

Article

Security and Resilience of Tourism Sector Entities: An Integrated Risk-Based Management Approach

Mardonova Malika Asatilloeyvna¹

1. International University of Tourism and Cultural Heritage "Silk Road", independent researcher

* Correspondence: malikakamron2017@gmail.com

Abstract: The rapid expansion and digitalisation of international tourism have increased the range and intensity of security risks faced by tourism enterprises. Hotels, tour operators, travel agencies, transport providers, catering businesses and other tourism entities are exposed to physical, occupational, sanitary, digital, financial, reputational and supply-chain risks, and a failure in one link of the service chain can quickly affect the whole tourism product and the image of the destination. The purpose of this article is to develop an integrated risk-based framework for strengthening the security and organisational resilience of tourism-sector entities. The study applies content and comparative analysis of peer-reviewed literature and international risk-management standards, risk classification, descriptive analysis of official tourism statistics of the Republic of Uzbekistan for 2020–2025 and conceptual modelling. The analysis shows that foreign tourism-purpose visits to Uzbekistan increased from 1.50 million in 2020 to approximately 11.68 million in 2025, which enlarges the volume of service interactions in which incidents may occur. On this basis, the article proposes the Tourism Entity Security and Resilience Model (TESRM), a seven-stage management cycle from risk identification to organisational learning, and the Tourism Entity Security Index (TESI), a weighted diagnostic instrument covering six dimensions: physical and infrastructure safety, occupational and personnel security, information and cybersecurity, financial resilience, partner and supply-chain reliability, and emergency-management capacity. Practical recommendations are formulated for a tiered and proportionate implementation in Uzbek tourism enterprises, particularly SMEs. The study concludes that sustainable destination safety depends on the resilience of the enterprises that deliver tourism services.

Keywords: tourism security, tourism enterprises, risk management, resilience, cybersecurity, occupational safety, crisis management, tourism SMEs, Uzbekistan

Citation: Asatilloeyvna, M. M. Security and Resilience of Tourism Sector Entities: An Integrated Risk-Based Management Approach. American Journal of Economics and Business Management 2026, 9(10), 798-809

Received: 03th Jul 2026

Revised: 18th Aug 2026

Accepted: 05th Sep 2026

Published: 16th Oct 2026



Copyright: © 2026 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>)

1. Introduction

The modern tourism product is created by a network of independent organisations. A single trip can combine the services of an airline, airport, transfer company, hotel, restaurant, guide, attraction, payment provider and digital booking platform. This interdependence creates value for the visitor, but it also means that a disruption in one link may quickly spread across the whole service chain. A hotel data breach, transport accident, food-safety incident or poorly managed emergency is therefore not an isolated operational problem; it can affect traveller confidence, partner relations and the reputation of an entire destination.

The scale of international tourism makes this problem economically significant. UN Tourism reported approximately 1.4 billion international tourist arrivals in 2024, marking

a return to pre-pandemic levels. In the first quarter of 2025, international arrivals increased by a further 5 per cent year on year, exceeding 300 million trips. Such growth increases demand for services, infrastructure and labour, but also enlarges the number of interactions in which operational, health, information and security risks may materialise [1], [2].

The issue is especially important for small and medium-sized enterprises. The International Labour Organization notes that micro, small and medium-sized enterprises represent the majority of tourism, hotel and food-service businesses and workers. At the same time, the sector continues to face problems such as long and variable working hours, informality, weak social protection and shortcomings in occupational safety and health [3]. This combination means that tourism growth may outpace the institutional capacity of individual firms unless safety and resilience become part of routine management.

Uzbekistan provides a relevant setting for this discussion. Official statistics show a rapid increase in foreign visits for tourism purposes, from 1.50 million in 2020 to 7.96 million in 2024 and approximately 11.68 million in 2025 [4], [5]. Rising visitor volumes create opportunities for enterprises, but they also increase the need for reliable service processes, trained staff, protected information systems, safe transport and accommodation, and clear crisis protocols.

Against this background, the purpose of this research is to develop an integrated risk-based approach to the security and resilience of entities operating in the tourism sector. The article focuses not only on the safety of tourists, but on the capability of the tourism organisation itself to prevent disruption, protect people and assets, continue critical operations and learn from incidents.

The theoretical and empirical literature provides the conceptual foundation for the present study. Tourism-security studies traditionally concentrated on hazards faced by visitors: crime, terrorism, health problems, natural disasters, accidents and political instability [6], [7]. Recent research, however, demonstrates that safety is also psychological and behavioural. Xie et al. developed the Tourist Metasafety Framework and, using 650 tourist interviews, identified physiological, psychological and ontological dimensions of perceived safety. Their results show that perceptions of safety influence safety compliance and participation behaviours [8]. This is important because organisational procedures are only effective when travellers and staff understand and follow them.

