International Journal of Safety and Security Engineering
Vol. 16, No. 6, June, 2026, pp. 1287-1296
Journal homepage: http://iieta.org/journals/ijsse

Incident-Driven Information System Risk Management Using ISO 31000:2018, STRIDE, and CIA Triad: A Case Study of an Indonesian Manufacturer

Robin Lai*, Nilo Legowo

Information Systems Management Department, BINUS Graduate Program - Master of Information Systems Management, Bina Nusantara University, Jakarta 11480, Indonesia

Corresponding Author Email: robin009@binus.ac.id

https://doi.org/10.18280/ijsse.160611

Received: 10 May 2026
Revised: 17 June 2026
Accepted: 22 June 2026
Available online: 30 June 2026

Keywords:
Confidentiality, Integrity and Availability Triad, information system risk management, ISO 31000:2018, operational resilience, STRIDE threat modelling

ABSTRACT

Indonesian manufacturers depend increasingly on integrated information systems (IS), yet studies that apply ISO 31000:2018 in its entirety to IS risk management in this sector remain limited and rarely use actual incident data. This study aims to operationalize the full eight-stage Clause 6 cycle of ISO 31000:2018 at an Indonesian manufacturer of decorative interior materials that experienced three actual 2024 incidents (a web-shell backdoor, an SQL-injection, and a Google Credential Provider for Windows (GCPW) authentication failure), and to formulate a prioritized mitigation plan. The methodology executes all eight Clause 6 stages, from Communication and Consultation through Recording and Reporting, within a single-case design with concurrent triangulation of an evaluation form, semi-structured interviews (N = 6), field observation, and a perception survey (N = 30); STRIDE threat modelling and the Confidentiality, Integrity and Availability (CIA) Triad serve as complementary analytical lenses. The results identify 14 IS risks across five domains, comprising two Extreme, nine High, and three Medium risks. CIA mapping shows dominance on Availability and Integrity, while perception scored 3.78 of 5 with process maturity lowest at 3.57. The study contributes a risk register, three-tier prioritization (P1 to P3), treatment plan for P1 and P2 risks, and a six-indicator KPI scheme, offering a transferable reference model for ISO 31000:2018 implementation in Indonesian manufacturing.

1. INTRODUCTION

Digital transformation has substantially transformed how manufacturing organizations operate, with integrated information systems (IS) such as Enterprise Resource Planning (ERP), Warehouse Management Systems (WMS) and identity-access services becoming central to production, distribution and decision making [1]. The same dependence, however, exposes organizations to a class of multi-dimensional risks that propagate quickly across coupled subsystems. According to the National Cyber and Crypto Agency of Indonesia (BSSN), 1,367 cyber-incident notifications were sent to stakeholders across strategic sectors, including manufacturing and logistics, in 2024 [2]. Globally, the average cost of a single data breach reached USD 4.44 million in 2025 [3], underlining that even individual incidents now translate into material business loss.

PT. ABC (a pseudonym used to preserve commercial confidentiality, with explicit consent from company management for academic publication), an Indonesian manufacturer of decorative interior materials with more than 1,000 employees and an integrated ERP-HRIS-portal landscape, is representative of this exposure. In 2024 the case organisation recorded three actual IS incidents that disrupted operations: (i) a web-shell backdoor uploaded through a profile-picture feature that led to portal defacement and four hours of downtime; (ii) an SQL-injection on the document-search module that exposed employee data; and (iii) a Google Credential Provider for Windows (GCPW) authentication failure following a Windows update, which interrupted ERP, WMS and Sales-Order access for more than one hour and required 65 hours of investigation. Internal evaluation confirmed weaknesses in application-security controls, IT governance and the absence of a formal risk-management framework. As shown in Figure 1, the period 2021–2023 was characterized by minor disruptions only (under 30 minutes of downtime), whereas 2024 marked a clear escalation to multi-dimensional incidents spanning Confidentiality, Integrity and Availability (CIA) [4], a profile that cannot be addressed by isolated technical controls alone.

Several studies have demonstrated that ISO 31000:2018 provides an effective foundation for IS risk management. The standard has been applied in diverse contexts, including e-commerce systems, where access- and fund-loss risks across two core systems were identified [5]; textile manufacturing, where 109 operational risks were identified [6]; agribusiness, where a rapid-assessment model was proposed [7]; and learning management systems, where IS-related risks were assessed [8]. Other studies have integrated ISO 31000 with ISO 14001/9001 in construction and thermal-power contexts

[9, 10], applied it to risk assessment in the Indonesian financial sector [11, 12], combined it with the POAC framework for quality-improvement projects [13], and proposed an IS-based roadmap to operationalize IT risk management in line with the ISO 31000 process [14]. Despite this breadth, two consistent gaps remain. First, most prior studies apply only a subset of the eight Clause-6 stages, treating Communication & Consultation, Monitoring & Review, and Recording & Reporting as ancillary rather than as integral parts of the cycle. Second, IS risk-management studies in the Indonesian manufacturing sector remain scarce, and even fewer are anchored in actual incident data; surveys and conceptual reviews remain the dominant evidentiary base [15, 16].

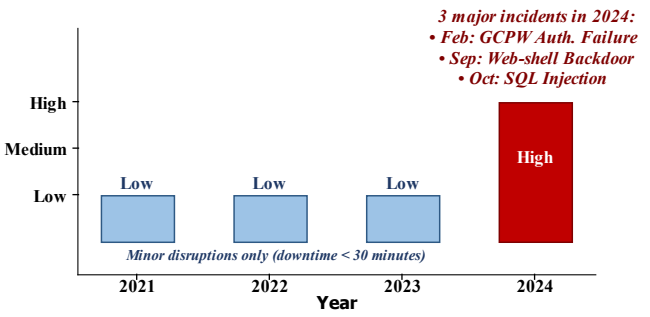

Figure 1. Information system incident severity profile (2021–2024)

This study addresses these gaps through a single-case implementation of ISO 31000:2018 Clause 6 in an Indonesian decorative-materials manufacturer. The aims are to (i) identify and characterize IS risks at the case organisation on the basis of actual 2024 incident records and stakeholder evidence, complemented by STRIDE threat modelling [17] and CIA classification; (ii) demonstrate the adaptability of all eight Clause-6 stages in an organisation that has no formal risk-management framework; and (iii) formulate a context-grounded, prioritized mitigation plan that supports operational resilience [18, 19]. The study's contribution is methodological rather than the introduction of a new technique: it grounds risk identification in three documented 2024 incidents and reads them through STRIDE and the CIA Triad, so that risks are derived from observed events rather than perception alone. This incident-anchored, triangulated approach distinguishes the work from prior ISO 31000 studies that rely mainly on surveys or expert judgement, and it is what the study offers beyond a single applied case.

