EVALUATION OF RISK CULTURE IMPLEMENTATION IN THE DIGITAL INVESTMENT COMPANY PT XYZ

Fanny Wiryana[1]
Universitas Indonesia, Jakarta Pusat, Indonesia
fannywirya@gmail.com

Tubagus Muhammad Yusuf Khudri[2]
Universitas Indonesia, Jakarta Pusat, Indonesia
yusufkh@ui.ac.id

Abstract

This study aims to evaluate the risk culture at digital investment company PT XYZ using the The Institute of Risk Management (IRM) 2012 framework. The research employs a case study design with a qualitative approach. Data were collected through semi-structured interviews and surveys. At the individual level, analysis was conducted using the Risk Type Compass and Moral DNA instruments. The Risk Type Compass results indicate that employees at PT XYZ tend to exhibit a relatively balanced tolerance across most risk types. PT XYZ shows a combination of adventurous–deliberate traits (bold yet calm and stable) as well as prudent–intense tendencies (careful and conscientious). Based on the Moral DNA analysis, employees at PT XYZ demonstrate a predominant inclination toward reason ethics in their decision-making processes. At the organizational level, analysis through interviews and the Double S Model shows that PT XYZ's culture falls into the communal category, indicating high levels of social cohesion and solidarity within the organization. Furthermore, evaluation using the eight aspects of the IRM Risk Culture Aspects Model reveals several areas that require improvement, specifically in the following aspects Risk Leadership, Responding to Bad News, Risk Governance, and Risk Resources. Meanwhile, the aspects that are already considered to be relatively strong include Risk Transparency, Risk Competence, Risk Decisions, and Rewarding Appropriate Risk Taking.

Keywords: Risk Culture, IRM 2012, Digital Investment

INTRODUCTION

Alongside the rapid advancement of digital financial technology, various threats have emerged and become increasingly complex. These threats primarily target humans, who often constitute the most easily exploited vulnerabilities. Research by Xia et al. (2020) demonstrates that crypto exchanges have become prime targets for hackers seeking financial gain due to the substantial volume of digital assets stored within them. The hacking incident involving the international cryptocurrency exchange Bybit (Krause, 2025) in February 2025 resulted in losses reaching IDR 22 trillion. The attack exploited weaknesses in Bybit's multisig cold-wallet framework, transaction interface design, and verification processes involving human intervention. According to SecurityWeak (2025), potential vulnerabilities existed within the user-interface system of the Safe.global platform, which may have been exploited during transaction processes to alter smart-contract logic and obscure the signing interface, enabling attackers to take control of cold-wallet assets.

Cyberattacks in the digital financial sector have occurred not only within international crypto exchanges but also domestically. Another domestic case involved Indodax, a crypto-asset trading platform, which suffered losses amounting to USD 22 million (Andjarwirawan et al., 2024). This attack specifically targeted internal staff through spear-phishing cyberattacks. As noted by Zein (2023), spear-phishing refers to attacks aimed at specific individuals or staff groups within an organization by gathering personal information from social-media profiles, company websites, and even employee blogs. In many cases, phishing emails or messages are embedded with malware, such as Trojans, designed to monitor or steal industrial data.

Andjarwirawan et al. (2024) further argue that internal staff are the primary targets of cyberattacks because they represent the most vulnerable entry points within an organization's defense chain. Higbee (2018) emphasizes that cybercrimes such as ransomware and phishing have increased by up to 65% globally, predominantly targeting humans as the weakest link. Most attacks originate from phishing emails capable of deceiving users into granting access to intruders, enabling data theft or malware installation.

Considering global cybersecurity dynamics, PT XYZ is not only exposed to external cyber threats but also to internal risks which, if left unmanaged, may jeopardize the firm's security and reputation. PT XYZ is a digital investment company providing a platform for trading various investment assets such as cryptocurrencies, global stocks, and digital gold. Established in 2021, PT XYZ is officially registered as a fully licensed Digital Financial Asset Trader (PAKD) under the Financial Services Authority (OJK).

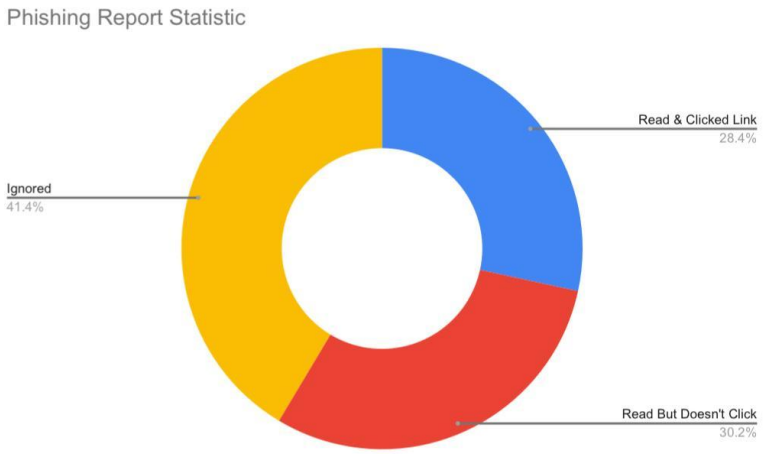

Figure 1
Phishing Report Campaign PT XYZ
Source: Author's reprocessed data (2025)

