicly available documentation, they were not considered in the maturity assessment.

The findings indicate strong support for auditability, accountability, and operational monitoring. However, the available evidence was insufficient to verify advanced operational cybersecurity capabilities typically associated with the highest maturity level.

Compliance, Governance, and Resilience

The Compliance, Governance and Resilience domain achieved Level 4 (Managed), indicating a mature governance framework supported by internationally recognised compliance practices and documented resilience measures. The assessment covered four dimensions: regulatory compliance, security governance, business continuity, and risk management (Infor Trust Center, n.d.).

The strongest evidence was identified in the regulatory compliance and security governance dimensions. Official documentation demonstrates that Infor maintains internationally recognised certifications and assurance programmes, including ISO certifications and SOC assurance reports, complemented by documented information security policies and privacy management practices. Together, these mechanisms establish a formal governance structure supporting regulatory compliance and the consistent implementation of cybersecurity controls across the cloud ERP environment (Infor Information Security Plan, 2023; Infor Business Continuity Plan Overview, 2020).

The business continuity dimension also demonstrated a high level of maturity. Publicly available documentation describes business continuity and disaster recovery planning, including organisational procedures for maintaining service availability and recovering from operational disruptions. These measures strengthen platform resilience and support the continuity of critical business services.

In contrast, the risk management dimension was supported primarily by documented vulnerability disclosure procedures and organisational security management practices. While these mechanisms demonstrate a structured approach to identifying and addressing security risks, the available documentation provides limited evidence of enterprise-wide cybersecurity risk metrics, continuous resilience testing, quantitative risk assessment, and governance performance indicators. Consequently, the available evidence was insufficient to verify the most advanced risk management capabilities.

The findings indicate that Infor CSI is supported by a mature governance framework integrating compliance, security management, and operational resilience. However, the available evidence was insufficient to justify the highest maturity level (Infor Trust Center, n.d.; Infor Information Security Plan, 2023; Infor Business Continuity Plan Overview, 2020).

Overall Assessment of the CECAF Capability Profile

The overall CECAF capability profile indicates that Infor CSI demonstrates a consistently high level of cybersecurity capability across the evaluated domains. Four domains achieved Level 4 (Managed), reflecting mature implementation of technical

security controls, centralised administration, secure integration mechanisms, and governance practices. The remaining two domains—Data Protection and Privacy and Monitoring, Logging and Auditability—achieved Level 3 (Defined).

These lower maturity levels should not be interpreted as evidence of weaker cybersecurity controls. Instead, they reflect the evidence-based assessment principles of the CECAF, under which capability levels were assigned exclusively based on publicly verifiable technical evidence. Where sufficient evidence was unavailable to verify advanced cybersecurity capabilities, higher maturity levels were not assigned.

This assessment approach enhances methodological transparency and reproducibility by emphasising documented technical capabilities rather than vendor claims or marketing materials. Consequently, the resulting capability profile represents an evidence-based evaluation of publicly documented cybersecurity capabilities rather than a comprehensive audit of all security mechanisms implemented within the platform.

Overall, the findings demonstrate that Infor CSI provides a mature cybersecurity environment characterised by robust identity management, secure cloud platform architecture, standardised API security, and comprehensive governance practices. They also highlight the importance of transparent technical documentation when assessing cybersecurity capabilities in cloud ERP platforms. This observation provides the basis for discussing the findings, their relationship to existing cybersecurity frameworks and prior research, and the methodological contribution of the CECAF.

Discussion

The primary objective of this study was to evaluate the cybersecurity capabilities of a cloud ERP platform using the proposed CECAF and to examine whether an evidence-based analytical framework can provide a transparent, systematic, and reproducible approach to cybersecurity assessment based on publicly available technical documentation. The assessment demonstrated that Infor CSI exhibits a consistently high level of cybersecurity capability, with four assessment domains achieving Level 4 (Managed) and two achieving Level 3 (Defined). Overall, the findings indicate that cybersecurity within the evaluated cloud ERP platform is supported by an integrated combination of technical controls, administrative mechanisms, and governance practices rather than isolated security measures.