A second research stream concerns the resilience of the enterprise. Glowka, Eller, Peters and Zehrer analysed 119 face-to-face interviews in small and medium-sized hospitality family enterprises and found that strategic orientation influences how managers perceive business, internal, tourism-specific and external risks [9]. The finding has direct managerial meaning: risk is not only an objective probability but also a matter of managerial awareness. A firm that systematically overlooks internal risks may appear stable until a disruption exposes weaknesses that have accumulated over time. Post-disaster research has further shown that organisational resilience can be assessed quantitatively and compared across tourism sub-sectors [10], while a systematic review of the hotel sector describes disaster resilience as a dynamic and multifaceted capacity and stresses that hotels are an integral part of the communities in which they operate [11].

Occupational safety is another underdeveloped dimension. A 2024 review of 531 academic articles in hospitality and tourism management concluded that worker safety, health and well-being had often remained outside the central research agenda and called for integrated, interdisciplinary approaches [12]. For tourism enterprises this is critical: frontline employees are simultaneously service providers, risk detectors and first responders during many incidents [13].

The methodological foundation of the present study is consistent with ISO 31000:2018, which treats risk management as an organisation-wide process involving identification, analysis, evaluation, treatment, monitoring and communication [14]. ISO 31030:2021 provides a more specific structured approach to organisational travel risks, including threat identification, risk assessment, prevention and mitigation. ISO explicitly notes that ISO 31030 does not directly apply to leisure tourism; therefore, this paper does not present

it as a tourism certification standard. Instead, its risk-management logic is adapted conceptually to enterprise-level tourism security [15].

The literature therefore contains strong but partly separated strands: tourist safety, worker safety, enterprise risk perception, cybersecurity, crisis management and destination resilience. The research gap addressed here is the lack of a simple integrated framework that tourism enterprises can use to connect these risks within one management cycle.

2. Materials and Methods

The study uses a conceptual-analytical design. It does not claim survey results that have not been empirically collected. This distinction is important for methodological transparency: official statistics are used to describe tourism-market dynamics, while the proposed model and index are theoretical instruments to be tested in subsequent empirical research.

Five methods were applied. First, content analysis was used to examine international standards, institutional sources and peer-reviewed literature. Second, comparative analysis was used to identify common elements across tourist safety, occupational safety and enterprise risk management. Third, official statistics from the National Statistics Committee of the Republic of Uzbekistan were used to examine tourism-flow dynamics and entry structure. Fourth, risk classification was applied to group enterprise threats into operationally meaningful categories. Finally, conceptual modelling was used to develop TESRM and the preliminary TESI scoring structure.

For the quantitative descriptive part, annual foreign visits to Uzbekistan for tourism purposes for 2020–2024 are taken from the National Statistics Committee's 2024 tourism-flow report, while the 2025 total is taken from the Committee's 2026 publication. Percentage changes are calculated by the author from these official values [4], [5].

3. Results

3.1. Tourism growth in Uzbekistan and its security implications

Table 1. Foreign citizens arriving in Uzbekistan for tourism purposes, 2020–2025

Year	Foreign visits, million	Year-on-year change
2020	1.504	-
2021	1.881	25.1%
2022	5.233	178.1%
2023	6.626	26.6%
2024	7.957	20.1%
2025	11.680	46.8%