On June 23rd, 2025, PT XYZ's Security Operations Team conducted an email-phishing campaign aimed at evaluating employee awareness and preparedness toward potential cyber threats transmitted via email. Figure 1 indicates that 41.1% of employees ignored the email without opening it, 30.2% opened but did not click the link, and 28.4% both opened the email and clicked the embedded link. These results reveal that a considerable proportion of employees remain vulnerable to social-engineering tactics by engaging in risky behaviors such as clicking malicious links. Moreover, the results fall significantly short of the internal target set by the Security Operations Team, which requires no more than 14% of employees to open and click phishing links. Notably, some individuals who clicked the link held Senior-level and above positions, who ideally should possess heightened understanding and responsibility regarding information security. This highlights the need for improved cybersecurity awareness and education within PT XYZ.

Currently, PT XYZ does not have a dedicated risk-management department; instead, it is integrated within the Operations and Risk Division. In an initial interview conducted on April 14, 2025, with the Senior Manager in Engineering, several critical incidents were revealed that underscore the weak risk culture within the organization. Issues were identified particularly with respect to information-system infrastructure, especially system resiliency, which should enable rapid and effective responses to technical disruptions. In one case in 2023, the company's services experienced a system outage; however, the access team lacked authorization and capability to resolve the issue independently. Consequently, service recovery required an entire night and resulted in substantial financial losses. This situation demonstrates that risk-management processes are not fully integrated into operational technology functions, which ideally serve as the first line of defense in handling incidents. It indicates that risk culture has not yet been embedded into the daily routines of operational teams.

In an interview with the Senior Manager in Business Intelligence, two additional incidents further highlighted weaknesses in PT XYZ's risk culture, particularly in data management and customer-service processes. One notable incident involved a client discovering that their data was stored in a Google Sheet accessible to multiple parties without

proper access restrictions for instance, using the "anyone can view" option. This not only violates basic principles of data privacy and security but also reveals inadequate internal controls and a lack of risk-mitigation procedures. As a result, the client lost trust in the company and terminated the business relationship. This demonstrates that inadequate awareness and mismanagement of risks especially those related to data governance can directly impact business continuity and corporate reputation.

Beyond technical and external aspects, internal behaviors also reflect risk-culture weaknesses. One example occurred when an employee discovered sensitive information about a colleague through the access portal and directly confronted them. This was disclosed during an offline security-awareness training for all employees on March 20, 2025. Although no system-level violation occurred, the incident illustrates a lack of understanding regarding ethical information usage and professional boundaries. In an organization with a strong risk culture, employees are expected to recognize the implications of their actions, especially when handling sensitive data and interpersonal trust. This situation highlights that awareness of non-technical risks such as reputational and behavioral risks remains insufficient within the organization.

In addition to data-security issues, problems have also arisen in the fund-deposit and withdrawal processes due to internal errors. These failures resulted in service disruptions and customer dissatisfaction, prompting some clients to discontinue using the company's services. In this context, the weak risk culture is reflected in the absence of early-warning systems, transactional-risk evaluations, and robust contingency planning. The inability to deliver reliable and consistent financial services constitutes an operational risk that should have been anticipated through continuous risk assessment.

As an organization, including digital-investment firms such as PT XYZ, assessing the level of risk culture is essential. However, available tools for comprehensively evaluating organizational risk culture remain limited. One of the most recognized frameworks is the Risk Culture Framework developed by The Institute of Risk Management (IRM). This framework provides a systematic evaluation approach, starting from the individual level up to the organizational level.

The IRM (2012) framework, published under the title *Risk Culture: Resources for Practitioners*, was developed as a guide to understanding, assessing, and strengthening risk culture within organizations. IRM emphasizes that risk culture is a key pillar of effective risk-management systems, as it shapes how individuals and groups identify, understand, and respond to risks.

In the context of digital-investment companies, a strong risk-aware culture plays an increasingly critical role. PT XYZ, which operates in a digital financial-services environment characterized by high operational, cyber, and compliance risks, requires a robust foundation of risk culture. Although the company continues to grow as a digital entity, it has not yet conducted an in-depth evaluation of its risk-aware culture using standardized frameworks. Strengthening risk culture therefore becomes a fundamental pillar for ensuring successful, comprehensive, and sustainable risk-management implementation.

Given the critical importance of risk-aware culture at PT XYZ based on the initial findings, it is evident that the company still faces various shortcomings in applying risk-culture principles, resulting in overlooked risks. Therefore, this study is essential to identify and understand organizational behaviors that underpin weak risk-management practices.

Consistent with Vidiarto et al. (2023), risk culture is closely linked to individual behavior within an organization. Accordingly, the objective of this study is to evaluate the extent to which risk culture has been implemented at PT XYZ and to assess the level of employee awareness and behavioral consistency in applying risk-culture principles in daily operations using the IRM 2012 framework as the analytical basis. The results of this study are expected to contribute to improving organizational risk culture and adding value to the digital-investment industry.