Although the Data Protection and Privacy and Monitoring, Logging and Auditability domains achieved Level 3 (Defined), these results should not be interpreted as evidence of weaker cybersecurity capabilities. Instead, they reflect the limited availability of publicly verifiable technical evidence for advanced capabilities, including encryption key management, behavioural monitoring, security operations, and automated incident response. Consequently, while such capabilities may be implemented within the platform, they could not be independently verified using the evidence available at the time of the assessment.

This observation highlights an important methodological contribution of the CECAF. The findings demonstrate that cybersecurity capability assessment depends not only on the

implementation of security controls but also on the availability of verifiable technical evidence to support them. By assigning capability levels exclusively on documented evidence, the CECAF promotes a transparent, reproducible, and evidence-based assessment while reducing reliance on vendor claims or marketing materials.

Taken together, these findings demonstrate that the CECAF addresses the identified research gap by providing a structured methodology for assessing cybersecurity capabilities in cloud ERP platforms, supported by documented technical evidence.

The findings are broadly consistent with previous research identifying identity and access management, secure cloud infrastructure, governance, and secure integration as fundamental components of cloud ERP cybersecurity (Lee et al., 2024; Anica-Popa et al., 2024; NIST, 2024). Consistent with these studies, the assessment confirms that effective cloud ERP cybersecurity depends on the coordinated implementation of technical, organisational, and governance controls rather than isolated security mechanisms.

The high maturity observed in the IAM and Integration and API Security domains reinforces previous research highlighting secure authentication, identity federation, API protection, and secure interoperability as essential requirements for cloud-based enterprise systems (Rose et al., 2020; Bertino, 2021; NIST, 2024). As cloud ERP platforms become increasingly interconnected with external applications and cloud services, these capabilities become critical for maintaining secure enterprise environments.

The findings for Data Protection and Privacy and Monitoring, Logging and Auditability also support

previous research emphasising privacy governance, regulatory compliance, continuous monitoring, auditability, and incident response as key cybersecurity capabilities in cloud environments (ISO/IEC, 2022; NIST, 2024; Anica-Popa et al., 2024). However, this study extends existing research by demonstrating that cybersecurity assessment should distinguish between implemented security capabilities and those that can be independently verified through official technical documentation. By incorporating documented technical evidence as an explicit assessment criterion, the CECAF strengthens the objectivity and reproducibility of cybersecurity capability assessment.

Compared with previous cloud ERP research, the principal contribution of this study lies not in identifying additional cybersecurity controls but in providing a structured methodology for evaluating documented cybersecurity capabilities. While existing studies have primarily focused on cybersecurity risks, adoption challenges, governance issues, and conceptual security requirements, the CECAF integrates assessment domains, predefined evaluation criteria, documented technical evidence, and capability maturity levels into a single analytical framework. In doing so, it complements existing cybersecurity maturity research by enabling transparent, systematic, and comparable assessments across cloud ERP platforms (Liyanage et al., 2024; Rose et al., 2020).

The findings have several theoretical implications for cloud ERP cybersecurity research. First, the primary contribution of this study is the development of the CECAF, which addresses the identified research gap by providing a structured analytical framework integrating cybersecurity assessment domains, predefined assessment

criteria, documented technical evidence, and capability maturity levels into a unified evaluation methodology. While previous studies have primarily focused on cybersecurity risks, security controls, or challenges in cloud ERP adoption, the CECAF provides a systematic approach for evaluating cybersecurity capabilities using consistent, transparent assessment criteria. In this respect, it contributes to the growing body of research on cybersecurity capability maturity assessment by operationalising cybersecurity evaluation within the context of cloud ERP platforms (Brezavšček & Baggia, 2025).

Second, this study demonstrates the application of the CECAF through a real-world case research of Infor CSI. Rather than presenting the framework as a conceptual model, it shows how publicly available official technical documentation can be systematically analysed to produce an evidence-based cybersecurity capability profile. This demonstrates the practical feasibility and reproducibility of the proposed methodology and provides a foundation for future comparative studies across cloud ERP platforms.