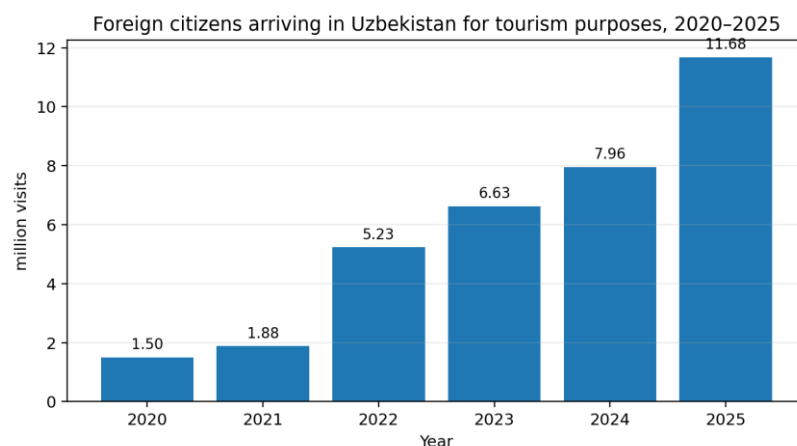


Figure 1. Dynamics of foreign tourism-purpose visits to Uzbekistan, 2020–2025

The figures show two distinct processes. The first is recovery after the pandemic shock: visits increased from 1.50 million in 2020 to 5.23 million in 2022. The second is acceleration after recovery: the indicator rose to 6.63 million in 2023, 7.96 million in 2024 and approximately 11.68 million in 2025. The 2025 level was about 46.8 per cent higher than in 2024 on the basis of the published annual totals. This growth is economically positive, but from a management perspective it also increases the number of transactions, service contacts, transfers, hotel check-ins, digital bookings and situations in which incidents can occur.

The rapid growth of inbound flows is not, by itself, a measure of safety. It is more useful to treat it as an indicator of the scale of the system that has to be managed. Every additional flow of visitors creates more hotel check-ins, transfers, cashless payments, food-service contacts, excursions, guide interactions and digital transactions. When these processes expand faster than internal procedures, staff competence or information security, seemingly small operational weaknesses can become visible to a much larger number of visitors. For this reason, the statistics in this section are interpreted as an argument for stronger organisational capacity rather than as evidence that a destination is either safe or unsafe.

A second implication concerns the diversity of tourism enterprises. Growth in visitor numbers is distributed across large hotels, family guesthouses, transport companies, restaurants, guides, attractions and online intermediaries. These organisations differ sharply in resources and managerial maturity. A large hotel may have security staff, backup systems and documented emergency procedures, whereas a small guesthouse may rely on the owner's personal experience. A risk-based framework is therefore useful only when it is proportionate: the same principles should apply to all firms, but the depth of documentation and the cost of controls should correspond to the scale and risk profile of the enterprise.

The official series also helps explain why security management should be incorporated into tourism policy at the enterprise level. Between 2020 and 2025, the number of recorded foreign tourism-purpose trips increased several times over. Such a change alters not only market demand but also the potential consequences of service failures. A disruption in a booking platform, a transport accident, a food-safety incident or a data breach can affect many more people when the market is larger and more interconnected. The managerial response should therefore focus on prevention, early detection and continuity rather than on emergency reaction alone.

Importantly, the indicator covers foreign citizens arriving for tourism purposes under the national statistical methodology; it should not be interpreted as a count of leisure holidaymakers only. In 2025, for example, official publications distinguished visits for relatives, travel, official, commercial, treatment and study purposes. For security management, this breadth is useful because tourism-sector entities interact with visitors whose mobility patterns and risk profiles differ.

The structure of border entry is also relevant to security planning. In 2024, 79.4 per cent of foreign visitors entered on foot, while 17.3 per cent entered by air, 2.1 per cent by motor road and 1.2 per cent by rail [4]. The predominance of land-border crossings implies that destination security cannot be designed only around airports and large hotels. It also requires safe road corridors, reliable transfer services, border-adjacent infrastructure, information support and coordination with smaller accommodation and catering businesses.

3.2. A multidimensional view of tourism-enterprise security

A tourism enterprise is secure not when it has eliminated every possible threat, which is unrealistic, but when it can recognise material risks, reduce preventable exposure, react proportionately and restore critical operations after disruption. This understanding moves the discussion away from isolated safety instructions toward organisational resilience.

In practice, the six dimensions are closely connected. A fire in a hotel is primarily a physical-safety event, but it can immediately become an occupational issue for employees, a financial problem if operations are interrupted, a reputational crisis if communication is

poor, and a digital problem if reservation or guest data cannot be accessed during evacuation. The same interdependence can be observed in cyber incidents: a compromised booking account may lead to fraudulent payments, customer complaints, legal exposure and loss of trust.

The human factor deserves particular attention. Tourism is a service-intensive industry in which employees continuously make small decisions that influence safety. Reception staff verify identities, guides decide whether a route remains suitable under changing weather conditions, drivers judge road conditions, restaurant personnel follow hygiene rules, and managers respond to complaints or suspicious transactions. Training therefore should not be limited to formal instruction once a year. It should include short scenario-based exercises that help employees recognise unusual situations and understand when to escalate them.

Another practical issue is the boundary between safety and service quality. In tourism these concepts often overlap. Clear signage, accurate information, clean premises, reliable transport, well-managed queues and respectful communication improve the visitor experience, but they also reduce risk. Conversely, chronic quality problems can be early warnings of deeper security weaknesses.