RESEARCH METHOD

Research Design

This study adopts a qualitative research design using a case study approach. The case study method enables an in-depth investigation of a specific phenomenon within its real organizational context through the systematic collection and analysis of empirical data. As noted by Ellet (2018), a case study represents a verbal reconstruction of an authentic situation that places the reader in the position of a decision-maker, allowing the dynamics of real-world conditions to be explored through narratives, documents, and other forms of evidence.

To achieve a comprehensive understanding of the risk culture within PT XYZ, this study integrates two primary sources of data: semi-structured interviews with senior managers and a structured survey administered to employees across relevant divisions.

Data Collection Methods

Semi-structured interviews were conducted to explore managerial perspectives on the organization's risk culture. The interviews followed an open-ended question format, allowing respondents to articulate their experiences and interpretations freely (DiCicco-Bloom & Crabtree, 2006; Alsaawi, 2014). The interview guide was developed based on the IRM (Institute of Risk Management) Risk Culture Framework (2012) and refined to capture contextual nuances specific to PT XYZ.

Given the limited availability of informants, interviews were conducted asynchronously using an online shared document. Participants provided written responses directly in the document, ensuring flexibility while maintaining depth of insight. Ethical research principles were upheld by securing informed consent and guaranteeing anonymity, consistent with recommendations by Saunders et al. (2015).

Informant	Position (Anonymized)
Informant 1	Senior Manager (Data & Analytics Division)
Informant 2	Senior Manager (Security Division)
Informant 3	Senior Manager (Legal & Compliance Division)
Informant 4	Senior Manager (Operations & Risk Division)
Informant 5	Senior Manager (Finance Division)

Purposive sampling was used to select five senior managers with more than five years of professional experience in risk-related roles. Their strategic positions were deemed essential for providing a holistic understanding of organizational risk practices (Bryman, 2004). Table 1 presents the list of interviewees and their respective roles within the company.

To complement managerial perspectives, a structured survey was distributed to employees of PT XYZ. Surveys are particularly effective for evaluating organizational risk culture from the standpoint of employees, who often possess crucial insights into how risk structures function in practice (Sheedy & Griffin, 2017).

The survey consisted of two sections:

1. **Respondent Demographics**
   Participants provided information on gender, position, division, and tenure. These data were also used to assess Moral DNA characteristics.
2. **Risk Culture Assessment**
   The survey comprised three validated instruments:
   - **Risk Type Compass** (16 items; five-point Likert scale) capturing individual risk perception profiles.
   - **Moral DNA** (18 items; five-point Likert scale) assessing ethical reasoning and personal values.
   - **Double S Model** (14 items; three-point Likert scale) evaluating structural and social dimensions of organizational culture.

Responses were analyzed using mean-score aggregation to generate representative characteristics for each construct. This method mitigates the influence of extreme responses and provides a balanced overview of organizational trends. The survey was administered via Google Forms to 35 employees across seven divisions, including both junior and senior staff. Twenty-six respondents had more than two years of tenure, enhancing the reliability of insights regarding organizational dynamics.

Data Analysis

Interview data were analyzed using a narrative analysis approach. Narrative analysis emphasizes that stories are socially constructed representations shaped by personal experience and contextual factors, rather than purely objective accounts (Afan Faizin, 2020; McLeod, 2024). Interview responses were categorized into four major themes and eight subthemes derived from the IRM model, then compared across participants to identify convergent and divergent perspectives.

Survey data were analyzed using descriptive statistics (Anderson et al., 2024; Fisher & Marshall, 2009). All responses were converted to Likert-scale values and processed using Microsoft Excel through pivot tables and visualized using cluster column charts and spidergrams. The descriptive results captured patterns in individual risk perceptions, ethical orientations, and organizational cultural attributes.

Triangulation was conducted by integrating findings from interviews, survey results, and the IRM Risk Culture Framework. This process strengthened the validity of the nalysis by cross-checking insights from multiple data sources to arrive at a comprehensive depiction of the risk culture at PT XYZ.

Mitigation of Research Bias

Potential biases inherent in interview and survey research, such as response bias, social desirability bias, and confirmation bias, were acknowledged (Populix, 2024). Given the sensitivity of risk culture issues, respondents might be inclined to present favorable views of the organization. Furthermore, the researcher's preconceptions might influence data interpretation.

To mitigate these risks, all questionnaire and interview items were designed in neutral wording, and respondents were assured confidentiality and anonymity to foster honest participation. Triangulation across data sources also reduced interpretive bias and enhanced the robustness of research findings.

RESULTS AND DISCUSSION

Descriptive Analysis

Risk Type Compass

The Risk Type Compass assessment provides insight into the dominant behavioral tendencies that shape decision-making patterns within PT XYZ. According to Trickey (2016), individual risk behavior is influenced by two core factors: (1) the degree of courage and low anxiety, and (2) impulsivity driven by curiosity and sensation seeking. These factors form eight distinct risk types, along with an Axial group representing a neutral and balanced disposition.