Third, the study contributes methodologically by demonstrating that the transparency and completeness of official technical documentation directly influence the objectivity and reproducibility of cybersecurity capability assessment. Accordingly, cybersecurity maturity should be evaluated not only by implemented security mechanisms but also by the availability of verifiable technical evidence supporting those mechanisms. This complements recent research on cybersecurity capability maturity models by emphasising the importance of evidence-based assessment principles (Brezavšček & Baggia, 2025; Liyanage et al., 2024).

From a practical perspective, the CECAF provides organisations with a structured methodology for evaluating cybersecurity capabilities during cloud ERP selection, implementation, governance, and periodic security reviews. By applying consistent assessment domains and predefined capability maturity criteria, it enables transparent and comparable evaluations based on publicly available technical documentation, reducing reliance on marketing materials or subjective assessments and supporting more informed decision-making.

Although this study focused on Infor CSI, the CECAF was designed to be vendor-independent and can be applied to other cloud ERP platforms with sufficient official technical documentation. As a result, the framework provides a practical basis for benchmarking cybersecurity capabilities across cloud ERP solutions using a consistent, transparent, and reproducible assessment methodology.

Conclusion

This study achieved its objective by developing and demonstrating the CECAF for systematically evaluating cybersecurity capabilities in cloud ERP platforms. Using Infor CSI as a case research, the framework was applied to assess six cybersecurity domains based exclusively on publicly available official technical documentation. The results indicate a consistently high level of cybersecurity capability, with four domains achieving Level 4 (Managed) and two achieving Level 3 (Defined). More importantly, the findings demonstrate that an evidence-based assessment approach enables transparent and reproducible evaluation of cloud ERP cybersecurity capabilities.

By addressing the identified research gap, this study

makes three principal contributions. First, it develops the CECAF, a structured analytical framework for systematically evaluating cybersecurity capabilities in cloud ERP platforms. Second, it demonstrates the practical application of the framework through an evidence-based assessment of Infor CSI using publicly available technical documentation. Third, it highlights the methodological importance of transparent and comprehensive technical documentation for objective, reproducible, and consistent cybersecurity capability assessment.

From a practical perspective, the CECAF provides organisations with a structured methodology to support cloud ERP selection, implementation, governance, and periodic cybersecurity assessments. By applying consistent assessment domains and predefined capability maturity criteria, it enables transparent and comparable evaluations across cloud ERP platforms.

Several limitations should be acknowledged. First,

the study is based on a single cloud ERP case, limiting the generalisability of the findings. Second, the assessment relied exclusively on publicly available official technical documentation; as a result, proprietary cybersecurity mechanisms could not be evaluated. Finally, because cloud ERP platforms and their technical documentation continuously evolve, the findings represent documented cybersecurity capabilities at the time of the assessment.

Future research should apply the CECAF to additional cloud ERP platforms, including SAP S/4HANA Cloud, Microsoft Dynamics 365, Oracle Fusion Cloud ERP, and Odoo, to enable comparative cybersecurity assessments across vendors. Further validation through multiple case studies, expert evaluations, and longitudinal assessments would strengthen the framework and support the continued development of evidence-based methodologies for cloud ERP cybersecurity assessment.

Data Availability: Findings in this paper are based on publicly available technical documentation of Infor CSI (Infor, n.d.).

