Modernizing Legacy ABAP to Clean-Core SAP: A Measurable Framework for Secure and Human-Centered ERP Transformation in U.S. Small and Mid-Sized Manufacturing

Azlan Ahmed[1], Syeda Tanjina Hasan[2]

[1]Sr Lead SAP Technical Consultant, SAP, Sir Syed University of Engineering and Technology, Pakistan
[2]Data Science Engineer, Data Science & AI, BRAC University, Bangladesh

Abstract

Small and mid-sized manufacturers that have operated SAP environments for many years often carry a substantial layer of custom ABAP code, interfaces, enhancements, and process-specific modifications. Those assets may encode valuable business knowledge, but they can also increase technical debt, complicate upgrades, weaken architectural transparency, and make security and skills management more difficult. At the same time, SAP's clean-core direction encourages organizations to preserve a stable ERP core, use standard capabilities where feasible, and place necessary differentiation in governed, upgrade-stable extension patterns. Existing studies provide important insights into ERP customization, technical debt, cloud ERP, digital transformation, cybersecurity, user resistance, human-centered manufacturing, and SME maturity; however, these streams are rarely integrated into a single modernization framework for resource-constrained manufacturing organizations. This paper develops a measurable framework for moving from legacy ABAP dependence toward secure and human-centered clean-core SAP. The study uses a structured integrative review of peer-reviewed ERP, information-systems, manufacturing, digital-transformation, and cybersecurity research, complemented by current SAP and U.S. National Institute of Standards and Technology guidance. The proposed framework contains six connected stages: legacy baseline, ABAP rationalization, clean-core architecture, security-by-design, human readiness, and measurable outcomes, with governance and continuous measurement spanning all stages. A multidimensional scorecard is proposed across technical cleanliness, security and resilience, human readiness, operational performance, and governance and maintainability. The paper also defines practical indicators such as custom-code retirement, extensibility risk, upgrade adaptation effort, security finding closure, user proficiency, process cycle time, defect escape, and change lead time. The framework is intended for U.S. small and mid-sized manufacturers that need a pragmatic modernization path without assuming that all customization should be eliminated or that technical migration alone constitutes transformation. The central contribution is a socio-technical measurement logic that makes clean-core modernization testable, governable, and accountable to both system and workforce outcomes.

Keywords: SAP; ABAP; Clean Core; SAP S/4HANA; ERP Modernization; Technical Debt; Cybersecurity; Human-Centered Transformation; Manufacturing SMEs; Digital Transformation

1. Introduction

Enterprise resource planning (ERP) systems provide the process and information backbone through which manufacturing firms coordinate finance, purchasing, inventory, production, sales, maintenance, quality, and related activities. The classical ERP literature emphasizes integration as the central value proposition: information that would otherwise be fragmented across functions becomes part of a common process architecture [1], [2]. Yet integration also creates path dependence. Once an ERP system has been used for many years, local business requirements, acquired-company processes, regulatory interpretations, emergency fixes, and user preferences can become embedded in custom code and interfaces. The result is often a technically functional but increasingly difficult-to-change enterprise system.

In SAP landscapes, ABAP has historically been the principal language for implementing company-specific reports, forms, transactions, enhancements, interfaces, and business logic. Custom ABAP is not inherently undesirable. It can support genuine differentiation and close gaps between standard ERP functionality and a firm's operating model. The problem emerges when the cumulative customization portfolio becomes weakly documented, tightly coupled to internal SAP objects, duplicated across units, rarely used, or expensive to test after each platform change. Research on ERP customization has long shown that customization creates maintenance consequences and that the trade-off between fit and long-term complexity must be actively governed [5, 6, 7, 8, 9]. Technical-debt research reinforces the same principle: short-term delivery decisions can create liabilities that surface later through reliability, maintenance, and change costs [4].

This issue is especially important as organizations move from older SAP Business Suite or ECC environments toward SAP S/4HANA and cloud-oriented operating models. Current SAP guidance frames clean core as an approach to keeping processes, extensions, data, integrations, and operations sufficiently standardized and decoupled to support ongoing innovation and upgradeability [39, 40, 41, 42, 43, 44]. Clean core does not mean 'zero customization.' It means that customization is justified, architected through appropriate extension points, monitored, and prevented from creating unnecessary coupling to the core. Modern ABAP therefore remains relevant, but the preferred technical patterns increasingly emphasize released APIs, ABAP Cloud, side-by-side extensions, and governed extensibility rather than unrestricted modification of standard objects [40], [41].

For small and mid-sized manufacturers, the transformation problem is broader than architecture. These firms often face tighter capital budgets, smaller internal IT teams, limited specialist capacity, operational dependence on a small number of key employees, and less tolerance for production disruption than large enterprises. Studies of ERP implementation and digital transformation in SMEs consistently identify management support, skills, implementation structure, process fit, communication, training, and change readiness as major determinants of outcomes [10, 11, 12, 13, 14, 15], [20, 21, 22, 23, 24]. Manufacturing research adds a further requirement: technology modernization must be aligned with human work, resilience, safety, and the practical realities of factories rather than treated as a purely technological exercise [25, 26, 27, 28, 29].

Security is equally inseparable from modernization. ERP systems concentrate high-value financial, customer, supplier, production, and employee data, while manufacturing environments often connect enterprise IT to operational technology (OT). A modernization that introduces APIs, cloud services, new identities, and extension platforms can reduce some legacy risks but also create new attack surfaces. Current standards-based research and NIST guidance emphasize governance, identity, access control, protection, detection, response, recovery, segmentation, and OT-aware risk treatment [33, 34, 35, 36, 37].

Secure clean-core modernization therefore requires security requirements to be designed into architecture and migration decisions rather than added after functional deployment.

Against this background, the paper addresses a practical and research problem: how can a U.S. small or mid-sized manufacturer determine whether its movement from legacy ABAP toward clean-core SAP is actually improving the enterprise system? A technically successful conversion can still fail if users create shadow processes, security controls are weakened, developers cannot support the new model, or maintenance costs simply move from the core to an unmanaged extension layer. Conversely, modernization can create substantial value even when some custom ABAP remains, provided that it is necessary, governed, secure, maintainable, and measurable. The study therefore develops a framework that links technical remediation to security, human readiness, operational performance, and governance outcomes.

2. Research Problem, Objectives, and Research Questions

The research problem is the absence of an integrated measurement logic for clean-core SAP modernization that simultaneously addresses legacy custom-code exposure, architectural decoupling, cybersecurity, workforce readiness, and business-process outcomes in smaller manufacturing organizations. Existing research provides strong pieces of this problem but typically treats them separately: customization studies focus on fit and maintenance [5, 6, 7, 8, 9]; ERP success research focuses on adoption, implementation, and performance [10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20]; manufacturing digital-transformation research focuses on readiness, maturity, human centricity, and SME constraints [21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32]; and cybersecurity literature focuses on control and risk [33, 34, 35, 36, 37]. Current SAP guidance provides detailed technical direction for clean-core extensibility and custom-code migration [38, 39, 40, 41, 42, 43, 44], but a vendor architecture model is not by itself an organizational transformation model.

This paper has four objectives: (1) synthesize the literature that explains why legacy customization becomes a modernization constraint; (2) define clean-core SAP modernization as a socio-technical transformation rather than a code-removal exercise; (3) integrate security and human-centered requirements into the modernization path; and (4) propose measurable indicators that allow organizations to establish a baseline, evaluate progress, and sustain clean-core discipline after migration.