2. LITERATURE REVIEW

2.1 Information system risk management

IS risk management is a structured process that identifies, analyses and treats threats to CIA of information assets [20]. Tambunan et al. [21] argued that ISO-based frameworks allow organizations to mitigate cyber risk in a measurable manner while reinforcing operational resilience through systematic control.

2.2 CIA Triad and STRIDE threat modelling

The CIA Triad has, since its formalization in the ISO/IEC 27000 series, been the dominant lens for classifying information-security risks [4, 22]. Confidentiality protects against unauthorized disclosure, Integrity preserves accuracy against unauthorized modification, and Availability ensures information access when required. STRIDE, developed by Microsoft [17], complements this lens at the threat modelling level by classifying threats into Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege. While ISO 31000 governs the process, CIA captures security outcomes and STRIDE captures threat characteristics; the three are therefore frequently used together rather than as alternatives.

2.3 ISO 31000:2018 framework

ISO 31000:2018 [22] is a generic, principle-based standard organised in three components: Principles (Clause 4), Framework (Clause 5) and Process (Clause 6). Clause 6 specifies an iterative cycle: Communication & Consultation (6.2), Scope/Context/Criteria (6.3), Identification (6.4.2), Analysis (6.4.3), Evaluation (6.4.4), Treatment (6.5), Monitoring & Review (6.6), and Recording & Reporting (6.7). This cycle encompasses both content and governance dimensions of the risk process [23, 24]. Compared with NIST SP 800-30, COBIT 5 and ISO/IEC 27001, which presuppose maturity in security or governance, and ISO/IEC 27005 [25], which assumes an existing Information Security Management System, ISO 31000 makes minimal prerequisites and therefore suits organizations without a formal risk function. The studies [26, 27] recently underlined the cross-sectoral adaptability of the standard for quality-management and strategic-planning contexts.

2.4 Prior implementations and research gap

Recent studies have applied ISO 31000:2018 in domains adjacent to the present study. In service-oriented systems, including e-commerce and learning management systems, the standard has been shown to help organizations without a pre-existing risk framework formalize previously implicit practices, particularly through the Identification and Treatment stages [5, 8]. Similar evidence has also been reported in operational contexts, where 109 operational risks were identified in the textile industry using ISO 31000:2018 [6]. However, evidence from the Indonesian banking sector suggests a more complex financial trajectory: ISO 31000 adoption may have a negative short-term effect on Return on Equity because implementation costs can temporarily outpace financial benefits, even though governance and resilience may improve over the longer term [12]. These studies therefore generally agree that ISO 31000 strengthens governance, but they differ in their assessment of its short-term financial implications. A common limitation is that few studies report on the full eight-stage cycle; Communication & Consultation, Monitoring & Review, and Recording & Reporting are often treated only briefly. Although a rapid-assessment model has been proposed to address some of these limitations, it does not fully incorporate the iterative monitoring loop that is central to ISO 31000 [7]. More recently, the Indonesian SPBE Risk Management Guidelines have been applied to assess IS audit tools in a government context, demonstrating the feasibility of formal risk frameworks in the Indonesian public sector [28]. The present study extends this line of work by applying the international ISO 31000:2018 standard to the manufacturing sector, with the additional dimension of incident-anchored risk

identification.

Synthesising these findings, three observations emerge. First, ISO 31000:2018 is empirically tractable across sectors but is rarely applied in its entirety. Second, Indonesian manufacturing, in contrast to e-commerce, banking and education, is under-represented in the IS risk-management literature despite its accelerating digitalization under the national Making Indonesia 4.0 roadmap [29]. Third, to the best of our knowledge, no published implementation starts from actual IS incident data and uses STRIDE and CIA jointly to enrich the Identification stage. The present study addresses these three points simultaneously.

3. METHODOLOGY

3.1 Research design

The study adopts a single-case design [30] suitable for the "how" and "why" research questions characteristic of risk-management studies, conducted on a bounded contemporary system, namely the case organisation introduced in Section 1. The case was selected purposively as an information-rich setting rather than as a statistically representative one. It is suitable for two reasons. First, like many mid-sized Indonesian manufacturers, it runs an integrated ERP, HRIS, and portal landscape that has no unified security-control standard, so a compromise in one component can propagate across the connected systems; this is the risk mechanism the study examines. Second, its core operations run on operationally critical systems, the ERP, which also handles order processing, and the warehouse management system, so any disruption is directly consequential for production and distribution. These conditions, together with three documented 2024 incidents and direct access to internal evidence, made the organisation well suited for observing the full Clause 6 cycle from a baseline in an organisation that had no formal risk framework. The inferential goal is therefore analytical, not statistical, generalization [30]. A concurrent-triangulation strategy [31] integrates four primary sources, namely a pre-interview evaluation form, semi-structured interviews, field observation, and a perception survey, with internal documents (incident reports, IT-audit reports) as secondary data.