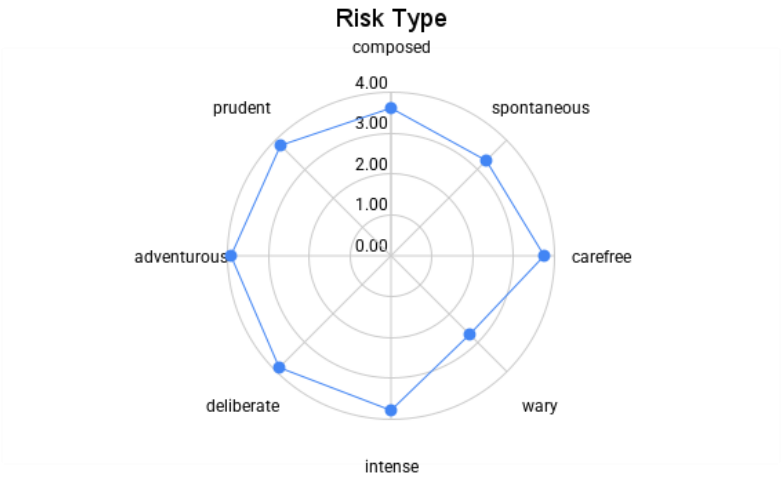

Figure 2
Risk Type PT XYZ

Figure 2 illustrates the aggregated spidergram profile generated from the survey results using mean scores for each risk category. Overall, PT XYZ exhibits a relatively balanced distribution across the eight risk types, with most dimensions falling within the range of 3 to 4 on the Likert scale. This pattern indicates that the organization does not lean toward any extreme behavioral orientation but instead reflects a moderate and adaptable risk disposition.

Table 3.
Mean Scores of Risk Type Dimensions

Risk Type	Mean Score
Composed	3.60
Spontaneous	3.29
Carefree	3.74

Risk Type	Mean Score
Wary	2.74
Intense	3.78
Deliberate	3.86
Adventurous	3.91
Prudent	3.81

The highest scores appear in the Adventurous (3.91) and Deliberate (3.86) dimensions. This combination suggests that PT XYZ demonstrates a controlled yet assertive approach to risk-taking—bold enough to pursue opportunities while maintaining analytical and calculated decision-making. Similarly, the strong Prudent (3.81) and Intense (3.78) dimensions indicate that employees possess a strong drive to achieve organizational objectives, accompanied by cautious evaluation when addressing potential risks.

The Composed score (3.60) implies that employees generally maintain emotional stability and composure under pressure, reflecting resilience in dynamic operational environments. Meanwhile, Carefree (3.74) and Spontaneous (3.29) highlight the organization's flexibility and responsiveness when navigating changes or emerging conditions.

The Wary dimension shows the lowest score (2.74), signaling that PT XYZ does not display overly defensive or risk-averse tendencies. This lower level of caution aligns with the high Adventurous score, indicating a willingness to move forward despite uncertainties. Such a profile suggests that the organization values progress, innovation, and strategic risk-taking rather than maintaining conservative or protective postures.

The overall risk profile situates PT XYZ within a moderate and balanced risk posture, characterized by a blend of calculated boldness and structured decision-making. This alignment between Adventurous, Deliberate, and Prudent tendencies reflects a culture where employees are encouraged to take initiative, provided that decisions remain grounded in rational analysis. Such a profile is particularly advantageous for organizations operating in dynamic sectors where innovation and adaptability are required, yet risk exposures must be managed responsibly.

The relatively low Wary score may also indicate an organizational culture that fosters confidence, openness to experimentation, and collective readiness to navigate uncertainties. However, this may also suggest potential vulnerabilities if caution and due diligence are not sufficiently emphasized in high-risk operational contexts. Therefore, strengthening structured risk communication and scenario-based decision frameworks may help ensure that strategic boldness is balanced with effective risk controls.

Overall, the Risk Type Compass results affirm that PT XYZ possesses a well-rounded and adaptive risk culture, characterized by a strategic blend of courage, prudence, responsiveness, and emotional stability. This profile provides a strong foundation for fostering risk-aware behavior and supporting sustainable organizational performance.

Moral DNA

The Moral DNA assessment was employed to examine the balance of ethical values among employees at PT XYZ, focusing on three core ethical dimensions: obedient ethics,

reason ethics, and care ethics as defined by the IRM (2012). Ten underlying moral values shape these ethical orientations and significantly influence the quality of everyday decision-making within an organizational context. Respondents' scores were analyzed based on gender, job level, age group, and length of experience to provide a multidimensional understanding of personal ethics within the company.

Figure 3 compares the moral profiles of male and female employees across the three ethical dimensions. Overall, both groups recorded moderately high average scores, indicating a generally well-developed moral awareness in decision-making.

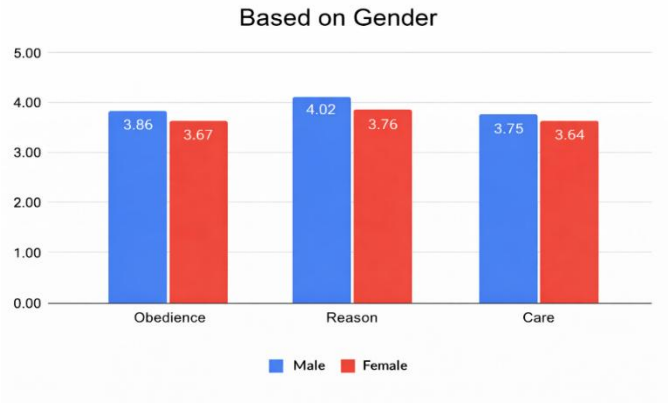

Figure 3
Personal Ethics Based on Gender

Male employees scored slightly higher in all dimensions: obedient ethics (3.86 vs. 3.67), reason ethics (4.02 vs. 3.76), and care ethics (3.75 vs. 3.64). These results suggest that men tend to be more rule-oriented, more logic-driven, and marginally more empathetic in workplace decision-making. However, the score differences remain small, indicating that both groups demonstrate relatively similar ethical commitments. The findings reinforce that gender does not create substantial variation in moral orientation within PT XYZ, and the organizational ethical climate appears cohesive.