The analysis is guided by four research questions. RQ1 asks which forms of legacy ABAP and ERP customization create the greatest modernization burden and why. RQ2 asks how clean-core principles can be translated into practical architectural decisions without assuming that all differentiation should be eliminated. RQ3 asks which security and human factors should be designed into modernization for small and mid-sized manufacturers. RQ4 asks how modernization success can be measured across technical, security, human, operational, and governance dimensions.

3. Conceptual Background

3.1 Legacy ABAP, ERP Customization, and Technical Debt

ERP customization exists because standard software and organizational requirements rarely match perfectly. Light [5] showed early that customization has direct implications for ERP maintenance, while Nah, Faja, and Cata [6] documented the distinctive maintenance characteristics of ERP packages. Later work has continued to treat customization as a decision problem rather than a binary choice. Hustad and Stensholt [8] propose a framework for deciding among customization options, while Hansen, Haddara, and Langseth [9] examine customization in cloud ERP environments. Abendroth, Bender, and Gronau [7] show an important architectural evolution: ERP customization has increasingly moved away from direct code modification toward interface- and integration-based approaches as cloud ERP constrains access to the core.

For SAP customers, legacy ABAP can be understood as a portfolio rather than a language problem. The portfolio can include custom Z/Y programs, enhancements, modified standard objects, custom tables, forms, batch jobs, interfaces, reports, and code that reads or writes data through internal structures. Some of this code may remain business-critical; some may duplicate capabilities now available in standard S/4HANA; some may no longer be used. A rational modernization program therefore needs evidence about usage, dependency, business criticality, technical quality, and replacement options before deciding what to remove or rebuild.

Technical debt provides a useful lens because it explains why locally rational decisions can accumulate into enterprise-wide constraints. Ramasubbu and Kemerer [4] show that technical debt in enterprise software is associated with reliability implications. In ERP, the liability is amplified by integration: a small customization may affect a process chain, authorization model, interface, data object, or downstream report. The modernization objective should therefore be reduction of unmanaged coupling and avoidable debt, not indiscriminate elimination of all custom code.

3.2 From SAP S/4HANA Conversion to Clean-Core Transformation

A platform conversion and an enterprise transformation are related but different. Conversion moves the technical system to a new platform; transformation changes how the organization designs processes, extensions, governance, security, and work. Haddara and Elragal [3] argued that ERP's future should be understood in relation to lessons from earlier generations, including the organizational consequences of enterprise-system decisions. That warning is relevant to S/4HANA: migrating legacy customization unchanged can preserve the very complexity that modernization is intended to reduce.

SAP's maintenance strategy creates an additional planning context. SAP continues to support S/4HANA as a long-term strategic platform and has communicated maintenance horizons for Business Suite 7 and S/4HANA [38]. This makes modernization a governance question as well as a technical deadline. Organizations need to determine which legacy processes should become standard, which extensions remain strategically necessary, and which dependencies should be removed before they become urgent upgrade blockers.

Current clean-core guidance describes cleanliness across processes, extensions, data, integrations, and operations [39]. For extensibility, SAP's current classification distinguishes more upgrade-stable patterns from more tightly coupled patterns. Released stable APIs and extension points represent the preferred end of the spectrum, while modifications, direct table writes, and similar techniques represent the highest clean-core concern [41]. SAP's ABAP extensibility guidance additionally distinguishes on-stack and side-by-side options and positions ABAP Cloud as a key mechanism for upgrade-stable development [40]. These principles support a risk-based modernization logic: the architectural question is not whether a custom object exists, but how it is coupled, why it exists, and how safely it can evolve.

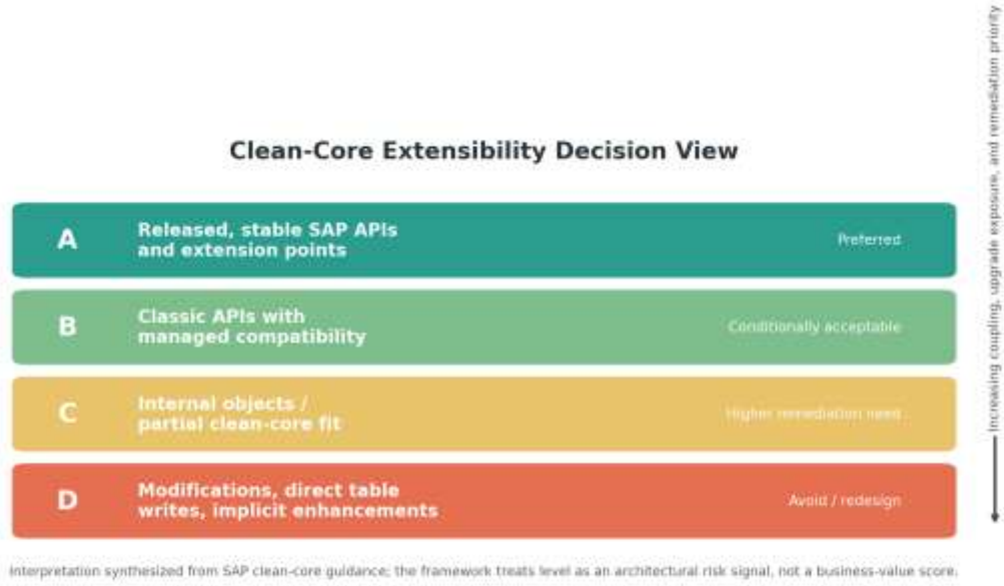

Figure 1: Clean-core extensibility decision view synthesized from current SAP guidance [39, 40, 41].

3.3 Security as a Modernization Design Constraint

Clean-core transformation changes trust boundaries. New APIs, cloud services, identity providers, integration middleware, developer tooling, and side-by-side applications can improve architectural separation while increasing the number of interfaces that require authentication, authorization, monitoring, and lifecycle control. Security should therefore be measured as an architectural property of the target state rather than treated as a final compliance checklist.

Qazi, Arshad, and Jadoon [33] demonstrate the value of standards-based ERP security assessment by mapping ERP security evaluation to NIST and ISO controls. NIST CSF 2.0 emphasizes six functions - Govern, Identify, Protect, Detect, Respond, and Recover - and explicitly strengthens governance as a core cybersecurity function [34]. For manufacturers, NIST SP 800-82 Rev. 3 adds OT-specific considerations, including the need to account for safety, availability, deterministic operations, and industrial constraints [35]. Guidance directed at smaller manufacturers further emphasizes practical standards adoption and segmentation approaches that can be implemented in environments with constrained resources [36], [37]. Within SAP modernization, these principles translate into concrete requirements: least-privilege role design, separation of duties, secure service identities, controlled API exposure, transport and change governance, logging, vulnerability remediation, data protection, backup and recovery, and clear ownership of extensions. A 'clean' core that is poorly governed or weakly secured is not a successful modernization outcome.

3.4 Human-Centered ERP Transformation

ERP projects alter work, decision rights, information visibility, and skill requirements. Critical-success-factor research repeatedly identifies top-management support, training, communication, project management, user involvement, and change management as central to ERP outcomes [10], [13]. User-resistance research shows that resistance is not merely an attitude problem; it emerges from perceived losses, poor fit, uncertainty, habits, and implementation choices [14]. Technology-acceptance research in ERP environments similarly links communication, training, shared beliefs, usefulness, and ease of use to

system adoption [15].
The human-centered manufacturing literature provides a complementary perspective. Lu et al. [26] frame human-centric manufacturing as a key direction for Industry 5.0, while Zhang et al. [27] synthesize human-centered smart manufacturing as a shift away from purely technology-centric optimization. Nazarejova, Soltysova, and Rudeichuk [28] identify requirements and barriers for human-centered SMEs, and Zincume and Maier [29] use a human-technology-organization perspective to examine the future of work in SME factories. These studies imply that ERP modernization should explicitly measure whether people can understand, use, challenge, and sustain the new system.
For ABAP teams, the human dimension includes developer reskilling. A developer who is highly productive in classic ABAP may need new capabilities in released APIs, ABAP Cloud, test automation, service-based integration, BTP, and clean-core governance. For business users, human-centered modernization means involving process owners in fit-to-standard decisions, validating usability and exception handling, providing role-based training, and monitoring whether users return to spreadsheets or manual workarounds after go-live.