3.2 Research procedure

The research followed the eight-stage Clause 6 cycle of ISO 31000:2018, preceded by an initial preparatory phase. The preparatory phase comprised literature study and preliminary field investigation at the case organisation to establish research focus. The Communication and Consultation stage (6.2) engaged internal stakeholders to obtain contextual information on information assets, security policies, and unit responsibilities. The Scope, Context, and Criteria stage (6.3) defined system boundaries, assets, and impact parameters. Field data collection was then conducted through semi-structured interviews, perception survey, and field observation, followed by triangulation across the three methods. The triangulated data informed Risk Identification (6.4.2) and Risk Analysis (6.4.3) to assess likelihood and impact and compile the risk register. Risk Evaluation (6.4.4) determined treatment priorities, and Risk Treatment (6.5) formulated mitigation strategies. Monitoring and Review (6.6) and Recording and Reporting (6.7) operationalized continuity and accountability through the proposed KPI scheme and documented deliverables.

3.3 Data collection procedures

Pre-interview evaluation form was distributed to six key informants prior to interviews, capturing initial perception of risk control practices, documentation readiness, and incident-handling patterns.

Semi-structured interviews (N = 6) were conducted with the IT Applications, IT Technical, Data Analyst, Functional Analyst, and Quality Assurance Managers from the Information Technology Division, and one Compliance Analyst (Internal Audit and Risk Management) from the Compliance and Risk Division. Each session lasted 30 to 45 minutes and was documented to ensure data accuracy.

Field observation covered operational conditions across business units to identify risk sources and potential threats.

Perception survey (N = 30) was administered on a five-point Likert scale to employees from six work units (Production, Warehouse, Operations, Information Technology, Finance, and Human Resources). Respondents were selected through non-probability convenience sampling, focusing on active employees relevant to the research objectives. The full perception-survey items, the semi-structured interview guide, the field-observation sheet, and the analysis templates (the ISO 31000 Clause 6 mapping, the STRIDE and CIA worksheet, and the risk-scoring heatmap) are provided as supplementary material in the study's Zenodo deposit (see the Data Availability Statement). The pre-interview evaluation form is described below but, like the per-respondent data, is withheld for confidentiality.

3.4 ISO 31000:2018 Clause 6 mapping

Each Clause 6 stage was mapped to a concrete research activity and a verifiable deliverable, as summarized in Table 1. The full eight-stage cycle was preserved. Communication and Consultation (6.2) was operationalized as the interview and evaluation-form process itself; Monitoring and Review (6.6) and Recording and Reporting (6.7) were operationalized as the cross-functional risk-coordination forum and KPI scheme proposed in Section 4.5 and as the structured deliverables (risk register, ranking, treatment plan) produced by the study.

Within this cycle the five central stages (6.3 to 6.5) form the core analytical sequence, each producing a verifiable deliverable, while Communication and Consultation (6.2), Monitoring and Review (6.6), and Recording and Reporting (6.7) operate as enveloping processes throughout rather than as discrete steps. Evidence from four parallel sources, collected through concurrent triangulation, feeds the Risk Identification (6.4.2) stage.

3.5 Analysis procedure

3.5.1 Qualitative coding

Evidence from the interviews, evaluation forms, and observation notes was coded against the eight Clause 6 stages and the five risk domains (Application, Data, Access and Security, Change and Operations, and Compliance and Continuity). Each coded item was traced to a candidate risk, which was then confirmed or merged with related items, producing the consolidated set of 14 risks.

Table 1. Mapping of ISO 31000:2018 Clause 6 to research activities

Clause	Stage	Research Activity	Output / Deliverable
6.2	Communication & Consultation	Stakeholder coordination; pre-interview evaluation form; informant identification	Coordination notes; stakeholder map; risk-communication map
6.3	Scope, Context & Criteria	Definition of system boundary, internal/external context, and impact criteria	Scope document; risk criteria; organisational context
6.4.2	Risk Identification	Synthesis of evaluation form, interviews, questionnaire and document review	Risk register (14 risks); STRIDE & CIA mapping
6.4.3	Risk Analysis	Likelihood × Impact scoring; qualitative analysis of impact	Risk register with L, I and level
6.4.4	Risk Evaluation	Comparison with criteria; risk ranking	Risk heatmap; priority assignment (P1–P3)
6.5	Risk Treatment	Mitigation design by priority and treatment option (avoid, reduce, transfer, accept)	Treatment plan with PIC, target time and indicators
6.6	Monitoring & Review	Effectiveness monitoring; review of context change	KPI scheme; cross-functional review forum
6.7	Recording & Reporting	Documentation of decisions and outcomes	Risk register; ranking; treatment plan; final report

3.5.2 Triangulation

Evidence from the evaluation form and the interviews was compared across the eight Clause 6 stages to identify where the sources converged, with the perception survey and internal documents (incident and IT-audit reports) used as corroborating evidence. Because the form and the interviews involved the same six key informants, they served as a consistency check across the stages, while the 30-respondent survey and the documents provided independent corroboration. Each risk in the register is grounded in this evidence. A de-identified summary of the triangulation across the Clause 6 stages is provided as supplementary material in the study's Zenodo deposit (see the Data Availability Statement).

3.5.3 STRIDE and CIA classification

Each of the three actual 2024 incidents was mapped against the six STRIDE categories based on incident analysis and interview findings.

Each identified risk was classified against one or more CIA dimensions based on documented or potential impact.

3.5.4 Scoring criteria and procedure

Likelihood and impact were each rated on a five-point scale; the level descriptors are given in Table 2. Likelihood was judged from how often each risk had recurred, drawing on the 2024 incident records and the informant accounts, and impact from the operational consequence those sources evidenced, ranging from negligible to business-stopping. The two ratings were multiplied (L × I, 1 to 25) and grouped into Low (1 to 4), Medium (5 to 9), High (10 to 16), and Extreme (17 to 25), as shown in the heatmap (Figure 2), with a short justification recorded for each risk. The scores were assigned by the first author, who is the IT Manager of the case organisation and therefore had direct operational knowledge of the systems and incidents; this position is stated in the Conflicts of Interest declaration. During scoring, the first author consulted the Compliance Analyst (Internal Audit and Risk Management) to validate the likelihood and impact ratings against audit and compliance records, while retaining sole responsibility for the final scores. Because a single assessor carried out the scoring, there were no inter-rater disagreements to resolve; where the underlying sources differed, the documented incident and IT-audit records were given precedence over individual perceptions, and each rating was cross-checked against the six interviews and those records. The perception survey was not used to score individual risks: it measured employees' general risk perception across ten aspects and served only as corroborating context.