Table 2. Core risk groups for tourism-sector entities and practical controls

Risk group	Typical threats	Possible impact	Priority controls
Physical / infrastructure	Fire, unsafe building elements, theft, route hazards, transport incident	Injury, service interruption, liability	Inspection, maintenance, access control, evacuation plan, route checks
Occupational / personnel	Fatigue, injury, violence, insufficient emergency skills	Staff harm, errors, turnover, weak response	OSH procedures, workload control, first aid, drills, reporting
Health / sanitary	Food contamination, infection, inadequate hygiene	Guest illness, closure, reputation loss	HACCP-type controls, sanitation, first aid, health protocols
Digital / information	Phishing, ransomware, weak passwords, data leakage	Financial loss, privacy breach, downtime	MFA, backups, patching, staff awareness, response plan
Financial	Liquidity shortage, cancellations, currency volatility, fraud	Inability to refund or continue operations	Cash buffer, fraud controls, insurance, scenario planning
Partner / supply chain	Unreliable transport, guide or supplier;	Cascade failure across tourism product	Supplier screening, contracts, SLA,

Risk group	Typical threats	Possible impact	Priority controls
	weak contractor safety		backup suppliers
Reputational / communication	Slow response, misinformation, viral complaints	Loss of trust and demand	Crisis spokesperson, monitoring, factual communication, recovery plan

Supply-chain security is particularly important because the visitor experiences the trip as one continuous product even when several independent firms are involved. A tour operator may perform its own tasks correctly and still face a serious incident caused by a subcontracted driver, restaurant or accommodation provider. Basic partner due diligence should therefore include licensing where required, insurance, previous incident history, contact availability, data-handling practices and emergency-response capability. The objective is not to create excessive bureaucracy, but to ensure that critical partners meet a minimum level of reliability.

Physical and infrastructure security includes building condition, fire safety, access control, evacuation routes, electrical and engineering systems, transport condition, lighting and the safety of visitor routes. These issues are visible and often regulated, but their effectiveness depends on maintenance and staff practice rather than on the mere existence of equipment.

Occupational and personnel security covers injury prevention, ergonomics, psychosocial stress, workload, workplace violence, first-aid competence and the ability of staff to act during emergencies. In tourism, employees are part of the security system: reception staff may identify suspicious behaviour, guides may detect route hazards, drivers may prevent transport incidents and food-service workers directly control hygiene risks.

Information and cybersecurity have become central because tourism organisations routinely process names, passport details, payment information, travel dates, contact information and location-related data. A cyber incident can therefore create simultaneous financial, privacy and reputational damage; empirical evidence also shows that data breaches in hospitality differ from those in other industries, with higher proportions of external actors, hacking, malware and point-of-sale compromises [16]. Basic controls include role-based access, multi-factor authentication, secure backups, timely software updates, phishing awareness and an incident-response procedure.

Financial resilience determines whether a business can continue meeting obligations after cancellations, exchange-rate movements, seasonal shocks or sudden costs. Supply-chain security concerns the reliability of transport companies, guides, catering providers, booking intermediaries and other partners. Reputational security cuts across all categories because a poorly handled incident may spread quickly through online reviews and social media.

3.3. Tourism Entity Security and Resilience Model (TESRM)

The proposed Tourism Entity Security and Resilience Model (TESRM) is designed as a practical management cycle rather than a one-time audit. Its seven stages are: risk identification → risk assessment → prevention → preparedness → response → recovery → organisational learning. The sequence is circular because lessons from incidents and near misses should update the next round of identification and assessment.

The practical value of TESRM lies in turning security from a static document into a recurring management routine. Many enterprises prepare emergency instructions because regulation or certification requires them, but such documents can remain

disconnected from daily operations. TESRM instead starts with the actual processes of the enterprise: receiving a guest, confirming a booking, arranging a transfer, conducting an excursion, processing a payment or closing a facility at night. Risks are identified within these processes, assigned to responsible persons and reviewed when conditions change.

Risk assessment should also avoid false precision. Small tourism businesses rarely possess enough historical incident data to calculate exact probabilities. A simple five-point judgement scale can therefore be more useful than a complicated model, provided that the criteria are clearly described and applied consistently. Managers can distinguish, for example, between an event that is unlikely but catastrophic and one that is frequent but relatively minor. The aim is to support prioritisation, not to create the appearance of mathematical certainty.

Preparedness is strongest when it is rehearsed. A written evacuation plan has limited value if employees do not know where guests should assemble or who contacts emergency services. Similarly, a data-backup policy is ineffective if restoration has never been tested. Short simulations can reveal practical problems that are invisible on paper: missing telephone numbers, blocked exits, unclear authority, incompatible communication channels or uncertainty about vulnerable guests. The lessons from such exercises should be recorded and used to update procedures.