References

- Almorsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. *Journal of Cloud Computing*, 5(1), 38. <https://doi.org/10.1186/s13677-016-0066-2>
- Anica-Popa, L.-E., Vrîncianu, M., Pugna, I.-B., & Boldeanu, D.-M. (2024). Addressing cybersecurity issues in ERP systems: Emerging trends and challenges. *Proceedings of the International Conference on Business Excellence*, 18(1), 1306–1323. <https://doi.org/10.2478/picbe-2024-0108>
- Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing maturity models for IT management: A procedure model and its application. *Business & Information Systems Engineering*, 1(3), 213–222. <https://doi.org/10.1007/s12599-009-0044-5>
- Bertino, E. (2021). Zero Trust Architecture: Does It Help? *IEEE Security & Privacy*, 19(6), 95–99. <https://doi.org/10.1109/MSEC.2021.3091195>
- Brezavšček, A., & Baggia, A. (2025). Recent trends in information and cyber security maturity assessment: A systematic literature review. *Systems*, 13(1), 52. <https://doi.org/10.3390/systems13010052>
- Cloud Security Alliance. (2024). *Cloud Controls Matrix (CCM)*. Retrieved from <https://cloudsecurityalliance.org/research/cloud-controls-matrix>
- Demi, S., & Haddara, M. (2018). Do cloud ERP systems retire? An ERP lifecycle perspective. *Procedia Computer Science*, 138, 587–594. <https://doi.org/10.1016/j.procs.2018.10.079>

- Dwivedi, Y. K., Hughes, L., Coombs, C., et al. (2021). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, 57, 101994. <https://doi.org/10.1016/j.ijinfomgt.2019.08.002>
- Infor. (2020). *Infor Business Continuity Plan Overview*. Retrieved from <https://webassets.infor.com/images/Infor-Business-Continuity-Plan-Overview-April-2020.pdf>
- Infor. (2023). *Information Security Plan (Software as a Service)*. Retrieved from <https://dam.infor.com/api/public/content/94cc462111741dfb603ed08dbb0f254>
- Infor. (2024). *Data Privacy*. Retrieved from <https://www.infor.com/about/data-privacy>
- Infor. (n.d.). *Audit Logging Documentation*. Retrieved June 10, 2026, from <https://docs.infor.com/>
- Infor. (n.d.). *Federated Security*. Retrieved June 9, 2026, from <https://docs.infor.com/inforos/>
- Infor. (n.d.). *Infor ION API Administration Guide*. Retrieved June 10, 2026, from <https://docs.infor.com/ionapi/>
- Infor. (n.d.). *Infor OS API Gateway Administration Guide*. Retrieved June 8, 2026, from <https://docs.infor.com/inforos/>
- Infor. (n.d.). *Infor OS Security Administration Guide*. Retrieved June 10, 2026, from <https://docs.infor.com/inforos/>
- Infor. (n.d.). *Infor OS User Administration Guide*. Retrieved June 9, 2026, from <https://docs.infor.com/inforos/>
- Infor. (n.d.). *Infor Trust Center*. Retrieved June 10, 2026, from <https://trust.infor.com/>
- International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements. <https://www.iso.org/standard/27001.html>
- Ivanović, T., & Marić, M. (2021). Cloud ERP systems in digital transformation: Opportunities and challenges. *Strategic Management*, 26(4), 28–40. <https://doi.org/10.5937/StraMan2104028I>
- Khan, M. Y., Ab-Rahim, R., & Yeng, S. (2025). A conceptual overview of Enterprise Resource Planning systems. *International Journal of Academic Research in Business and Social Sciences*, 15(5). <https://doi.org/10.6007/IJARBS/v15-i5/25490>
- Khokrale, R. (2025). Cybersecurity in ERP-integrated supply chains: Risks and mitigation strategies. *The Eastasouth Journal of Information System and Computer Science*, 3(2). <https://doi.org/10.58812/esiscs.v3i02.869>
- Klaus, H., Rosemann, M., & Gable, G. G. (2000). What is ERP? *Information Systems Frontiers*, 2(2), 141–162. <https://doi.org/10.1023/A:1026543906354>
- Lee, Y., Lee, J., & Kim, S. (2024). Cybersecurity challenges and strategies in cloud ERP environments: A systematic literature review. *Journal of Enterprise Information Management*, 37(3), 742–768. <https://doi.org/10.1108/JEIM-07-2023-0283>
- Liyanage, L., Arachchilage, N. A. G., & Russello, G. (2024). SoK: Identifying limitations and bridging gaps of cybersecurity capability maturity models (CCMMs). arXiv. <https://doi.org/10.48550/arXiv.2408.16140>
- Llivisaca-Villazhañay, J., Paredes-Gualtor, J., Paredes-Valverde, M. A., & Ortiz-Crespo, A. (2025). Cloud ERP adoption and digital transformation in organisations: A systematic literature review. *Information Systems Frontiers*. Advance online publication. <https://doi.org/10.1007/s10796-025-10625-5>
- Mushtaq, S., Mohsin, M., & Mushtaq, M. M. (2025). A systematic literature review on the implementation and challenges of Zero Trust Architecture across domains. *Sensors*, 25(19), 6118. <https://doi.org/10.3390/s25196118>
- National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. U.S. Department of Commerce. <https://www.nist.gov/cyberframework>
- Paulk, M. C., Curtis, B., Chrissis, M. B., & Weber, C. V. (1993). Capability Maturity Model, Version 1.1. *IEEE Software*, 10(4), 18–27. <https://doi.org/10.1109/52.219617>
- Qazi, A., Khorram-Manesh, A., Vaziri, S., & Dimitrov, D. (2026). Cybersecurity capability assessment in cloud ERP systems: A maturity model approach. *Computers & Security*, 142, Article 103821. <https://doi.org/10.1016/j.cose.2025.103821>
- Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). <https://doi.org/10.6028/NIST.SP.800-207>
- Singh, U. K., & Sharma, A. (2021). Cloud computing security framework based on shared responsibility models: Cloud computing. In *Cyber-Physical, IoT, and Autonomous Systems in Industry 4.0* (pp. 39-55). CRC Press.
- Sternad Zabukovšek, S., & Bobek, S. (2025). Using the technology acceptance model for factors influencing acceptance of enterprise resource planning solutions. In *Encyclopedia of Information Science and Technology*, Sixth Edition (pp. 1-28). IGI Global Scientific Publishing.
- Sunyaev, A. (2020). *Internet computing: Principles of distributed systems and emerging internet-based technologies* (2nd ed.). Springer. <https://doi.org/10.1007/978-3-030-34957-8>
- Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). SAGE Publications.