Table 2. Likelihood and impact scoring scale

Score	Likelihood	Impact
1	Very Low: almost never occurs	Very Low: no operational impact
2	Low: rarely occurs	Low: minor impact, easily recoverable
3	Moderate: occasionally occurs	Moderate: limited operational disruption
4	High: frequently occurs	High: significant operational disruption
5	Very High: almost always occurs	Very High: major impact, difficult to recover

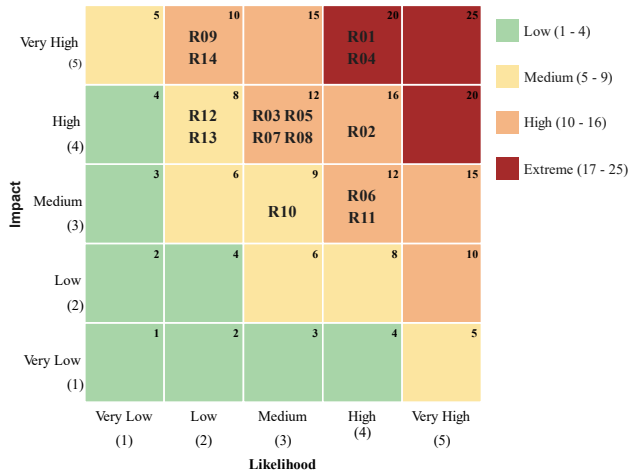

Figure 2. Risk heatmap of the 14 IS risks (L × I)

3.5.5 Perception interpretation

Likert scores were interpreted descriptively against five intervals (Very Low, Low, Medium, Good, Very Good) to support, rather than replace, the qualitative findings.

4. RESULTS AND DISCUSSION

4.1 Respondent profile and risk perception

Thirty employees from Finance (26.7%), Warehouse (16.7%), IT (16.7%), Operations (13.3%), Production (13.3%) and HR (13.3%) participated in the perception survey. The six interview informants comprised the IT Applications, IT

Technical, Data Analyst, Functional Analyst, and Quality Assurance Managers from the Information Technology Division, and one Compliance Analyst (Internal Audit and Risk Management) from the Compliance and Risk Division. Four of six informants (67%) had at least two years' tenure, giving longitudinal insight into recurring risk patterns.

The perception score for each aspect was the mean Likert response across the 30 respondents. Across the ten ISO 31000-aligned aspects, the overall mean was 3.78/5 ("Good"). The highest score was on Operational Impact (4.03), reflecting strong awareness of business consequences when IS fails. Process Maturity scored the lowest (3.57), pointing to inconsistent periodic evaluation and documentation.

Beyond the means, Table 3 reports the standard deviation and the share of respondents who rated each aspect 4 or 5. Dispersion is moderate (standard deviations from 0.76 to 1.14), and agreement tracks the means, highest for Operational Impact (73%) and lowest for Process Maturity (57%). The survey is treated descriptively, to support and not replace the qualitative findings.

Perception also varies by work unit (Table 4). Because the per-unit samples are small (n = 4 to 8), the differences are descriptive only and no significance tests were applied.

The contrast between the highest and lowest aspects is itself a finding: employees recognize the consequences of IS failure but lack systematic mechanisms (periodic review, documented procedures, structured CAPA) to act on that awareness. This converges with the interviews, where informants reported that technical controls operate while formal evaluation and documentation remain inconsistent. The work-unit pattern points the same way: perception is highest in IT and lowest in Human Resources and Warehouse, confirming that risk practice is uneven across units. Together these results give the awareness-maturity gap independent support and motivate the governance-oriented treatments in Section 4.4.

Table 3. Perception by aspect: Mean, standard deviation, and agreement (N = 30)

Perception Aspect	Mean	SD	Agree (4 or 5)
Context Establishment	3.87	0.78	70%
Risk Awareness	3.77	1.01	60%
Risk Identification Process	3.70	1.06	63%
Risk Analysis	3.70	0.92	63%
Risk Evaluation	3.73	0.94	60%
Control and Mitigation	3.73	1.14	67%
Incident Response	3.87	0.90	67%
Process Maturity	3.57	1.04	57%
Operational Impact	4.03	0.76	73%
Operational Resilience	3.83	0.87	67%
Overall mean	3.78	–	65%

Table 4. Mean perception by work unit

Work Unit	Respondents	Mean Perception
Information Technology	5	4.26
Operations	4	3.90
Finance	8	3.88
Production	4	3.60
Warehouse	5	3.52
Human Resources	4	3.38

4.2 Risk identification (Clause 6.4.2)

Identification proceeded in two passes. Pass 1 classified the three actual 2024 incidents against STRIDE to characterize the threat vectors observed in practice. The result is shown in Table 5.

Table 5. STRIDE classification of the three actual incidents (2024)

Incident	S	T	R	I	D	E
Web-shell backdoor (Sept. 2024)	√	√		√	√	√
SQL injection (Oct. 2024)		√		√		
GCPW authentication (Feb. 2024)					√	

Note: S = Spoofing, T = Tampering, R = Repudiation, I = Information Disclosure, D = Denial of Service, E = Elevation of Privilege.

Web-shell backdoor (September 2024). The portal was compromised when login credentials captured from an unmanaged personal endpoint were reused to reach the server, and a script uploaded through a profile-image feature executed because the upload directory permitted execution, leading to portal defacement and about four hours of downtime. The incident is analytically instructive because it shows how weak controls cascade: the absence of endpoint management enabled credential capture, weak access control allowed the credentials to be reused, and an unrestricted upload directory turned an ordinary content feature into an execution path. As classified in Table 5 it spans five of the six STRIDE categories, and its effect falls mainly on Integrity and Availability. The underlying weaknesses are therefore matters of access governance and configuration rather than any single technical flaw.