Recovery should begin before an incident occurs. Enterprises need to know which functions are critical and how long they can be interrupted without causing serious harm. For a hotel, these may include guest communication, room access, payment processing and safety systems. For a tour operator, critical functions may include traveller lists, transport contacts, itinerary changes and emergency communication. Identifying these dependencies in advance makes it easier to choose backup arrangements that are realistic and affordable. This logic corresponds to the business impact analysis and continuity planning approach set out in ISO 22301:2019 [17].

1. Risk identification. Each enterprise should maintain a concise risk register linked to real business processes. For every material risk, the register should indicate the source of risk, exposed people or assets, existing controls, responsible employee, early warning signs and the planned response. A small guesthouse may have a short register, while a large hotel or tour operator may require a more detailed one; the principle is proportionality.

2. Risk assessment. A simple semi-quantitative matrix can help SMEs prioritise action. For each risk, probability (P) and impact (I) are scored from 1 to 5. The basic score is $R = P \times I$. A score of 1–4 can be treated as low, 5–9 as moderate, 10–16 as high and 17–25 as critical. This does not replace professional engineering or cybersecurity assessment where required, but it creates a common language for managers.

3. Prevention and preparedness. Prevention seeks to reduce the probability or impact of an incident before it occurs. Preparedness recognises that some disruption will still occur and therefore focuses on response capacity. Tourism enterprises should combine technical controls with procedures, staff training, contact lists, backup communication, alternative suppliers, data backup and periodic drills.

4. Response and recovery. During an incident, clarity is more valuable than a long policy document. Staff should know who makes decisions, who contacts emergency services, who communicates with tourists, how vulnerable guests are assisted and how essential records are protected. Recovery begins when immediate danger has been controlled and continues until critical services, customer communication and operational capacity are restored.

5. Organisational learning. After an incident or near miss, the enterprise should conduct a short structured review: what happened, why existing controls failed or succeeded, what the consequences were, what should change, who is responsible for the change and by what date. This converts individual experience into organisational memory and prevents the same weakness from recurring.

3.4. Tourism Entity Security Index (TESI)

To make the framework measurable, the study proposes a Tourism Entity Security Index (TESI). The index is intended as a management and research instrument, not as an

official certification score. It combines six dimensions that together represent enterprise security maturity.

TESI is deliberately designed as a diagnostic instrument rather than a certification score. Its purpose is to help an enterprise see where weaknesses are concentrated. Two businesses with the same total score may have very different risk profiles: one may be physically secure but digitally weak, while another may have good cybersecurity yet poor crisis preparedness. For management, the profile of dimension scores is therefore more informative than the overall number alone.

The suggested weights are preliminary. They reflect the idea that physical safety and emergency capability deserve substantial attention because failures in these areas may directly threaten life and continuity. Nevertheless, sector-specific adjustment is necessary. A digital travel agency may assign greater weight to information security, while an adventure-tour operator may emphasise route, equipment and emergency risks. Future empirical research should test whether the weights predict actual incident exposure, recovery time, insurance claims or customer trust.

To reduce subjectivity, each dimension can be assessed through observable indicators. Instead of asking whether an enterprise has 'good cybersecurity', an audit can check whether multifactor authentication is used, backups are performed and tested, staff access is removed when employment ends, and suspicious messages are reported. In physical safety, indicators can include inspection records, emergency lighting, evacuation signage and documented maintenance. This approach makes the index more transparent and easier to compare over time.

Each dimension is scored on a 0–100 scale through a checklist or audit. The weighted total is calculated as $TESI = \sum(W_i \times S_i)$, where W_i is the weight of dimension i and S_i is the score achieved by the enterprise in that dimension. The suggested weights reflect the direct importance of physical safety and emergency capacity while maintaining meaningful weight for digital, financial and supply-chain resilience. These weights require empirical validation before normative use.

For interpretation, a preliminary scale may classify 0–39 points as critical vulnerability, 40–59 as vulnerable, 60–79 as satisfactory, 80–89 as high security maturity and 90–100 as resilient. The practical value of the index is not the label itself, but the ability to see which dimension is pulling the enterprise downward. For example, a hotel can have strong fire systems but still be fragile because of weak backup procedures or poor protection of guest data.