3.5 Why the U.S. Small and Mid-Sized Manufacturing Context Matters

The SME literature consistently cautions against transferring large-enterprise transformation assumptions directly to smaller firms. Ahmad and Pinedo Cuenca [10] identify critical ERP success factors in SMEs; Alaskari, Pinedo-Cuenca, and Ahmad [11] provide an implementation framework developed around SME conditions; and Sørheller et al. [12] show that cloud ERP adoption introduces intertwined technical and socio-technical concerns such as fit, integration, migration, organizational change, data security, and reliability. These factors are especially consequential for manufacturers, where ERP transactions are closely connected to material flow, production schedules, quality, maintenance, and delivery commitments.
Manufacturing-SME digital-transformation research reinforces the resource constraint. Ghobakhloo et al. [22] synthesize drivers and barriers to Industry 4.0 adoption among manufacturing SMEs, while Krishnan [23] organizes the challenges and benefits of smart-manufacturing transformation. Sagala and Ori [21] show that SME digital-transformation success depends on organizational baseline conditions and continuous capability development. Njah et al. [24] respond to similar limitations by developing a manufacturing-SME digital maturity model with actionable indicators. Latino [25] extends maturity thinking toward Industry 5.0 and human centricity. Together, these studies support a modernization framework that is modular, evidence-based, and sensitive to resource capacity rather than assuming an unlimited transformation program.
The U.S. manufacturing context also requires attention to cybersecurity and operational continuity. NIST's Manufacturing Extension Partnership and manufacturing-focused cybersecurity resources are explicitly aimed at improving the competitiveness and resilience of small and medium-sized U.S. manufacturers [36], [37]. Accordingly, the framework proposed here treats security, workforce capability, and measurable operational continuity as first-class modernization dimensions.

4. Literature Review and Research Gap

The literature was organized into six evidence streams: ERP integration and customization; technical debt and maintenance; ERP implementation and success; SME and manufacturing digital transformation; human-centered manufacturing; and ERP/manufacturing cybersecurity. A seventh stream - current SAP clean-core and custom-code guidance - was used to translate the research findings into SAP-specific architectural choices. Table 1 summarizes representative evidence and shows why no single stream is sufficient on its own.

Evidence stream	What the literature establishes	Representative references	Implication for this study
ERP integration	Integrated processes create value and cross-functional dependency.	[1, 2, 3]	Preserve process integrity while removing avoidable legacy dependency.
Customization	Fit gains can increase maintenance and governance demands.	[5, 6, 7, 8, 9]	Classify objects by necessity, use, coupling, and replacement path.
Technical debt	Accumulated debt can impair reliability and future change.	[4]	Baseline and measure debt retirement.
ERP success	Training, participation, change management, fit, and measurement affect outcomes.	[10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20]	Include human readiness and outcome KPIs.

Table 1A: Literature synthesis - ERP, customization, debt, and implementation evidence.

Evidence stream	What the literature establishes	Representative references	Implication for this study
SME transformation	SMEs face distinct resource, capability, and maturity constraints.	[21, 22, 23, 24, 25]	Use staged modernization and proportional governance.
Human-centered manufacturing	Technology should augment human capability and work design.	[26, 27, 28, 29]	Measure proficiency, usability, acceptance, and skill transition.
Cybersecurity	Standards-based and OT-aware controls improve risk treatment.	[33, 34, 35, 36, 37]	Embed security baselines and quality gates.
SAP clean core	Current guidance emphasizes upgrade-stable extensions, analysis, and measurement.	[38, 39, 40, 41, 42, 43, 44]	Translate research into SAP-specific architecture and evidence.

Table 1B: Literature synthesis - SME, human, security, and SAP clean-core evidence.

4.1 Research Gap

The central gap is not an absence of research on SAP, ERP modernization, SMEs, security, or human-centered transformation. The gap is fragmentation across these literatures. Customization research explains the maintenance consequences of modifying enterprise systems, but it generally does not provide a current clean-core SAP target architecture [5, 6, 7, 8, 9]. SAP guidance defines current extension patterns and tools but is primarily architectural and vendor-specific rather than a complete socio-technical transformation theory [39, 40, 41, 42, 43, 44]. ERP-success and digital-transformation research identifies change, skills, adoption, governance, and performance factors but rarely operationalizes them for legacy ABAP remediation [10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24], [30], [31]. Human-centered manufacturing research provides strong principles for worker-centered transformation but does not directly connect them to ERP clean-core decisions [26, 27, 28, 29]. Cybersecurity standards offer robust control structures but do not specify how legacy custom-code rationalization should be prioritized [33, 34, 35, 36, 37].

Accordingly, limited research integrates five questions in one measurable framework: Which legacy customizations should be retired or retained? Which clean-core extension pattern should replace tightly coupled code? Which security controls must be evidenced during the transition? How should developer and user readiness be assessed? Which technical and business indicators demonstrate that the new architecture is actually easier, safer, and more effective to operate? The gap is especially consequential for U.S. small and mid-sized manufacturers, where transformation must be achieved with constrained resources and minimal disruption to production. This study addresses that gap through an integrative, measurable framework rather than by claiming a universal 'best' migration path.

5. Methodology

This study uses a structured integrative literature-review and conceptual-framework-development method. An integrative review is appropriate because the research question crosses several mature and emerging literatures that use different methods, units of analysis, and outcome measures. A formal meta-analysis would not be appropriate: ERP customization studies, human-centered manufacturing research, cybersecurity standards, and SAP architecture guidance do not report a common effect size that could be meaningfully pooled.

Evidence was selected from peer-reviewed journal and conference literature in ERP, information systems, manufacturing systems, digital transformation, and cybersecurity, together with authoritative U.S. government and SAP technical sources. The review prioritizes recent work where concepts are rapidly changing, particularly clean-core extensibility, manufacturing digital maturity, and ERP security. Older studies were retained when they provide foundational constructs that remain directly relevant, including ERP integration, customization maintenance, technical debt, user acceptance, ERP success, and implementation critical-success factors [1, 2, 3, 4, 5, 6], [13, 14, 15, 16, 17, 18].

The synthesis followed four analytical steps. First, the literature was coded for the problem it addresses: customization burden, architectural modernization, security, human/organizational readiness, SME/manufacturing context, or measurement. Second, recurring constructs were mapped to modernization decisions. Third, current SAP guidance was used to translate general constructs such as coupling and technical debt into SAP-specific categories such as custom-code usage analysis, released APIs, ABAP Cloud, side-by-side extensibility, and clean-core classification [39, 40, 41, 42, 43, 44]. Fourth, the constructs were organized into a staged framework and a KPI dictionary. The proposed indicators are therefore design propositions derived from the literature; they are not presented as empirically validated universal thresholds.

To protect validity, the paper does not fabricate case-study outcomes, survey responses, company performance percentages, or migration statistics. Where the literature does not establish a universal benchmark, the framework requires each organization to set a baseline and compare post-modernization performance against its own verified evidence. This makes the framework suitable for future empirical validation through case studies, longitudinal SAP programs, or multi-firm surveys.