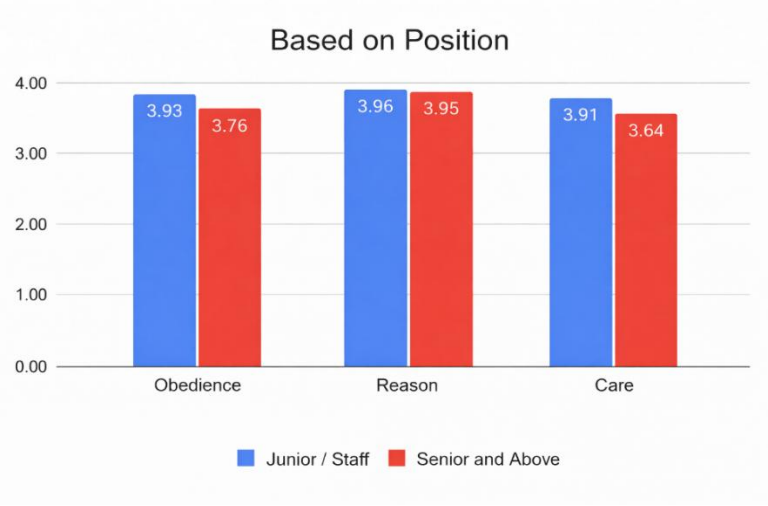

Figure 4
Personal Ethics Across Job Levels

Figure 4 compares ethical tendencies between Junior staff and Senior-level employees. Interestingly, Juniors consistently scored slightly higher across all three dimensions: obedient ethics (3.93 vs. 3.76), reason ethics (3.96 vs. 3.95), and care ethics (3.91 vs. 3.64). This pattern aligns with Steare et al. (2015), who found that non-managerial employees tend to exhibit higher compliance.

Junior employees' elevated scores may reflect a stronger desire to align with organizational expectations during early career stages. They demonstrate not only higher adherence to rules but also a more pronounced sense of empathy toward colleagues. Meanwhile, Senior employees show comparable but lower scores, which may be attributed to greater autonomy, role complexity, and broader strategic responsibilities that shape their ethical reasoning differently.

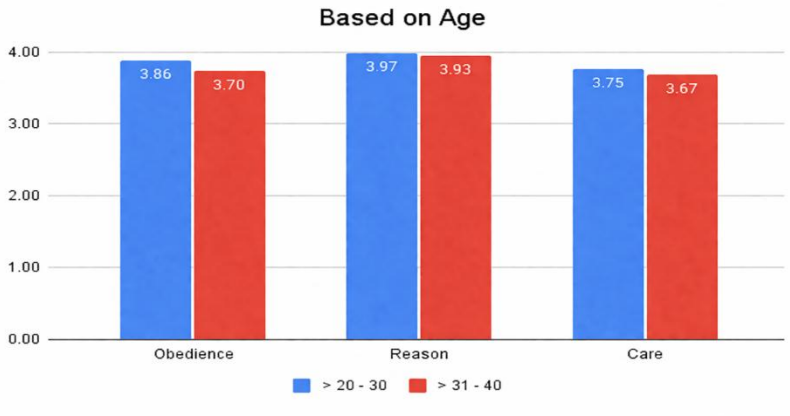

Figure 5
Personal Ethics Across Age Categories

Figure 5 presents differences in ethical tendencies between employees aged 20–30 years and 31–40 years. Younger employees recorded slightly higher scores in obedient ethics (3.86 vs. 3.70) and care ethics (3.75 vs. 3.67), suggesting a greater inclination toward following rules and demonstrating empathy. In contrast, employees aged 31–40 scored marginally higher in reason ethics (3.97 vs. 3.93), reflecting more mature logical reasoning and informed judgment driven by experience.