Razvoj ocenjevalnega okvira kibernetске varnosti za ERP-rešitve v oblaku (CECAF): ocenjevanje zmogljivosti kibernetске varnosti oblačnih ERP-platform

Izvleček

Namen raziskave je razviti okvir za ocenjevanje kibernetске varnosti ERP-rešitev v oblaku (CECAF), ki omogoča sistematično vrednotenje zmogljivosti kibernetске varnosti oblačnih ERP-platform. Okvir je bil razvit s sintezo znanstvene literature, mednarodno priznanih standardov kibernetске varnosti, načel ocenjevanja zrelosti zmogljivosti kibernetске varnosti in specifičnih zahtev kibernetске varnosti ERP-rešitev v oblaku. Njegova uporabnost je prikazana na primeru ocenjevanja rešitve Infor CloudSuite na podlagi javno dostopne uradne tehnične dokumentacije. Ugotovitve kažejo, da CECAF omogoča strukturirano, pregledno in ponovljivo vrednotenje zmogljivosti kibernetске varnosti na več ocenjevalnih področjih. Raziskava prispeva k razvoju področja z uvedbo analitičnega ocenjevalnega okvira, prilagojenega ERP-platformam v oblaku, ter poudarja metodološki pomen dokumentiranih tehničnih dokazov za objektivno ocenjevanje zmogljivosti kibernetске varnosti. Okvir zagotavlja praktične smernice za ocenjevanje kibernetске varnosti in primerjalno vrednotenje ERP-platform v oblaku.

Ključne besede: ERP-rešitve v oblaku; kibernetска varnost; okvir za ocenjevanje kibernetске varnosti; ocenjevanje zmogljivosti kibernetске varnosti; ocenjevanje na podlagi dokazov; zrelost kibernetских zmogljivosti.