6. Findings from the Evidence Synthesis

6.1 Modernization Value Begins with Rationalization, Not Conversion

The first finding is that migration effort should not be equated with modernization value. A system conversion can move legacy code to S/4HANA while preserving obsolete functionality, duplicated logic, and tight coupling. Customization research suggests that the maintenance consequence depends on what is customized and how [5, 6, 7, 8, 9]. SAP's custom-code migration tooling follows the same logic by supporting usage-based analysis and S/4HANA checks before adaptation [42, 43, 44]. The economically relevant question is therefore: what percentage of the custom portfolio remains justified after business and usage review?

A disciplined rationalization step classifies each object into four actions: retire, replace, refactor, or retain. Retire applies to unused or obsolete objects. Replace applies where standard S/4HANA functionality or a supported product can meet the requirement. Refactor applies where the business requirement remains valid but the implementation should move to a cleaner extension pattern. Retain applies where the existing implementation is justified, technically acceptable, and monitored. This logic is deliberately different from 'rewrite everything,' which can create cost and risk without proportional value.

6.2 Clean Core Is a Governance Capability

The second finding is that clean core is not a one-time architecture state. It is a governance capability. Even a well-designed target system can become heavily coupled again if teams lack extension standards, architecture review, API discipline, lifecycle ownership, or measurement. SAP's current guidance explicitly connects clean core with quality gates and monitoring [39], [44]. The research literature similarly shows that ERP outcomes depend on organizational capabilities and sustained governance rather than software features alone [13], [19], [20].

For this reason, the proposed framework treats clean-core compliance as a recurring decision process. Each new requirement should answer: Is there a standard process? Is the differentiation strategically necessary? Is there a released extension point or API? Can the requirement be implemented on-stack with ABAP Cloud or side-by-side where appropriate? What security boundary is created? Who owns lifecycle support? How will the extension be tested against upgrades? The target is controlled differentiation, not architectural purity for its own sake.

6.3 Human Readiness and Security Are Leading Indicators, Not Afterthoughts

The third finding is that security and human readiness should be treated as leading indicators of modernization quality. If they are measured only after go-live, the program detects failure late. ERP adoption studies show that training, communication, perceived usefulness, user involvement, and change management shape whether new systems become embedded in work [13, 14, 15, 16]. Human-centered manufacturing research further shows that people, technology, and organization must be designed together [26, 27, 28, 29].

Security has the same temporal logic. Identity architecture, API authorization, segregation of duties, logging, and recovery design cannot be effectively retrofitted after dozens of extensions have been deployed. NIST CSF 2.0's Govern function supports explicit ownership and risk decisions before technical implementation [34]. For manufacturing, OT security guidance adds the need to protect availability and safety while changing enterprise connectivity [35]. Therefore, the framework uses pre-go-live security and proficiency gates as conditions for scale-up.

6.4 Measurement Must Be Multidimensional

The fourth finding is that no single metric can represent modernization success. Counting the number of migrated programs rewards activity rather than outcomes. Counting the number of removed programs can be equally misleading if critical functionality is lost or recreated elsewhere as ungoverned shadow IT. ERP-success research has long used multiple dimensions of system quality, information quality, user outcomes, and organizational benefits [16, 17, 18]. Manufacturing maturity research likewise uses multidimensional assessment because readiness is distributed across technology, organization, people, and processes [24], [25].

A defensible scorecard therefore needs at least five domains: technical cleanliness, security and resilience, human readiness, operational performance, and governance and maintainability. An organization may weight these differently according to risk and business priorities, but it should not omit a domain simply because it is difficult to measure.

7. Proposed Measurable Framework

Figure 2 presents the proposed six-stage modernization framework. The stages are sequential enough to support governance but iterative enough to accommodate real projects. A manufacturer can pilot one process domain, learn from the evidence, and repeat the cycle rather than undertaking an all-at-once transformation.

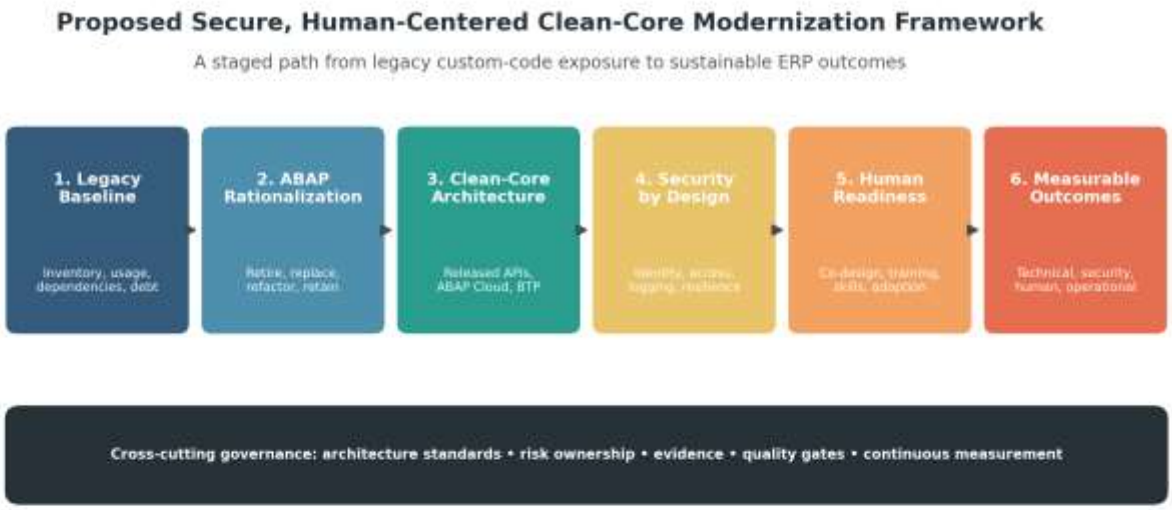

Figure 2: Proposed measurable framework for secure and human-centered clean-core SAP modernization. Source: authors' synthesis based on [4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15], [21, 22, 23, 24, 25, 26, 27, 28, 29], and [33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44].

7.1 Stage 1 - Establish the Legacy Baseline

The baseline stage creates the evidence against which progress will be judged. It inventories custom code, enhancements, interfaces, forms, batch jobs, modifications, security dependencies, critical process links, and ownership. Usage evidence is essential because object counts alone do not indicate business value.

The baseline should record at minimum: active versus inactive custom objects; objects with no recent usage evidence; criticality; dependency on internal SAP structures; test coverage where available; current upgrade adaptation effort; recurring defects; key privileged roles; major interfaces; user groups; and current process performance. SAP custom-code analysis and migration tools can support technical discovery, while business owners validate functional necessity [42, 43, 44].

7.2 Stage 2 - Rationalize the ABAP Portfolio

Rationalization converts inventory into decisions. Each object or functional cluster receives a disposition: retire, replace, refactor, or retain. Business criticality prevents technically convenient but operationally harmful deletion. Usage evidence prevents teams from preserving code merely because it has existed for years. Architecture and security assessment identify tightly coupled or risky implementations that should be prioritized for refactoring. The output is a modernization backlog ranked by business value, clean-core exposure, security risk, and expected effort.

7.3 Stage 3 - Select a Clean-Core Architecture

The target architecture applies fit-to-standard first and uses controlled extension patterns where differentiation remains necessary. Current SAP guidance supports released stable APIs and extension points as the preferred end of clean-core extensibility, with ABAP Cloud and BTP-based patterns providing upgrade-stable options for different scenarios [39, 40, 41]. The framework does not prescribe one extension technology for every requirement. Instead, it requires an architecture decision record that explains why the selected pattern is appropriate, what it depends on, how it will be tested, and who owns it.