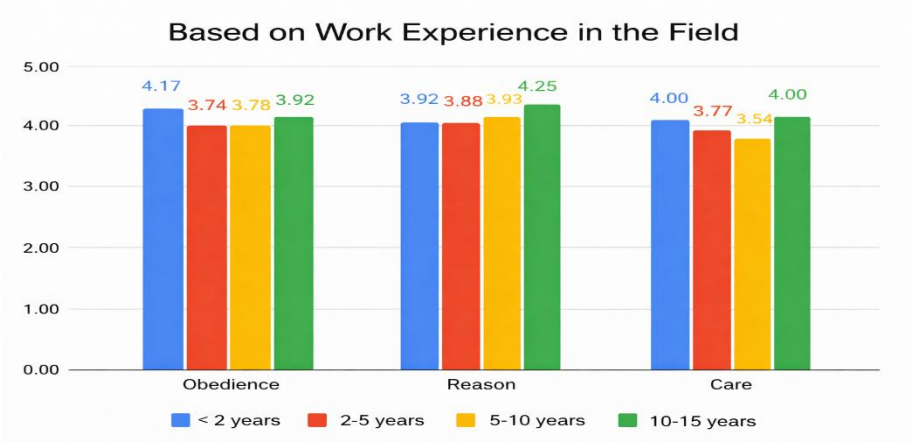

Figure 6
Personal Ethics According to Experience in the Relevant Field

Figure 6 examines ethical scores based on years of experience in the respondents' fields. Employees with less than two years of experience recorded the highest score in obedient ethics (4.17), reinforcing the pattern observed among younger and junior staff. Their heightened compliance likely reflects their need to adapt to organizational norms.

In contrast, reason ethics peaked among employees with 10–15 years of experience (4.25), followed by those with 5–10 years (3.93). This suggests that longer tenures cultivate stronger analytical and logic-based decision-making, likely due to accumulated expertise and exposure to complex organizational scenarios.

For care ethics, both the most junior (<2 years) and the most senior (10–15 years) employees scored highest (4.00). This U-shaped pattern indicates that empathy is strongest among newcomers who are still building workplace relationships and among highly experienced employees who typically assume mentoring or stewardship roles.

Overall, the experience-based patterns highlight a progression from compliance-driven ethics among newer employees to reason-driven and care-oriented ethics among more seasoned staff.

Across gender, job level, age, and experience, Moral DNA results reveal that PT XYZ's workforce demonstrates a balanced ethical profile, with consistently moderate-to-high scores across all moral dimensions. The findings suggest:

1. **Compliance is strongest among younger and newer employees**, indicating robust internalization of organizational rules during early career stages.
2. **Rational and logic-driven ethics strengthen with experience**, highlighting the role of accumulated knowledge in shaping ethical judgment.
3. **Empathy is highest among the least and most experienced employees**, reflecting transitional and leadership-based moral dynamics.
4. **Gender differences are minimal**, demonstrating a uniform ethical climate.

Collectively, these findings suggest a workplace culture characterized by moral coherence, disciplined behavior, and a strong foundation for ethical decision-making. Such an ethical landscape provides an essential pillar for cultivating a healthy and sustainable risk culture in the organization.

Double S

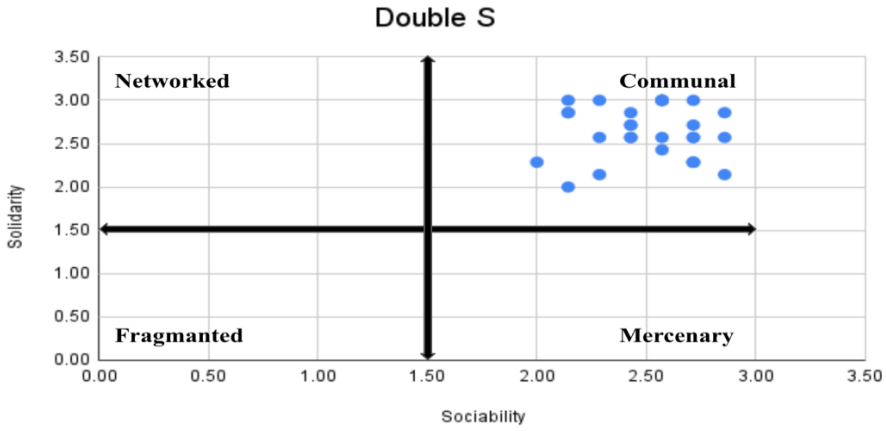

Figure 7
Double S Method

Figure 7 presents the results of the Double S Method survey, which maps the position of PT XYZ employees across two key dimensions: solidarity and sociability. This method is applied to assess organizational culture by examining the extent to which workplace relationships are shaped by social closeness (sociability) and professional cooperation driven by shared goals (solidarity).

The processed survey data show that most respondents are concentrated in the upper-right quadrant, representing high solidarity and moderate to high sociability. This position indicates that PT XYZ tends to exhibit a communal organizational culture. The high level of solidarity reflects employees' strong orientation toward achieving the company's vision and objectives. Meanwhile, the sociability scores ranging from moderate to high suggest that employees also value positive interpersonal relationships in the workplace. According to Goffee and Jones (1996), this cultural type describes employees who demonstrate a strong commitment to collective goals while simultaneously maintaining cooperative and supportive interpersonal interactions.

However, a communal culture is often challenging to sustain in many business contexts. First, high levels of sociability and solidarity commonly emerge under the influence of a charismatic founder or leader; once such leaders leave the organization, the strength of social ties often weakens. Second, strong sociability within communal cultures frequently conflicts with organizational demands during periods of growth, diversification, or international expansion (Goffee & Jones, 1996).

Narrative Analysis

The evaluation of the company's risk culture was conducted with reference to the framework of the Institute of Risk Management (IRM, 2012). In this study, the IRM Aspect Model is employed to analyze eight key issues of risk culture, which are subsequently categorized into four primary dimensions: Tone at the Top, Governance, Competency, and Decisions. The information was obtained through in-depth interviews with five informants who hold managerial positions and possess extensive work experience within the company.