SQL injection (October 2024). An input field in the document-search module that was not consistently validated allowed an attacker to read and alter database contents and to expose part of the employee data. The significance of the incident lies less in the technique than in what it reveals: secure-development practice, and input validation in particular, was applied unevenly across the portal's modules, so one unprotected field was enough to compromise confidentiality and data integrity. It maps to Tampering and Information Disclosure (Table 5) and affects Confidentiality and Integrity. The study therefore treats it as a systemic application-security risk rather than an isolated coding error.

GCPW authentication failure (February 2024). An operating-system update conflicted with a third-party authentication component and blocked logins to the ERP and other core applications. Warehouse, finance, and sales staff lost access for more than an hour, which disrupted order processing and delayed distribution, sales reporting, and stock updates. Unlike the first two incidents this was not an attack but an availability failure rooted in change management, where an uncontrolled update combined with dependence on an external authentication service. It maps to Denial of Service (Table 5) and affects Availability, and it shows that operational risk in an integrated environment can arise from routine maintenance as readily as from external threats. The breadth of STRIDE coverage in a single year confirms the multi-dimensional character of IS risk in an integrated manufacturing environment and motivates Pass 2.

Pass 2 consolidated 14 IS risks through triangulation of interviews, evaluation forms, observation notes, and incident records. The risks are distributed across five domains: Application, Data, Access and Security, Change and Operations, and Compliance and Continuity. The consolidated risk register is summarized in Table 6, listing each risk with its source, affected unit, and CIA dimension.

Following the CIA definitions in the Methodology, each

risk was tagged on one or more dimensions where evidence supported it.

Availability and Integrity dominate (10 and 9 risks respectively), consistent with the operational-critical character of ERP, WMS, and Sales Order systems where service interruption directly halts production and distribution. The three Confidentiality-affecting risks (R08, R09, R10), although fewer in number, carry significant regulatory and reputational consequences.

4.3 Risk analysis and evaluation (Clauses 6.4.3-6.4.4)

Using the scale and four-level scheme defined in the Methodology, each risk's L × I score places it in the heatmap (Figure 2).

Two risks reach the Extreme level: application service downtime (R01) and low data quality (R04), both scoring 20. Both combine very high impact (5) with high likelihood (4) and lie at the centre of operational continuity. Nine risks are High, with operational drivers (defect leakage, ETL failures, change/release control, access governance) dominating. Three risks are Medium, concerning third-party dependence, hardware failure, and audit readiness.

Following ISO 31000:2018 Clause 6.4.4, risks were ranked first by score and then by impact severity (where scores tied, higher impact ranked first). Three priority tiers were assigned: P1 for risks requiring immediate treatment (both Extreme risks and High risks with maximum impact of 5); P2 for High risks with score 12 requiring structural treatment within the planning horizon; and P3 for Medium risks managed through routine controls and monitoring. The full ranking is shown in Table 7.

Table 6. Risk register of identified IS risks (Clause 6.4.2)

Code	Risk	Source	Affected Unit	CIA
R01	Application service downtime	Defects, change, configuration, capacity	IT App., Functional, Business	A
R02	Integration / API errors between modules	Unstable inter-system integration	IT App., QA, Functional	I, A
R03	Defect leakage past UAT/QA	Insufficient testing, manual bug tracking	QA, IT App., Business	I, A
R04	Low data quality (mismatch, duplication, non-real-time)	Manual validation, inconsistent processes	Data, IT App., Business	I
R05	Data process failure (ETL/job)	Pipeline errors, inconsistent monitoring	Data, Business	I, A
R06	User input / transaction errors	Awareness, unbaselined procedure	Functional, Business, IT App.	I
R07	Uncontrolled change/release	No baselined change SOP	IT Tech., IT App., QA	I, A
R08	Excessive or misaligned access	Irregular access review, JML control	IT, Data, Compliance	C
R09	Data breach / privacy violation	Phishing, excessive access, weak controls	Compliance, IT, all units	C, I
R10	Weak audit readiness (evidence)	Ad-hoc documentation	Compliance, IT, related units	C, I, A
R11	Inconsistent RCA/CAPA	No standard, untracked closure	Compliance, QA, IT App., Data	I, A
R12	Third-party / vendor dependency	Weak SLA, external service reliance	IT, Compliance, Business	A
R13	Hardware / infrastructure failure	Aging assets, limited capacity	IT Operations, all units	A
R14	Weak / untested BCP and resilience	BCP not formalized, no DR test	All units, IT, Compliance	A

Table 7. Risk ranking and priority assignment (Clause 6.4.4)

Rank	Code	Risk	L	I	Score	Level	Priority
1	R01	Application service downtime	4	5	20	Extreme	P1
2	R04	Low data quality	4	5	20	Extreme	P1
3	R02	Integration / API errors	4	4	16	High	P1
4	R09	Data breach / privacy violation	2	5	10	High	P1
5	R14	Weak / untested BCP	2	5	10	High	P1
6	R03	Defect leakage past UAT/QA	3	4	12	High	P2
7	R05	Data process failure (ETL)	3	4	12	High	P2
8	R07	Uncontrolled change / release	3	4	12	High	P2
9	R08	Excessive or misaligned access	3	4	12	High	P2
10	R06	User input / transaction errors	4	3	12	High	P2
11	R11	Inconsistent RCA/CAPA	4	3	12	High	P2
12	R12	Third-party / vendor dependency	2	4	8	Medium	P3
13	R13	Hardware / infrastructure failure	2	4	8	Medium	P3
14	R10	Weak audit readiness	3	3	9	Medium	P3

4.4 Risk treatment (Clause 6.5)

Treatment options were selected per risk from the ISO 31000:2018 set (Avoid, Reduce, Transfer, Accept), guided by feasibility within the case organisation's current capacity, the control gap identified in evidence, and cost-benefit balance. Reduce dominates because the identified risks are predominantly internal and addressable through process and control strengthening. Avoid was selected only for R09 (data breach and privacy violation), which carries significant regulatory, reputational, and sanction risks, in combination with Reduce. Transfer and accept were not selected for any P1 or P2 risk, as the identified risks are addressable through internal control strengthening. Table 8 summarises the core

treatment direction; the full plan with PIC, target time, and indicators is recorded in the project risk register.