7.4 Stage 4 - Secure by Design

Security-by-design maps each modernization component to risk ownership and verifiable controls. Required evidence may include role design and segregation-of-duties review, service-identity ownership, API authentication and authorization tests, encryption settings, transport approvals, vulnerability scan results, logging coverage, backup and recovery tests, and incident-response ownership. The security baseline should align to a recognized control framework such as NIST CSF 2.0, supplemented by OT-specific considerations where ERP integration reaches production environments [33, 34, 35, 36, 37].

7.5 Stage 5 - Build Human Readiness

Human readiness is assessed for both users and technical staff. User readiness includes task proficiency, perceived process fit, usability issues, support demand, exception-handling confidence, and evidence of workaround behavior. Technical readiness includes developer capability in clean-core patterns, code quality, testing, API design, authorization, and operational support. Training completion by itself is not sufficient; the framework favors proficiency and task-performance evidence because attendance does not prove capability [13, 14, 15, 16].

7.6 Stage 6 - Measure Outcomes and Sustain Governance

The final stage compares post-change evidence with the baseline and determines whether modernization should be scaled, adjusted, or paused. The measurement cadence should include release-level technical indicators, periodic security control evidence, user and support indicators, and business-process outcomes. Governance continues after the migration because new extensions and new process requests can recreate technical debt. Clean-core quality gates and ongoing monitoring therefore become part of normal SAP lifecycle management rather than a temporary project activity [39], [44].

Framework stage	Decision question	Example evidence	Primary output
Legacy baseline	What exists, what is used, and what creates dependency?	Custom object inventory; usage; criticality; interfaces; privileged roles; upgrade effort	Verified baseline and modernization backlog
ABAP rationalization	What should be retired, replaced, refactored, or retained?	Retirement ratio; duplication; business criticality; remediation priority	Smaller, justified custom portfolio
Clean-core architecture	How should remaining differentiation be implemented?	Extension classification; released API use; coupling; architecture exceptions	Upgrade-stable target architecture
Security by design	Are new trust boundaries governed and testable?	Control closure; privileged access; API/auth findings; logging; recovery tests	Risk acceptance and security evidence
Human readiness	Can people use and sustain the new model?	Task proficiency; adoption; support demand; shadow-process use; developer skills	Go-live readiness and capability plan
Measurable outcomes	Did the change improve the system and business process?	Upgrade effort; defects; lead time; downtime; cycle time; cost; user outcomes	Scale/adjust decision and continuous-improvement backlog

Table 2: Decision logic and evidence required at each modernization stage.

8. Measurement Model and KPI Dictionary

The framework proposes a five-domain scorecard. Let T represent technical cleanliness, S security and resilience, H human readiness, O operational performance, and G governance and maintainability. Each domain is normalized to a common 0-100 scale using organization-specific evidence. A composite modernization score can then be expressed as $M = wT(T) + wS(S) + wH(H) + wO(O) + wG(G)$, where the weights sum to 1. The paper deliberately does not prescribe universal weights. A manufacturer with high cyber-physical exposure may place greater weight on security and resilience, while a firm facing severe upgrade delay may prioritize technical cleanliness and maintainability. The governance requirement is that weights, thresholds, and data sources are documented before results are evaluated.

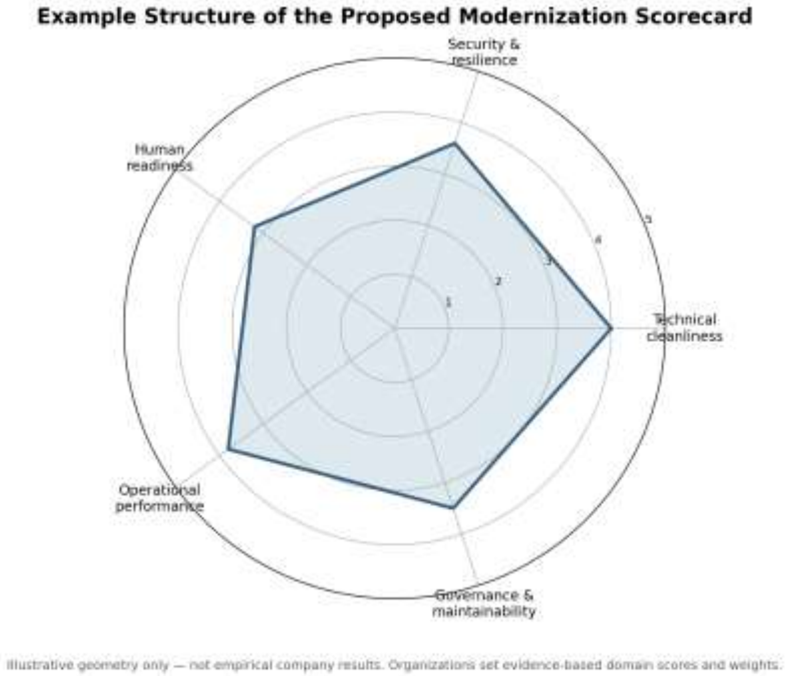

Figure 3: Illustrative structure of the five-domain modernization scorecard. The geometry is illustrative, not company performance data.

Domain	KPI	Definition / formula	Data source	Interpretation
Technical	Legacy-object retirement ratio	Retired legacy objects / baseline legacy objects	Custom-code inventory; usage evidence	Shows reduction of unnecessary legacy footprint; interpret with criticality.
Technical	Clean-core alignment rate	Objects meeting approved extension policy / assessed active custom objects	Architecture review; clean-core classification	Tracks movement toward governed, upgrade-stable patterns.
Technical	Upgrade adaptation effort	Person-hours required for custom-code adaptation per release or upgrade	Change records; project time logs	Tests whether architectural decoupling reduces future maintenance.
Technical	ATC / quality finding density	Relevant unresolved findings per 100 active custom objects	ABAP Test Cockpit / quality tools	Provides a normalized technical-quality signal.
Security	Security-control closure rate	Closed required controls / required controls before release	GRC, security testing, risk register	Measures whether security gates are actually satisfied.

Domain	KPI	Definition / formula	Data source	Interpretation
Security	Privileged-access exception rate	Unresolved privileged-access exceptions / privileged roles reviewed	IAM/GRC evidence	Highlights authorization debt and segregation-of-duties exposure.
Security	Mean time to remediate critical findings	Average elapsed time from verified critical finding to closure	Security ticketing / vulnerability records	Measures response discipline and risk ownership.
Security	Recovery evidence rate	Critical interfaces/services with tested recovery evidence / critical services	BCP/DR records	Connects modernization to operational resilience.

Table 3A: Technical and security KPIs for measurable clean-core modernization.

Domain	KPI	Definition / formula	Data source	Interpretation
Human	Task proficiency rate	Users meeting defined task proficiency threshold / users assessed	Role-based assessments; simulations	More meaningful than training attendance alone.
Human	Support demand after release	ERP support tickets per 100 active users or transactions	Service desk	Signals usability, training, or process-fit problems.
Human	Shadow-process incidence	Verified spreadsheet/manual workarounds for in-scope process	Process audit; user interviews	Detects nominal adoption without real process adoption.
Human	Developer clean-core capability	Technical staff passing defined architecture/coding proficiency criteria	Skills matrix; code review	Measures sustainment capacity after consultants leave.
Operational	Process cycle time	Elapsed time for selected end-to-end process	ERP process logs	Tests whether modernization improves or harms flow.
Operational	Defect escape rate	Production defects / total defects detected for release	Testing and incident records	Tests release quality and regression risk.
Operational	Change lead time	Elapsed time from approved requirement to production	ALM/change records	Tests whether cleaner architecture improves responsiveness.