3.5. Application to tourism-sector entities in Uzbekistan

The legal and institutional context of Uzbekistan already places safety responsibilities on tourism participants. The Law of the Republic of Uzbekistan No. O'RQ-549 "On Tourism" remains a key sectoral act and has subsequently been amended. Its safety provisions establish responsibilities connected with protecting tourists and providing assistance in emergency situations [18]. The proposed TESRM does not replace legal compliance; it extends the management perspective from minimum compliance toward continuous enterprise resilience.

For Uzbekistan, implementation should recognise the structure of the national tourism market. International brands, local hotels, guesthouses, tour operators, guides and transport firms operate under very different conditions. A uniform security requirement can therefore become either too weak for high-risk organisations or too burdensome for microbusinesses. A tiered approach would be more practical: a common minimum set of controls for every tourism entity, followed by additional requirements according to size, service type, visitor volume and exposure to specific hazards.

Regional context also matters. The operational risks of a city hotel in Tashkent are not identical to those of a pilgrimage operator in Samarkand, a desert tour in Bukhara or Khorezm, or mountain tourism in areas exposed to weather and terrain hazards. Local risk registers should therefore complement national standards. Destination authorities can support enterprises by sharing verified information on seasonal hazards, transport disruptions, emergency contacts and recurring incidents, reducing the cost of risk intelligence for small firms.

Digitalisation creates a further policy opportunity. If tourism enterprises increasingly use national and private digital platforms, the same environment can support structured incident reporting and self-assessment. A simple digital module could allow firms to complete periodic risk checks, record incidents, receive targeted guidance and compare their progress over time. Aggregated and anonymised data could help authorities identify recurring vulnerabilities without turning the system into a punitive reporting mechanism.

A supportive approach is especially important for SMEs. Security improves when firms understand the practical benefit of controls, not when they merely collect documents for inspection. Training materials should therefore use real tourism scenarios, explain the cost of common failures and provide ready-to-use templates for risk registers, emergency contacts and partner checks. This would make risk management accessible to enterprises that do not employ specialised safety or compliance staff.

The rapid increase in visitor flows strengthens the case for differentiated implementation. A large international hotel requires formal cybersecurity, engineering and crisis-management functions. A family guesthouse requires a simpler version: safe electrical and gas systems, clear evacuation information, emergency contacts, secure handling of passport and payment data, basic first-aid readiness and a backup plan for essential services. A tour operator needs destination and route risk assessment, transport-provider verification, traveller information, communication redundancy and procedures for lost persons, health incidents or itinerary disruption.

Particular attention should be given to service-chain responsibility. The tourist does not experience organisational boundaries in the same way managers do. If a hotel books an unsafe transfer, a tour operator uses an unverified driver or a restaurant partner breaches hygiene rules, the visitor often attributes the failure to the whole destination or package. Security assessment should therefore extend to critical partners and not stop at the legal boundary of the firm.

Digitalisation also changes the risk profile. Online booking, QR payments, messaging platforms and integrated databases improve convenience, but they concentrate personal and transactional information. For smaller enterprises, the first practical steps are not expensive technologies: unique passwords, multi-factor authentication where available, controlled staff access, regular backup and the ability to recognise phishing attempts can substantially improve basic cyber hygiene.

4. Discussion

The statistical expansion of tourism in Uzbekistan makes enterprise-level resilience an increasingly practical issue. The increase from 7.96 million foreign tourism-purpose visits in 2024 to about 11.68 million in 2025 does not itself prove that risk has increased or decreased. What it does show is that the tourism system is handling a larger volume of people, transactions and service interactions. In such a setting, the absolute consequences of weak organisational controls can become more significant even if the probability of any individual incident remains unchanged.

The main theoretical implication of the study is that tourism security should be located between service management and organisational resilience. It is not a parallel function that becomes relevant only during crises. A resilient organisation designs ordinary processes in a way that reduces the chance that routine errors develop into emergencies. This interpretation brings tourism security closer to modern risk management and also explains why leadership, training and organisational learning are central components.

There is also an economic argument. Preventive controls require resources, but unmanaged incidents generate direct and indirect costs: refunds, medical assistance, downtime, legal disputes, reputational damage, staff turnover and loss of future demand. Security investment should therefore be evaluated through avoided disruption and continuity, not only through immediate expenditure. For SMEs, low-cost controls such as clear responsibilities, reliable backups, supplier verification and scenario training may produce substantial resilience benefits without requiring sophisticated technology.

The relationship between enterprise security and destination competitiveness is cumulative. A destination's reputation is produced by thousands of individual service encounters. Public authorities can maintain order and infrastructure, but repeated failures by private firms can still undermine visitor confidence. Conversely, well-managed enterprises support the destination by detecting problems early, communicating responsibly and recovering quickly when disruption occurs. This is why enterprise-level resilience deserves a clearer place in destination-management policy.