Table 4
Risk Culture Evaluation Based on the IRM Aspect Model

Aspect	Expectation	Summary	Evaluation, Recommendations, and Suggestions
1. Risk Leadership	Senior management sets strategic direction and clear expectations for risk management and serves as a role model for risk-based decision-making.	• Top management's commitment to risk management is evident through formal policies, verbal communication, and annual reviews of the Risk Register. • Management consistently reiterates the importance of good governance and sound risk management practices. • Management demonstrates concrete actions in applying	The implementation of Risk Leadership at PT XYZ meets the IRM 2012 criteria; however, improvements are recommended: 1) Conduct Risk Register reviews more frequently, preferably quarterly.

Aspect	Expectation	Summary	Evaluation, Recommendations, and Suggestions
		risk management in decision-making, strategic directions, and budgeting processes.	
2. Responding to Bad News	Management encourages transparency in reporting both positive and negative risk information and values openness in risk disclosure.	• The organization promotes transparency in reporting good and bad news through a tiered reporting process from staff to the Board, without penalizing reporters. Issues are reviewed to ensure accuracy before distribution. • Employees reporting critical issues are supported through a protected whistleblowing mechanism. Although no formal rewards exist, speak-up behavior is highly appreciated.	The implementation meets IRM 2012 criteria; however, improvements are suggested: 1) Formalize and socialize the whistleblowing mechanism to all employees. 2) Establish formal recognition for whistleblowers.
3. Risk Governance	Responsibilities and accountabilities for risk management are clearly defined and aligned with business objectives.	• Accountability and risk ownership are clearly established through the assignment of risk owners in each unit. • Risk prevention and management processes are consistently documented through policies, RACI matrices, the risk register, and online records, and communicated in internal and cross-functional meetings. • Risk review and monitoring processes are conducted in a structured and phased manner through two-way communication, periodic meetings, and SOP enforcement.	Implementation meets IRM 2012 criteria; however: • The three lines of defense should be strengthened by establishing an internal audit team, which is currently not available.
4. Risk Transparency	Risk information is communicated in a timely and relevant manner to enable effective action by decision-makers.	• Risk information is communicated transparently through routine reports and escalation of critical issues. • Strategic direction is clearly conveyed through documented risk appetite and	The implementation of Risk Transparency at PT XYZ fully meets IRM 2012 criteria.

Aspect	Expectation	Summary	Evaluation, Recommendations, and Suggestions
		risk tolerance statements. • Successful risk-taking is acknowledged through sharing sessions, and lessons learned from adverse events are conducted through post-mortem reviews and root cause analysis (RCA) to strengthen policies and procedures.	
5. Risk Resources	The risk function has adequate mandate, resources, and expertise to support effective risk management.	• The risk function has direct access to senior management through formal reporting lines and strategic forums within the Ops and CX teams. • The risk function operates effectively with existing resources, although team capacity remains limited. Key risk discussions are facilitated through cross-unit forums and risk workshops.	Implementation meets IRM 2012 criteria; however: • Establish an independent risk management department to ensure stronger oversight, evaluation, and risk-control functions aligned with organizational mandates.
6. Risk Competence	Leaders and employees are encouraged to enhance awareness, training, and competence in risk management.	• Competence in risk management is recognized as a critical organizational asset. • The organization supports capability building through internal training, professional certification, and continuous learning programs. Competencies such as “Risk Awareness” and “Risk Mindfulness” are formally defined but not yet comprehensively implemented. • Risk awareness is reinforced through routine communication by top management and the risk team during weekly meetings.	The implementation of Risk Competence meets IRM 2012 criteria.
7. Risk Decisions	Decision-making incorporates high-quality risk	• Risk information is presented transparently and made available in a timely	The implementation of Risk Decisions meets IRM 2012 criteria.

Aspect	Expectation	Summary	Evaluation, Recommendations, and Suggestions
	information, and risk awareness is reflected in all strategic processes.	manner to decision-makers. • Risk reports are submitted periodically through formal reporting mechanisms, ensuring management has access to relevant information before major decisions. • Risk analysis forms part of key decision-making processes, including investment evaluations, new project assessments, and strategic planning, although still concentrated at the unit level.	
8. Rewarding Appropriate Risk Taking	Appropriate risk-taking is rewarded while inappropriate behavior is sanctioned; risk awareness is embedded in performance criteria and leadership development.	• Appropriate risk-taking behavior is encouraged through informal recognition. • Successful risk management practices are used as best practices to strengthen positive risk culture. • Significant negative consequences due to poor risk-taking or failure to report risks may result in coaching, evaluation, or formal sanctions (e.g., written warnings).	The implementation of this aspect meets IRM 2012 criteria.

CONCLUSION

This study demonstrates that PT XYZ operates within a high-risk digital-investment environment in which cyber threats, operational disruptions, and internal behavioral vulnerabilities pose substantial challenges to organizational security and resilience. A review of past incidents, ranging from phishing attacks and credential breaches to data-management failures and system outages, reveals that weaknesses in risk culture remain a critical root cause of recurring risk exposures. Although PT XYZ continues to grow as a licensed Digital Financial Asset Trader under the Financial Services Authority (OJK), its risk-management practices have not yet been fully supported by a deeply embedded risk-aware culture.