Domain	KPI	Definition / formula	Data source	Interpretation
Operational	Unplanned ERP-related downtime	Verified downtime attributable to in-scope ERP/extension changes	Monitoring / incident records	Protects manufacturing continuity.

Table 3B: Human and operational KPIs for measurable clean-core modernization.

Domain	KPI	Definition / formula	Data source	Interpretation
Governance	Architecture exception aging	Average age of approved but unresolved clean-core exceptions	Architecture decision register	Prevents temporary exceptions from becoming permanent debt.
Governance	Evidence completeness	Required modernization controls/KPIs with current evidence / total required	Audit evidence repository	Measures governance reliability and auditability.
Governance	New technical-debt intake	New exceptions or debt items created per release	Backlog; architecture review	Tests whether debt is being recreated after cleanup.

Table 3C: Governance KPIs for measurable clean-core modernization. Thresholds should be set from organizational baselines rather than treated as universal benchmarks.

8.1 Measurement Principles

Four measurement principles are important. First, baseline before intervention. Without a baseline, improvement claims become retrospective narratives. Second, distinguish activity from outcome. Number of programs converted, training sessions delivered, or controls documented are activities; upgrade effort, proficiency, defect rate, process cycle time, and security closure are outcomes or outcome-proximate indicators. Third, normalize where size matters. Findings per 100 custom objects or tickets per 100 users are often more interpretable than raw totals. Fourth, triangulate technical evidence with business and user evidence. A technically clean system that creates slower work or extensive shadow processing should trigger review rather than be declared successful.

The scorecard also supports staged investment. A smaller manufacturer does not need to measure every possible indicator in the first pilot. It can select a minimum viable set - for example, legacy retirement, clean-core alignment, upgrade effort, critical security findings, user proficiency, cycle time, and support demand - and expand the measurement model as maturity improves. This proportional approach is consistent with SME digital-transformation research, which emphasizes fit to baseline capability and actionable maturity pathways [21, 22, 23, 24, 25].

9. Implementation Roadmap for U.S. Small and Mid-Sized Manufacturers

Figure 4 translates the framework into a practical seven-phase roadmap. The roadmap is intentionally incremental. It allows a manufacturer to start with one business domain - for example, procure-to-pay, production planning, inventory, maintenance, or order-to-cash - and demonstrate measurable improvement before expanding.

Figure 4: Practical staged roadmap for resource-constrained SAP modernization.

Phase	Primary activities	Key participants	Exit evidence
0. Govern	Define scope, accountable owners, risk appetite, architecture policy, measurement baseline, and evidence repository.	Executive sponsor, SAP owner, security lead, business process owner	Approved charter; KPI definitions; decision rights
1. Discover	Analyze custom code, usage, process dependencies, interfaces, roles, vulnerabilities, and current performance.	SAP technical team, business analysts, security	Verified legacy baseline
2. Rationalize	Apply retire/replace/refactor/retain decisions and prioritize by business value and risk.	Business owners + architecture board	Approved rationalization backlog
3. Re-architect	Apply fit-to-standard and clean-core extension patterns; document exceptions.	SAP architects and developers	Target solution and architecture decision records
4. Secure and validate	Perform security, authorization, integration, regression, recovery, and performance testing.	Security, QA, SAP, operations	Release evidence and risk acceptance
5. Enable people	Co-design workflows, train by role, assess proficiency, and prepare technical sustainment skills.	Change lead, super users, technical leads	Readiness evidence and support model

Phase	Primary activities	Key participants	Exit evidence
6. Measure and sustain	Compare KPIs to baseline, review exceptions, monitor new technical-debt intake, and scale only where evidence supports it.	Governance board and process owners	Outcome report and next-wave plan

Table 4: Suggested implementation roadmap and governance evidence.

10. Discussion

The proposed framework changes the question from 'How much legacy ABAP can be removed?' to 'How much unnecessary coupling can be removed while preserving or improving business capability?' This distinction matters because customization can represent both technical debt and legitimate differentiation. Earlier ERP customization literature warned against simplistic fit-versus-customization decisions [5, 6, 7, 8, 9]. Current clean-core architecture provides better technical options for managing that trade-off, but the organizational decision remains context dependent [39, 40, 41].

A second contribution is the explicit integration of cybersecurity with clean-core design. Modern architectures commonly introduce more service boundaries and interfaces even as they reduce direct core modifications. That can improve maintainability but demands stronger identity, API, logging, and lifecycle governance. Qazi et al. [33] demonstrate that ERP security can be evaluated through a structured standards-based model, while NIST CSF 2.0 [34] and OT guidance [35] provide a risk-management structure that is particularly relevant for manufacturers. The framework therefore rejects the assumption that decoupling automatically equals security.

A third contribution is the treatment of human readiness as a measurable technical-success condition. ERP research has repeatedly shown that organizations can install functioning software without achieving effective use [13, 14, 15, 16, 17, 18]. In clean-core programs, this risk appears in several forms: users may reject standardized processes, developers may reproduce classic patterns inside new extension platforms, and managers may approve exceptions that recreate legacy complexity. Human-centered manufacturing research [26, 27, 28, 29] strengthens the case for measuring capability, work design, and organizational fit alongside architecture.

The framework also adds a practical measurement contribution. Sun, Yazdani, and Overend [17] demonstrate the usefulness of assessing ERP implementation achievement against critical success factors, while Wu and Wang [16] focus on ERP success from the key-user perspective and Hendricks, Singhal, and Stratman [18] connect enterprise-system implementation to corporate performance. More recent maturity models for manufacturing SMEs [24], [25] show the value of multidimensional assessment and roadmaps. The proposed scorecard adapts that logic to clean-core modernization by linking code, security, people, operations, and governance in one evidence model.

Finally, the U.S. small and mid-sized manufacturing focus changes the expected implementation style. A large multinational may be able to fund parallel architecture teams, security programs, extensive test automation, and long transformation waves. Smaller manufacturers often cannot. The framework therefore emphasizes modular pilots, minimum viable KPI sets, proportionate governance, and progressive capability building. This is consistent with SME digital-transformation evidence that maturity, skills, resources, and contextual fit shape viable transformation paths [10, 11, 12], [21, 22, 23, 24, 25].

11. Theoretical and Practical Contributions

11.1 Theoretical Contribution

The theoretical contribution is an integrative socio-technical view of clean-core ERP modernization. The framework links the technical-debt logic of enterprise software [4, 5, 6, 7, 8, 9] with ERP adoption and success research [10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20], SME digital-transformation and maturity research [21, 22, 23, 24, 25], human-centered manufacturing [26, 27, 28, 29], digital-transformation theory [30], [31], and standards-based cybersecurity [33, 34, 35, 36, 37]. Rather than treating these as parallel concerns, the framework proposes that modernization value emerges from their interaction. Architectural decoupling can reduce maintainability risk only if the organization can secure, operate, and govern the resulting extension landscape; user-centered process standardization can improve adoption only if the technical platform remains responsive to legitimate differentiation.

11.2 Practical Contribution

For practitioners, the paper provides a decision sequence, a KPI dictionary, and a governance roadmap. SAP teams can use the framework to structure custom-code discovery and clean-core architecture decisions. Security teams can connect extension changes to recognized risk controls. Business owners can require evidence that standardization does not degrade critical manufacturing processes. Change leaders can assess task proficiency rather than treating training completion as proof of readiness. Executives can compare modernization waves using a consistent scorecard instead of relying on subjective claims that a system is 'cleaner' or 'more modern.'