At the same time, the framework should not be interpreted as an attempt to eliminate all uncertainty. Tourism depends on movement, weather, human behaviour and external systems; some risk is unavoidable. The objective is reasonable preparedness and proportionate control. Excessive security can reduce hospitality, increase costs and create unnecessary friction for travellers. The management challenge is therefore to protect people and continuity while preserving the openness and convenience that make tourism attractive.

The proposed approach also helps distinguish destination safety from enterprise security. A destination may have low crime and good public infrastructure, yet an individual operator can still be vulnerable because of unsafe transport, weak employee training, poor food handling or cyber exposure. Conversely, a resilient enterprise can reduce the effects of external disruption by preparing alternative routes, communication channels, suppliers and recovery procedures.

The TESRM is intentionally cyclical. This is consistent with the broader risk-management principle that risks evolve as technology, markets, climate conditions and traveller behaviour change. A static checklist completed once a year cannot capture this dynamic. The model therefore gives organisational learning the same conceptual importance as prevention and response.

The TESI offers a basis for future empirical research. It could be tested on hotels, tour operators, guesthouses and tourism transport providers in Samarkand, Tashkent, Bukhara or other destinations. Reliability analysis and expert methods could be used to refine indicators and weights. Cluster analysis could then identify profiles of enterprises—for example, physically secure but digitally vulnerable firms, or operationally capable firms with weak partner controls. Such evidence would allow public policy and industry associations to provide targeted support rather than uniform recommendations.

4.1. Scientific Novelty

The first element of novelty is a shift in the unit of analysis. Instead of treating tourism security only as a relationship between the tourist and the destination, the article introduces the tourism enterprise as an independent level connecting the two. This makes it possible to analyse how organisational weaknesses inside hotels, tour operators, transport providers and other service firms can influence the broader safety image of a destination.

Second, the study operationalises enterprise security as a multidimensional condition that combines physical and infrastructure safety, occupational and personnel security, information and cybersecurity, financial resilience, partner and supply-chain reliability, and emergency-management capacity. Bringing these dimensions together reduces the fragmentation that is common when each risk is managed by a separate function.

Third, the Tourism Entity Security and Resilience Model (TESRM) is proposed as a continuous seven-stage cycle linking risk identification, assessment, prevention, preparedness, response, recovery and organisational learning. The model is intended to support repeated managerial practice rather than one-off compliance checks.

Fourth, the Tourism Entity Security Index (TESI) is introduced as a possible diagnostic instrument for measuring security maturity and comparing progress over time. Its current structure is conceptual and requires empirical validation, but it creates a basis for future quantitative research and sector-specific benchmarking.

Finally, the framework links enterprise resilience with destination competitiveness through a cumulative logic: resilient enterprises are more likely to deliver reliable services; reliable services support visitor confidence; and repeated positive experiences

strengthen destination reputation. This connection gives enterprise security a strategic, not merely technical, role in tourism development.

5. Conclusion

Tourism security is increasingly an organisational capability: protecting tourists cannot be separated from protecting employees, information, assets, cash flow and the continuity of the enterprise itself. The rapid growth of tourism flows, both globally and in Uzbekistan, raises the strategic value of preventive and proportionate management that makes the most serious risks visible, assigns responsibility and improves readiness without overburdening small enterprises. The proposed TESRM and TESI offer such a structure by placing enterprise security between tourist safety and destination resilience. As the framework is conceptual, its weights and thresholds remain working hypotheses; the next research stage should therefore involve expert validation and empirical testing on hotels, tour operators, guesthouses and transport providers in different regions of Uzbekistan. Ultimately, a safe destination is built not only through public order and infrastructure, but also through the day-to-day decisions of tourism enterprises that identify risks early, prepare staff, protect information, verify partners and recover quickly from disruption.