Through a qualitative case study combining managerial interviews, a structured survey, and the IRM (2012) Risk Culture Framework, this research finds that risk culture at PT XYZ reflects both strengths and significant gaps. The Risk Type Compass results indicate that employees exhibit a balanced and adaptable behavioral profile, characterized by

deliberate, prudent, and adventurous tendencies that support innovation and opportunity-seeking. Emotional stability and responsiveness further contribute to a moderate and constructive risk posture. However, low scores in the Wary dimension suggest that insufficient caution may contribute to complacency in high-risk operational settings.

The Moral DNA assessment shows that employees across gender, job levels, age groups, and experience categories generally display moderate to high ethical awareness. While junior and younger employees exhibit stronger rule compliance and empathy, senior and more experienced staff demonstrate slightly higher reason-based judgment. These findings reflect a broadly cohesive ethical climate, though variations in ethical emphasis may influence consistency in risk-related decisions.

Despite these positive characteristics, the organizational practices identified through interviews expose substantial risk-culture weaknesses. These include inconsistent data-governance behavior, inadequate access controls, the misuse of communication channels, insufficient system resiliency, ethical misjudgments in handling sensitive information, and a lack of early-warning mechanisms for operational processes. These behavioral and procedural gaps indicate that risk-culture principles have not yet been internalized across daily operations, particularly in areas that require vigilance, accountability, and proactive risk mitigation.

Overall, the study concludes that PT XYZ must strengthen its risk-aware culture by institutionalizing structured risk-management practices, enhancing data-protection systems, improving governance mechanisms, and implementing sustained cybersecurity and ethical-behavior training. Embedding risk culture at both the individual and organizational levels is essential for ensuring operational reliability, protecting corporate reputation, and supporting sustainable growth in the increasingly complex digital-financial sector. The findings contribute practical insights for digital-investment companies seeking to reinforce their risk-management foundations and build resilient organizational cultures capable of withstanding evolving cyber and operational threats.

REFERENCES

Afan Faizin. (2020). Narrative research: A research design. *Jurnal Disastri (Jurnal Pendidikan Bahasa dan Sastra Indonesia)*, 2(3), 142–148. https://doi.org/10.33752/disastri.v2i3.1139

Alsaawi, A. (2014). A critical review of qualitative interviews. *European Journal of Business and Social Sciences*, 3(1), 149–156. https://doi.org/10.2139/ssrn.2819536

Anderson, D. R., Sweeney, D. J., Williams, T. A., Camm, J. D., & Cochran, J. J. (2024). *Statistics for business and economics*.

Andjarwirawan, J., Santoso, L. W., & Gunadi, K. (2024). Cybersecurity threats through phishing attacks targeting internal staff: Mitigation and prevention. *IJAREEIE*, 13(12), 1–7. https://doi.org/10.15662/IJAREEIE.2024.1312001

Bryman, A. (2004). Qualitative research on leadership: A critical but appreciative review. *The Leadership Quarterly*, 15(6), 729–769. https://doi.org/10.1016/j.leaqua.2004.09.007

DiCicco-Bloom, B., & Crabtree, B. F. (2006). The qualitative research interview. *Medical Education*, 40(4), 314–321. https://doi.org/10.1111/j.1365-2929.2006.02418.x

Fisher, M. J., & Marshall, A. P. (2009). Understanding descriptive statistics. *Australian Critical Care*, 22(2), 93–97. https://doi.org/10.1016/j.aucc.2008.11.003

Goffee, R., & Jones, G. (1996). What holds the modern company together. *Harvard Business Review*.

Higbee, A. (2018). The role of crypto-currency in cybercrime. *Computer Fraud & Security*, 2018(7), 13–15. https://doi.org/10.1016/S1361-3723(18)30064-2

IRM. (2012). *Risk culture: Resources for practitioners*.

Krause, D. S. (2025). The $1.4 billion Bybit hack. *International Journal of Cryptocurrency Research*, 5(1), 52–62. https://doi.org/10.51483/ijccr.5.1.2025.52-62

McLeod, S. (2024). *Narrative analysis in qualitative research*.

Populix. (2024). 8 cara menghindari bias penelitian.

Saunders, B., Kitzinger, J., & Kitzinger, C. (2015). Anonymising interview data. *Qualitative Research*, 15(5), 616–632. https://doi.org/10.1177/1468794114550439

Sheedy, E., & Griffin, B. (2017). Risk governance and culture. *Corporate Governance*, 26(1), 4–22. https://doi.org/10.1111/corg.12200

Trickey, G. (2016). *Risk type compass*.

Vidiarto, A., et al. (2023). Pengaruh budaya peduli risiko. *Bullet: Jurnal Multidisiplin Ilmu*, 2(4), 982–991.

Xia, P., et al. (2020). Characterizing cryptocurrency exchange scams. *Computers & Security*, 98. https://doi.org/10.1016/j.cose.2020.101993

Zein, A. (2023). Analisa penyerangan cyber security social engineering. *Jurnal Informatika Universitas Pamulang*, 8(4), 642–648. https://doi.org/10.32493/informatika.v8i4.35931