12. Limitations

This study is conceptual and literature-based. It does not report original survey data, controlled experiments, or verified before-and-after results from U.S. manufacturers. The proposed indicators and scorecard therefore require empirical validation before they can be treated as predictive measures of business performance. The clean-core concept is also evolving, and SAP may refine technical classifications, tooling, and product boundaries over time. Organizations should confirm current SAP documentation when applying architecture-specific guidance. Finally, the U.S. small and mid-sized manufacturing context is justified through the literature on SME constraints, manufacturing digital transformation, and NIST manufacturing security guidance; however, the framework has not yet been calibrated against a representative U.S. firm sample.

13. Future Research

Future work should validate the framework through longitudinal case studies of manufacturers moving from SAP ECC or heavily customized S/4HANA landscapes toward clean-core architectures. A useful design would capture baseline custom-code inventory, architecture classifications, security findings, user proficiency, upgrade effort, and process KPIs before and after a bounded modernization wave. Multiple cases could then test whether the same indicators remain meaningful across discrete manufacturing, process manufacturing, and mixed-mode environments.

A second research direction is to calibrate the proposed scorecard. Researchers could use expert elicitation, analytic hierarchy processes, or multi-criteria decision methods to test domain weights for different risk profiles. A third direction is to study developer transition from classic ABAP to ABAP Cloud and API-based extension models, including learning curves, code-quality outcomes, and organizational identity. A fourth direction is to investigate whether clean-core discipline measurably reduces upgrade adaptation effort and defect escape over several release cycles rather than only immediately after migration. Finally, security research should examine whether decoupled extension architectures reduce overall ERP risk or simply redistribute risk to identity, integration, and platform layers.

14. Conclusion

Legacy ABAP is not a problem merely because it is old, and clean core is not valuable merely because it is new. The managerial problem is whether an organization's custom ERP portfolio remains necessary, secure, understandable, upgradeable, and supportable. Decades of ERP customization and maintenance research show that fit has long-term consequences [5, 6, 7, 8, 9]. Current SAP architecture provides stronger mechanisms for separating necessary differentiation from the ERP core [39, 40, 41, 42, 43, 44]. The opportunity is to combine those mechanisms with disciplined governance rather than repeat earlier customization patterns in a new platform.

This paper proposes a measurable path for doing so. The framework starts with evidence about the legacy baseline, rationalizes the custom ABAP portfolio, selects clean-core extension patterns, embeds security by design, builds human readiness, and measures technical and business outcomes. Governance spans the full lifecycle. The associated scorecard deliberately includes technical cleanliness, security and resilience, human readiness, operational performance, and governance and maintainability because ERP transformation succeeds only when these dimensions reinforce one another.

For U.S. small and mid-sized manufacturers, the framework favors incremental modernization over architectural idealism. The objective is not to eliminate every customization or maximize a vendor-defined cleanliness score. It is to reduce unnecessary technical debt, protect production and data, preserve legitimate process differentiation, improve the ability of people to work with the system, and generate evidence that future changes can be delivered with lower risk and better control. In that sense, clean-core modernization is best understood not as a destination but as a measurable organizational capability.

Acknowledgement

The authors acknowledge the scholarly and technical communities whose published research and public guidance informed this integrative review. Author-specific institutional acknowledgements and any required disclosure regarding writing or research-assistance tools should be completed in accordance with the final journal submission policy before publication.

References

1. T. H. Davenport, “Putting the enterprise into the enterprise system,” Harvard Business Review, vol. 76, no. 4, pp. 121-131, 1998.
2. H. Klaus, M. Rosemann, and G. G. Gable, “What is ERP?,” Information Systems Frontiers, vol. 2, no. 2, pp. 141-162, 2000. https://doi.org/10.1023/A:1026543906354
3. M. Haddara and A. Elragal, “The future of ERP systems: look backward before moving forward,” Procedia Technology, vol. 5, pp. 21-30, 2012. https://doi.org/10.1016/j.protcy.2012.09.003
4. N. Ramasubbu and C. F. Kemerer, “Technical debt and the reliability of enterprise software systems: A competing risks analysis,” Management Science, vol. 62, no. 5, pp. 1487-1510, 2016. https://doi.org/10.1287/mnsc.2015.2196

5. B. Light, “The maintenance implications of the customization of ERP software,” Journal of Software Maintenance and Evolution: Research and Practice, vol. 13, no. 6, pp. 415-429, 2001. https://doi.org/10.1002/smr.240
6. F. F.-H. Nah, S. Faja, and T. Cata, “Characteristics of ERP software maintenance: A multiple case study,” Journal of Software Maintenance and Evolution: Research and Practice, vol. 13, no. 6, pp. 399-414, 2001. https://doi.org/10.1002/smr.239
7. A. Abendroth, B. Bender, and N. Gronau, “The evolution of original ERP customization: A systematic literature review of technical possibilities,” in Proceedings of the 26th International Conference on Enterprise Information Systems (ICEIS), vol. 1, pp. 17-27, 2024. https://doi.org/10.5220/0012305500003690
8. E. Hustad and J. Stensholt, “Customizing ERP-systems: A framework to support the decision-making process,” Procedia Computer Science, vol. 219, pp. 789-796, 2023. https://doi.org/10.1016/j.procs.2023.01.352
9. H. F. Hansen, M. Haddara, and M. Langseth, “Investigating ERP system customization: A focus on cloud-ERP,” Procedia Computer Science, vol. 219, pp. 915-923, 2023. https://doi.org/10.1016/j.procs.2023.01.367
10. M. M. Ahmad and R. Pinedo Cuenca, “Critical success factors for ERP implementation in SMEs,” Robotics and Computer-Integrated Manufacturing, vol. 29, no. 3, pp. 104-111, 2013. https://doi.org/10.1016/j.rcim.2012.04.019
11. O. Alaskari, R. Pinedo-Cuenca, and M. M. Ahmad, “Framework for implementation of enterprise resource planning (ERP) systems in small and medium enterprises (SMEs): A case study,” Procedia Manufacturing, vol. 55, pp. 424-430, 2021. https://doi.org/10.1016/j.promfg.2021.10.058
12. V. U. Sørheller, E. J. Høvik, E. Hustad, and P. Vassilakopoulou, “Implementing cloud ERP solutions: A review of sociotechnical concerns,” Procedia Computer Science, vol. 138, pp. 470-477, 2018. https://doi.org/10.1016/j.procs.2018.10.065
13. A. Tarhini, H. Ammar, T. Tarhini, and R. Masa’deh, “Analysis of the critical success factors for enterprise resource planning implementation from stakeholders’ perspective: A systematic review,” International Business Research, vol. 8, no. 4, pp. 25-40, 2015. https://doi.org/10.5539/ibr.v8n4p25
14. M. Haddara and H. Moen, “User resistance in ERP implementations: A literature review,” Procedia Computer Science, vol. 121, pp. 859-865, 2017. https://doi.org/10.1016/j.procs.2017.11.111
15. K. Amoako-Gyampah and A. F. Salam, “An extension of the technology acceptance model in an ERP implementation environment,” Information & Management, vol. 41, no. 6, pp. 731-745, 2004. https://doi.org/10.1016/j.im.2003.08.010
16. J.-H. Wu and Y.-M. Wang, “Measuring ERP success: The key-users’ viewpoint of the ERP to produce a viable IS in the organization,” Computers in Human Behavior, vol. 23, no. 3, pp. 1582-1596, 2007. https://doi.org/10.1016/j.chb.2005.07.005
17. A. Y. T. Sun, A. Yazdani, and J. D. Overend, “Achievement assessment for enterprise resource planning (ERP) system implementations based on critical success factors (CSFs),” International Journal of Production Economics, vol. 98, no. 2, pp. 189-203, 2005. https://doi.org/10.1016/j.ijpe.2004.05.013
18. K. B. Hendricks, V. R. Singhal, and J. K. Stratman, “The impact of enterprise systems on corporate performance: A study of ERP, SCM, and CRM system implementations,” Journal of Operations Management, vol. 25, no. 1, pp. 65-82, 2007. https://doi.org/10.1016/j.jom.2006.02.002