4.5 Monitoring, review, recording and reporting (Clauses 6.6-6.7)

Sustained effectiveness is operationalized through three mechanisms. First, a cross-functional IS risk-coordination forum, drawing IT, QA, Data and Compliance, meets monthly or quarterly to update the risk register, follow up CAPAs and align priorities. Second, a minimum KPI scheme is proposed: incident-frequency trend, defect-leakage rate, access-review compliance, MTTR, audit-evidence readiness and CAPA on-time closure rate, all reported quarterly to executive leadership (Table 9).

Third, risk review is integrated into the system-development life cycle so that risk identification becomes a planning-stage activity rather than a post-incident reaction. Recording and reporting are sustained through the risk register, ranking and treatment plan documented in this study, fulfilling the accountability requirement of Clause 6.7.

Table 8. Risk treatment plan summary for P1 and P2 risks (Clause 6.5)

Pri.	Code	Treatment	Core Recommendation
P1	R01	Reduce	Standardize monitoring & alerting, define SLA/SLO and escalation, conduct structured post-incident reviews
P1	R04	Reduce	Automated pipeline validation; data-ownership definition; data-quality KPI dashboard
P1	R02	Reduce	Strengthen integration & regression testing; minimum release gate; documented dependencies
P1	R09	Reduce / Avoid	Tighten role-based access; restrict and approve data export; awareness training and audit-trail review
P1	R14	Reduce	Formal BCP/DRP for critical systems; defined RTO/RPO; scheduled DR drills and follow-up
P2	R03	Reduce	Standard UAT sign-off criteria; QA metrics as release-readiness gate
P2	R05	Reduce	Job monitoring with retry; alerts on critical jobs; root-cause documentation
P2	R07	Reduce	Minimum change procedure (request–review–approval–rollback); pre-release risk review
P2	R08	Reduce	Least-privilege; periodic access review; approval workflow for critical access
P2	R06	Reduce	Stronger input validation, baselined SOPs, short user training
P2	R11	Reduce	Standard RCA/CAPA template, status tracking to closure, periodic recurrence review

Table 9. KPI scheme with operational definitions (Clauses 6.6 and 6.7)

KPI Indicator	Calculation Formula	Owner	Baseline	Target	Review or Corrective Action
Incident-frequency trend	Number of incidents per risk category per quarter	IT Operations	To be established	Downward trend versus baseline	If it rises over two consecutive quarters, review the risk register
Defect-leakage rate	Defects found in production / total defects found (UAT and production) × 100%	QA	To be established	Reduction versus baseline	If it rises versus baseline, run a release-gate review
Access-review compliance	Accounts reviewed on schedule / total accounts due for review × 100%	IT Security	To be established	Increase toward full on-schedule review; threshold set after baseline	If it falls versus baseline, require access recertification
Mean time to repair (MTTR)	Total repair time of major incidents / number of major incidents	IT Operations	To be established	Reduction versus baseline	If it rises versus baseline, review the incident-response process
Audit-evidence readiness	Controls with current evidence / total controls × 100%	Compliance	To be established	Increase versus baseline	If it falls versus baseline, issue a remediation plan
CAPA on-time closure rate	CAPAs closed on time / total CAPAs due × 100%	Compliance and Internal Audit	To be established	Increase toward timely closure; threshold set after baseline	If it falls versus baseline, escalate to the risk-coordination forum

4.6 Discussion

4.6.1 Comparison with prior literature

The findings reinforce, but also extend, the prior literature. They reinforce previous findings [5, 8] that in organizations without a formal risk function, ISO 31000:2018 first delivers value by formalising existing implicit practice (testing, role-based access, post-incident response), then by standardizing what is missing (RCA/CAPA, change governance, KPI). They extend this by demonstrating that the full eight-stage cycle is feasible and beneficial, with Communication & Consultation, Monitoring & Review, and Recording & Reporting becoming explicit deliverables rather than implicit assumptions. Compared with earlier studies that identified many operational risks but few cross-domain interdependencies in textiles [6], the present case shows how integrated ERP-HRIS-portal landscapes propagate risk across CIA dimensions, motivating the joint use of STRIDE and CIA. Compared with previous findings that reported short-term financial drag [12], this study foregrounds operational resilience as the primary value channel for organizations that have not yet adopted the standard.

4.6.2 Practical implications for the case organisation's management

The findings yield three practical implications for the case organisation's management. First, the study indicates the need for more explicit top-management commitment to IS risk management. Interview findings suggest that current management support is more output-project oriented than

formally directed at technical risk control. Top management therefore needs to establish formal risk-management policy, allocate adequate resources for control implementation, and directly lead the formation of a risk-aware culture across the organisation, consistent with Clause 5 of ISO 31000:2018 which positions leadership and commitment as the foundation of an effective risk-management framework [22].

Second, formalization of IT risk governance is required through clearly defined policy, procedure, and accountability structures. The current condition, in which risk management runs reactively and is based on individual experience, increases dependence on tacit knowledge held by key personnel and reduces organisational resilience to staff turnover. Such formalization becomes a strategic priority that affects not only information security but also operational continuity and corporate reputation [21].

Third, the study recommends that the management of the case organisation defines an explicit risk appetite as a reference for risk decision-making. A clearly defined risk appetite supports unit managers in determining acceptable risk tolerance, enabling more consistent and objective prioritization across functions. Without an explicit risk appetite, risks with significant impact may not receive proportional attention due to the absence of a uniform assessment standard across units.