REFERENCES

- [1] UN Tourism, "International tourism recovers pre-pandemic levels in 2024," *UN Tourism News*, Jan. 21, 2025. [Online]. Available: <https://www.untourism.int/News/International-Tourism-Recovers-Pre-Pandemic-Levels-in-2024>
- [2] UN Tourism, "International tourist arrivals grew 5% in Q1 2025," *UN Tourism News*, May 27, 2025. [Online]. Available: <https://www.untourism.int/news/international-tourist-arrivals-grew-5-in-q1-2025>
- [3] International Labour Organization, "Tourism, hotel and food & beverage services," ILO, Geneva, Switzerland. [Online]. Available: <https://www.ilo.org/topics-and-sectors/industries-and-sectors/tourism-hotel-and-food-beverage-services>
- [4] National Statistics Committee of the Republic of Uzbekistan, "Socio-economic situation of the Republic of Uzbekistan: Tourist flows, January–December 2024," Tashkent, Uzbekistan, 2025. [Online]. Available: <https://stat.uz/files/483/choraklik-natijalar-yanvar-dekabr2024eng/3854/18TOURIST-FLOWS.pdf>
- [5] National Statistics Committee of the Republic of Uzbekistan, "Tourist flows in the Republic of Uzbekistan, January–December 2025," Tashkent, Uzbekistan, 2026. [Online]. Available: <https://stat.uz/>
- [6] Y. Mansfeld and A. Pizam, Eds., *Tourism, Security and Safety: From Theory to Practice*. Burlington, MA, USA: Elsevier Butterworth-Heinemann, 2006.
- [7] B. W. Ritchie, "Chaos, crises and disasters: A strategic approach to crisis management in the tourism industry," *Tourism Management*, vol. 25, no. 6, pp. 669–683, 2004, doi: [10.1016/j.tourman.2003.09.004](https://doi.org/10.1016/j.tourman.2003.09.004).
- [8] C. Xie, M. Wang, J. Zhang, S. S. Huang, and J. Yu, "The tourist metasafety framework (TMF): Toward a holistic understanding of tourist safety," *Tourism Management*, vol. 107, Apr. 2025, Art. no. 105071, doi: [10.1016/j.tourman.2024.105071](https://doi.org/10.1016/j.tourman.2024.105071).
- [9] G. Glowka, R. Eller, M. Peters, and A. Zehrer, "Risk perception in small- and medium-sized hospitality family enterprises," *Tourism Review*, vol. 80, no. 7, pp. 1335–1351, 2025, doi: [10.1108/TR-06-2023-0421](https://doi.org/10.1108/TR-06-2023-0421).
- [10] C. Orchiston, G. Prayag, and C. Brown, "Organizational resilience in the tourism sector," *Annals of Tourism Research*, vol. 56, pp. 145–148, 2016, doi: [10.1016/j.annals.2015.11.002](https://doi.org/10.1016/j.annals.2015.11.002).
- [11] N. A. Brown, J. E. Rovins, S. Feldmann-Jensen, C. Orchiston, and D. Johnston, "Exploring disaster resilience within the hotel sector: A systematic review of literature," *International Journal of Disaster Risk Reduction*, vol. 22, pp. 362–370, Jun. 2017, doi: [10.1016/j.ijdrr.2017.02.005](https://doi.org/10.1016/j.ijdrr.2017.02.005).
- [12] K. Ciarlante, C. Mejia, and E. Broker, "A research agenda for occupational safety, health, & well-being in hospitality & tourism management," *International Journal of Hospitality Management*, vol. 123, Oct. 2024, Art. no. 103887, doi: [10.1016/j.ijhm.2024.103887](https://doi.org/10.1016/j.ijhm.2024.103887).

-
- [13] International Labour Organization, "Occupational safety and health in the hotels, catering and tourism sector," ILO, Geneva, Switzerland, Aug. 8, 2013. [Online]. Available: <https://www.ilo.org/resource/occupational-safety-and-health-hotels-catering-and-tourism-sector>
 - [14] *Risk Management — Guidelines*, ISO 31000:2018, International Organization for Standardization, Geneva, Switzerland, 2018. [Online]. Available: <https://www.iso.org/standard/65694.html>
 - [15] *Travel Risk Management — Guidance for Organizations*, ISO 31030:2021, International Organization for Standardization, Geneva, Switzerland, 2021. [Online]. Available: <https://www.iso.org/standard/54204.html>
 - [16] K. Gwebu and C. W. Barrows, "Data breaches in hospitality: Is the industry different?" *Journal of Hospitality and Tourism Technology*, vol. 11, no. 3, pp. 511–527, 2020, doi: [10.1108/JHTT-11-2019-0138](https://doi.org/10.1108/JHTT-11-2019-0138).
 - [17] *Security and Resilience — Business Continuity Management Systems — Requirements*, ISO 22301:2019, International Organization for Standardization, Geneva, Switzerland, 2019. [Online]. Available: <https://www.iso.org/standard/75106.html>
 - [18] Law of the Republic of Uzbekistan No. O'RQ-549 "On Tourism," Jul. 18, 2019 (with subsequent amendments). National Database of Legislation of the Republic of Uzbekistan. [Online]. Available: <https://lex.uz/docs/4428101>