19. E. J. Martins and F. P. Belfo, “Major concerns about enterprise resource planning (ERP) systems: A systematic review of a decade of research (2011-2021),” Procedia Computer Science, vol. 219, pp. 378-387, 2023. https://doi.org/10.1016/j.procs.2023.01.303
20. I. Ali, N. D. K. Nguyen, and S. Gupta, “A multi-disciplinary review of enablers and barriers to cloud ERP implementation and innovation outcomes,” Journal of Enterprise Information Management, vol. 36, no. 5, pp. 1209-1239, 2023. https://doi.org/10.1108/JEIM-08-2022-0273
21. G. H. Sagala and D. Őri, “Toward SMEs digital transformation success: A systematic literature review,” Information Systems and e-Business Management, vol. 22, pp. 667-719, 2024. https://doi.org/10.1007/s10257-024-00682-2
22. M. Ghobakhloo, M. Iranmanesh, M. Vilkas, A. Grybauskas, and A. Amran, “Drivers and barriers of Industry 4.0 technology adoption among manufacturing SMEs: A systematic review and transformation roadmap,” Journal of Manufacturing Technology Management, vol. 33, no. 6, pp. 1029-1058, 2022. https://doi.org/10.1108/JMTM-12-2021-0505
23. R. Krishnan, “Challenges and benefits for small and medium enterprises in the transformation to smart manufacturing: A systematic literature review and framework,” Journal of Manufacturing Technology Management, vol. 35, no. 4, pp. 918-938, 2024. https://doi.org/10.1108/JMTM-07-2022-0255
24. S. Njah, C. Danjou, F. Armellini, C. Beaudry, and E. Mosconi, “A digital maturity model for assessing SMEs in the manufacturing sector,” Digital Engineering, vol. 9, art. 100084, 2026. https://doi.org/10.1016/j.dte.2025.100084
25. M. E. Latino, “A maturity model for assessing the implementation of Industry 5.0 in manufacturing SMEs: Learning from theory and practice,” Technological Forecasting and Social Change, vol. 214, art. 124045, 2025. https://doi.org/10.1016/j.techfore.2025.124045
26. Y. Lu, H. Zheng, S. Chand, W. Xia, Z. Liu, X. Xu, L. Wang, Z. Qin, and J. Bao, “Outlook on human-centric manufacturing towards Industry 5.0,” Journal of Manufacturing Systems, vol. 62, pp. 612-627, 2022. https://doi.org/10.1016/j.jmsy.2022.02.001
27. C. Zhang, Z. Wang, G. Zhou, F. Chang, D. Ma, Y. Jing, W. Cheng, K. Ding, and D. Zhao, “Towards new-generation human-centric smart manufacturing in Industry 5.0: A systematic review,” Advanced Engineering Informatics, vol. 57, art. 102121, 2023. https://doi.org/10.1016/j.aei.2023.102121
28. J. Nazarejova, Z. Soltysova, and T. Rudeichuk, “Requirements and barriers for human-centered SMEs,” Sensors, vol. 24, no. 14, art. 4681, 2024. https://doi.org/10.3390/s24144681
29. P. N. Zincume and M. Maier, “Human-centred SME factories: The future of work in SMEs under Industry 5.0,” Future Business Journal, vol. 11, art. 133, 2025. https://doi.org/10.1186/s43093-025-00553-3
30. G. Vial, “Understanding digital transformation: A review and a research agenda,” Journal of Strategic Information Systems, vol. 28, no. 2, pp. 118-144, 2019. https://doi.org/10.1016/j.jsis.2019.01.003
31. P. C. Verhoef, T. Broekhuizen, Y. Bart, A. Bhattacharya, J. Q. Dong, N. Fabian, and M. Haenlein, “Digital transformation: A multidisciplinary reflection and research agenda,” Journal of Business Research, vol. 122, pp. 889-901, 2021. https://doi.org/10.1016/j.jbusres.2019.09.022
32. M. R. Robatian, “Implementation of SAP S/4HANA in the manufacturing industry: Challenges and opportunities for the business model,” Journal of Economy & Society (Gazdaság & Társadalom), vol. 17, no. 3, pp. 27-41, 2024. https://doi.org/10.21637/GT.2024.3.02

33. A. Qazi, S. Arshad, and A. A. K. Jadoon, "Security evaluation framework for cloud ERP systems using NIST and ISO standards," Scientific Reports, vol. 16, art. 16069, 2026. https://doi.org/10.1038/s41598-026-45550-w
34. C. Pascoe, S. Quinn, and K. Scarfone, "The NIST Cybersecurity Framework (CSF) 2.0," NIST Cybersecurity White Paper 29, National Institute of Standards and Technology, 2024. https://doi.org/10.6028/NIST.CSWP.29
35. K. Stouffer, M. Pease, C. Y. Tang, T. Zimmerman, V. Pillitteri, S. Lightman, A. Hahn, S. Saravia, A. Sherule, and M. Thompson, "Guide to Operational Technology (OT) Security," NIST Special Publication 800-82 Rev. 3, National Institute of Standards and Technology, 2023. https://doi.org/10.6028/NIST.SP.800-82r3
36. T. Zimmerman, C. Y. Tang, M. Pease, and K. A. Stouffer, "Cybersecurity standards and guidelines to assist small and medium-sized manufacturers," National Institute of Standards and Technology, 2021. https://www.nist.gov/publications/cybersecurity-standards-and-guidelines-assist-small-and-medium-sized-manufacturers
37. M. Powell, J. Hoyt, A. Sherule, and L. Wilcox, "Security segmentation in a small manufacturing environment," NIST Cybersecurity White Paper 28, National Institute of Standards and Technology, 2023. https://doi.org/10.6028/NIST.CSWP.28
38. SAP SE, "Maintenance 2040: SAP S/4HANA innovation commitment and SAP Business Suite 7 maintenance strategy," SAP Support, accessed September 3, 2026. https://support.sap.com/en/release-upgrade-maintenance/maintenance-information/maintenance-strategy.html
39. SAP SE, "Clean Core Extensibility for SAP Cloud ERP," SAP Help Portal, accessed September 3, 2026. https://help.sap.com/docs/clean-core
40. SAP SE, "Extend SAP S/4HANA in the Cloud and On Premise with ABAP-Based Extensions," Version 2.3, SAP BTP ABAP Product Management, August 2025.
41. SAP SE, "How to Extend SAP S/4HANA Cloud the Right Way: Clean Core," SAP News Center, August 2025. https://news.sap.com/2025/08/extend-sap-s4hana-cloud-right-way-clean-clear/
42. SAP SE, "Custom Code Migration," SAP Help Portal, accessed September 3, 2026. https://help.sap.com/docs/SAP_S4HANA_ON-PREMISE/custom-code-migration/
43. SAP SE, "Analyzing Customizations after System Conversion," SAP Learning, accessed September 3, 2026. https://learning.sap.com/
44. SAP SE, "Clean Core Measurement and SAP Cloud ALM," SAP Help Portal / RISE with SAP Methodology, accessed September 3, 2026. https://help.sap.com/docs/cloud-alm/