4.6.3 Implications for Indonesian manufacturing sector

Beyond the case organisation, this study provides empirical evidence that ISO 31000:2018 can be effectively implemented as an IS risk-management framework in the Indonesian manufacturing sector undergoing digital transformation. Unlike prior research that has predominantly focused on the financial sector [12] or remained at a conceptual level [8], this study demonstrates a practical implementation grounded in actual incident data, offering an implementation model that can be adapted by other manufacturers with comparable characteristics.

The findings further confirm that operational resilience cannot be achieved through the strengthening of technical controls alone. It requires an integrated approach encompassing process formalization, documentation enhancement, human-resource capacity building, and the integration of risk management into the system-development life cycle. This broadens the understanding of operational resilience from a narrow technical-recovery capability to an organisational capability that is adaptive and sustainable [19].

5. CONCLUSIONS

This study has shown that ISO 31000:2018 Clause 6 can be implemented end-to-end in an Indonesian manufacturer that previously lacked a formal risk-management framework. Triangulating four primary sources and combining ISO 31000 with STRIDE and CIA Triad classification, the study identified 14 IS risks across five operational domains, with exposure concentrated on Availability and Integrity and process maturity emerging as the weakest perceived aspect.

The implementation produced four concrete deliverables: an empirically grounded risk register, a three-tier prioritization (P1 to P3), a structured treatment plan with PIC, target time, and success indicators, and a six-indicator KPI scheme operationalized through a cross-functional risk-coordination forum. Theoretically, the work demonstrates that the full eight-stage Clause 6 cycle, including the often-overlooked Communication and Consultation, Monitoring and Review, and Recording and Reporting stages, is operationally tractable in an organisation without a pre-existing risk-management framework. Practically, the resulting framework provides a transferable reference model for ISO 31000:2018 implementation in Indonesian manufacturing organizations undergoing digital transformation, while acknowledging that empirical validation across multiple cases remains a direction for future research.

Three limitations should be noted. First, scoring relied on a single insider assessor, mitigated by documented-evidence grounding, validation by the organisation's Compliance function, and per-risk justification, but not by formal multi-rater validation. Second, as a single-case study what transfers is the method (the staged Clause 6 operationalization, risk-register structure, STRIDE-CIA mapping, prioritization logic, and KPI scheme), whereas the specific risks, scores, and incident profile are bound to this organisation; the single-sector scope and small respondent base further limit external validity, so replication across manufacturers is needed before the register itself can be generalized. Third, treatment effectiveness is forward-looking and remains to be measured against the proposed KPIs. Future work should compare incident data before and after mitigation, integrate the framework with ISO/IEC 27001, and assess the impact of treatment on operational performance indicators.

AUTHOR CONTRIBUTIONS

Robin Lai: Conceptualization, Methodology, Investigation, Formal Analysis, Data Curation, Writing - Original Draft, Visualization. Nilo Legowo: Conceptualization, Methodology, Supervision, Validation, Writing - Review and Editing, Project Administration.

DATA AVAILABILITY STATEMENT

The aggregated datasets and research instruments analyzed during this study are publicly available in the Zenodo repository at https://doi.org/10.5281/zenodo.20103920 under a Creative Commons Attribution 4.0 International (CC BY 4.0) license. Raw primary data, including interview transcripts, internal incident reports, internal IT audit findings, and per-respondent questionnaire data, are not publicly available due to commercial-confidentiality agreements with the case organisation.

CONFLICTS OF INTEREST

The first author is employed as the IT Manager of the case organisation; this insider position provided the study's access to systems and informants and was the basis for the risk scoring described in the Methodology. The authors declare no other competing interests.

ACKNOWLEDGMENT

The authors express their deepest gratitude to the management of the case organisation for granting permission

and trust to conduct this research, and to the six key informants and 30 survey respondents who generously shared their time and insights to ensure the success of this study. The first author also thanks Prof. Nilo Legowo, for his invaluable guidance, reviews, feedback, and support throughout the writing of this paper. Sincere appreciation is also extended to the Master of Information Systems Management Program, BINUS Graduate Program, Bina Nusantara University, for the academic support provided during this research.

REFERENCES

[1] Saeed, S., Altamimi, S.A., Alkayyal, N.A., Alshehri, E., Alabbad, D.A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. Sensors, 23(15): 6666. https://doi.org/10.3390/s23156666

[2] BSSN. (2025). Lanskap keamanan siber Indonesia 2024. https://ppid.bssn.go.id/api/ppid-document/Informasi-serta-merta/lanskap-keamanan-siber-indonesia/Lanskap%20Keamanan%20Siber%20Indonesia%202024.pdf.

[3] IBM Security. (2025). Cost of a data breach report 2025. https://www.ibm.com/reports/data-breach.

[4] Whitman, M.E., Mattord, H.J. (2009). Principles of Information Security. Boston, MA: Thomson Course Technology.

[5] Usmany, E.K., Legowo, N. (2025). Information security planning with risk management using ISO 31000:2018 at e-commerce XYZ. Journal of Information Systems Engineering and Management, 10(33s): 75-89. https://doi.org/10.52783/jisem.v10i33s.5460

[6] Yonatan, A.Z., Susanto, S., Sukapto, P., Zagloel, T.Y.M., Timotius, E. (2025). Navigating risks with ISO 31000 for a sustainable future: A strategic approach in the Indonesia textile industry. Management Systems in Production Engineering, 33(2): 82-92. https://doi.org/10.2478/mspe-2025-0009

[7] Hardjomidjojo, H., Pranata, C., Baigorria, G. (2022). Rapid assessment model on risk management based on ISO 31000:2018. IOP Conference Series: Earth and Environmental Science, 1063(1): 012043. https://doi.org/10.1088/1755-1315/1063/1/012043

[8] Hardianti, S., Riadi, I. (2022). Service risk assessment learning management system using ISO 31000:2018/31010. International Journal of Computer Applications, 184(4): 1-11. https://doi.org/10.5120/ijca2022921993

[9] Smirnova, E., Larionov, A., Shkarovskiy, A. (2023). Risk management model in ISO-standards as the implementation of environmental safety for housing construction. Rocznik Ochrona Srodowiska, 25: 282-288. https://doi.org/10.54740/ros.2023.030

[10] Majerník, M., Daneshjo, N., Malega, P., Drábik, P., Ševčíková, R., Vravec, J. (2023). Integrated management of the environment-safety risks in the thermal power station. Polish Journal of Environmental Studies, 32(5): 4725-4738. https://doi.org/10.15244/pjoes/168290

[11] Kristanti, F.T., Riyadh, H.A., Ginting, E.S.B., Beshr, B.A.H. (2024). Exploring the level of realm disclosure for Indonesian insurance business using ISO 31000. Journal of Infrastructure, Policy and Development, 8(8): 1-25. https://doi.org/10.24294/jipd.v8i8.5865

[12] Purwanti, L., Triyuwono, I., Maski, G., Pusposari, D., Prakoso, A., Ibrahim, M. (2025). The impact of ISO 31000 adoption on the performance of banking companies in Indonesia. Cogent Business & Management, 12(1): 2507222. https://doi.org/10.1080/23311975.2025.2507222

[13] Sulistiyowati, W., Suef, M., Singgih, M.L. (2025). Integrating ISO 31000 with POAC: A novel framework for risk management in quality improvement projects. Journal of Information Systems Engineering and Management, 10(34s): 184-201. https://doi.org/10.52783/jisem.v10i34s.5787

[14] Berrada, H., Boutahar, J., El Houssaini, S.E.G. (2023). Roadmap and information system to implement information technology risk management. International Journal of Safety and Security Engineering, 13(6): 987-1000. https://doi.org/10.18280/ijsse.130602

[15] Parviainen, T., Goerlandt, F., Helle, I., Haapasaari, P., Kuikka, S. (2021). Implementing Bayesian networks for ISO 31000:2018-based maritime oil spill risk management: State-of-art, implementation benefits and challenges, and future research directions. Journal of Environmental Management, 278: 111520. https://doi.org/10.1016/j.jenvman.2020.111520

[16] Sahibu, S., Sakti, A., Iskandar, A. (2024). Risk management analysis of SMK Telkom Makassar's integrated academic information system in compliance with ISO 31000 standards. Ingenierie des Systemes d'Information, 29(1): 205-218. https://doi.org/10.18280/isi.290121

[17] Shostack, A. (2014). Threat Modelling: Designing for Security. John Wiley & Sons.

[18] Antunes, M., Maximiano, M., Gomes, R., Pinto, D. (2021). Information security and cybersecurity management: A case study with SMEs in Portugal. Journal of Cybersecurity and Privacy, 1(2): 219-238. https://doi.org/10.3390/jcp1020012

[19] Monazzam, A., Crawford, J. (2024). The role of enterprise risk management in enabling organisational resilience: A case study of the Swedish mining industry. Journal of Management Control, 35(1): 59-108. https://doi.org/10.1007/s00187-024-00370-9

[20] Al-Dosari, K., Fetais, N. (2023). Risk-management framework and information-security systems for small and medium enterprises (SMEs): A meta-analysis approach. Electronics, 12(17): 3629. https://doi.org/10.3390/electronics12173629

[21] Tambunan, P.N.P., Legowo, N., Tambunan, D.R. (2024). Strengthening payment card data security: A study on compliance enhancement and risk mitigation through MFA implementation under PCI DSS 4.0. Journal of Theoretical and Applied Information Technology, 102(9): 4093-4102. https://www.jatit.org/volumes/Vol102No9/31Vol102No9.pdf.

[22] International Organization for Standardization. (2018). ISO 31000:2018 risk management: Guidelines. Geneva: ISO.

[23] Björnsdottir, S.H., Jensson, P., Thorsteinsson, S.E., Dokas, I.M., De Boer, R.J. (2022). Benchmarking ISO risk management systems to assess efficacy and help identify hidden organizational risk. Sustainability, 14(9): 4937. https://doi.org/10.3390/su14094937

[24] Kosztyán, Z.T., Csizmadia, T., Kovács, Z., Mihálcz, I.

(2020). Total risk evaluation framework. International Journal of Quality and Reliability Management, 37(4): 575-608. https://doi.org/10.1108/IJQRM-05-2019-0167
[25] International Organization for Standardization. (2022). ISO/IEC 27005: 2022 Information security, cybersecurity and privacy protection - Guidance on managing information security risks. Geneva.
[26] Yazo-Cabuya, E.J., Ibeas, A., Rey-Caballero, R. (2025). Multi-criteria decision making for risk management in quality management systems. Sustainability, 17(3): 1092. https://doi.org/10.3390/su17031092
[27] Markovic, P., Stevanovic, D., Kolonja, B., Slavkovic, D., Krzanovic, D. (2025). A hybrid model for risk-based strategic planning in open-pit mining: Integrating deterministic, stochastic, and ISO 31000 approaches. Applied Sciences, 15(5): 2500. https://doi.org/10.3390/app15052500
[28] Prafitia, H.A., Legowo, N. (2025). Risk assessment of information system audit tools based on SPBE risk management guidelines. International Journal of Safety and Security Engineering, 15(7): 1471-1480. https://doi.org/10.18280/ijsse.150714
[29] Ministry of Industry of the Republic of Indonesia. (2018). Making Indonesia 4.0: Indonesia's Strategy to Enter the Fourth Industrial Revolution. https://kemenperin.go.id/artikel/18967/Making-Indonesia-4.0:-Strategi-RI-Masuki-Revolusi-Industri-Ke-4.
[30] Yin, R.K. (2018). Case Study Research and Applications. Thousand Oaks, CA: Sage.
[31] Creswell, J.W., Plano Clark, V.L. (2018). Designing and Conducting Mixed Methods Research. Sage Publications.