Document

Classification:	TLP;CLEAR. Unrestricted.
Version:	5.0 (revised, April 2026)
Coverage:	Fez, Marrakech, Casablanca
Author:	Roberto Pinna
Client:	Redwalls Hospitality Group

Handling caveat

Client, properties, and quantitative indicators are illustrative. The methodology, analytic standards, and reasoning reflect how a real pre-investment engagement of this type would be conducted. No active collection, exploitation, or asset-level validation was performed.

Hospitality pre-investment digital Infrastructure and Operational Risk

Pre-investment assessment of digital operating environment, inherited cyber exposure, and compliance risk for a three-city hospitality portfolio in the Kingdom of Morocco.

Illustrative assessment

direct@robpinna.com
www.robpinna.com

Italy
Cagliari

Morocco
Fez / Marrakech

+39
3426988107

1. Executive Summary

Redwalls Hospitality Group is evaluating three hospitality assets in Morocco: a riad in the Fez medina, a riad-hotel in the Marrakech medina, and a boutique hotel in Casablanca's Gauthier district. This assessment reviews the digital operating environment around those assets and the main cyber, fraud, and compliance risks likely to affect the portfolio after acquisition.

Each candidate asset sits inside a local digital environment where consumer-grade networking equipment, weak wireless security settings, exposed surveillance infrastructure, and informal infrastructure-sharing practices are common enough to create a materially elevated baseline risk. The evidence is strongest at city and district level. It is weaker at property level because no full on-site network inspection was conducted inside the target buildings.

Three risks matter most at transaction stage.

First, inherited technical exposure. The Moroccan hospitality environment is one in which surveillance exposure, weak local wireless controls, and convenience-led network administration are common enough to make inherited weakness a live due-diligence concern. This does not prove compromise at the three candidate assets. It does show an environment in which the cost of access, misuse, or persistence is relatively low for actors with modest capability until property-level review closes that uncertainty.

Second, brand abuse and booking fraud during transition. Newly branded hospitality properties are exposed to duplicate-listing fraud, cloned identity use, and deposit-collection scams, especially during the early operating phase when brand recognition is still limited and platform trust has not stabilised.

Third, compliance burden. A European acquirer inheriting small-scale Moroccan hospitality operations should expect a gap between local practice and the data-handling standard expected by European owners, partners, insurers, or payment providers. In practical terms, that gap usually concerns guest identity handling, camera retention, unmanaged staff communications, and flat or weakly governed local networks.

The Fez and Marrakech assets present the stronger combined exposure picture in this comparison. They represent the type of environment in which weak wireless controls, older hardware, and informally extended infrastructure are more likely to coexist. Casablanca presents a better baseline in this comparison, but not a clean one. The external commercial appearance of a building there should not be mistaken for a validated internal security posture.

The portfolio remains investable, but digital infrastructure should sit inside the diligence process itself rather than being treated as an IT clean-up item left for after closing. The single highest-value action available before commitment is a property-level technical review at each site focused on network topology, surveillance access, credential hygiene, router configuration, staff communication channels, and data-handling practice.

Key Judgements

Judgement	Confidence
The three candidate assets operate in districts where weak wireless controls and consumer-grade network infrastructure are common.	High
The surrounding environment makes inherited technical exposure plausible at each asset, but compromise at the three properties is unverified.	Medium
Fez and Marrakech carry greater structural exposure than Casablanca because of denser medina architecture, more informal infrastructure practices, and weaker observed wireless baselines.	High
Booking fraud and brand impersonation are the most likely early post-acquisition external threat scenarios.	Medium
A European owner should expect compliance remediation to extend beyond policy paperwork and into network, process, and staff-channel changes.	High

Confidence labels follow a three-tier scheme. **High**: well-established environmental patterns; low inferential dependency. **Medium**: structural plausibility supported by partial evidence; additional collection would increase certainty. **Low**: derived from comparable-environment reasoning; speculative pending direct validation.

2. Scope, Method, and Analytic Standard

Scope

This assessment covers three issues relevant to acquisition diligence:

1. The surrounding digital infrastructure environment in Fez, Marrakech, and Casablanca.

2. Threat scenarios likely to affect newly acquired hospitality assets in those environments.

3. The likely first-order remediation burden facing an acquirer.

Each city assessment includes a short in-person visit focused on the target property, the surrounding streets, nearby hospitality density, visible infrastructure patterns, a brief check of the device estate and high-level network arrangement where observable, and a limited survey window rather than a prolonged field deployment.

Out of Scope

This assessment does not include penetration testing, authenticated scanning, legal opinion, forensic review, interviews with operators or vendors, financial due diligence, or full physical security assessment.

Collection Model

Public-source enumeration. Passive enumeration of internet-facing assets via Shodan and Censys, focused on RTSP streams (port 554), camera and NVR administration interfaces (ports 80, 443, 8080, 8443), and related web management services. Results deduplicated by IP and port composite key. ISP-level ASN filtering applied to bound results to the target city area.

Wi-Fi proximity survey. Passive WiGLE-methodology wardriving across the district immediately surrounding each target property. Collection limited to beacon frames observable in public space: no authentication, association, packet injection, credential capture, or service interaction. BSSIDs deduplicated across multiple passes; vendor attribution derived from IEEE hardware identifier prefix analysis on anonymised hardware identifiers.

Regulatory review. Review of publicly available Moroccan data-protection and cybersecurity materials, including CNDP publications, Loi 09-08, Loi 05-20, and related secondary legal commentary, with attention to requirements relevant to a European acquirer inheriting Moroccan hospitality operations.

Field component. Short, time-bounded in-person visits by the analyst to each city to walk the areas around the target properties, assess the immediate operating environment, and conduct limited survey work. Where brief site access is granted, the field component also includes a property-focused check of visible devices and the apparent network arrangement as far as it can be understood during a limited visit, without prolonged deployment, authenticated access, or full technical validation.

Analytic Standard

Estimative language follows conventions consistent with Intelligence Community Directive 203 (ICD-203). Probability terms map to approximate ranges as follows.

Term	Approximate probability range
Highly likely	80 to 95%
Likely	55 to 80%
Unlikely	20 to 45%
Remote	Less than 5%

Terms in the intermediate range (Roughly even, 45 to 55%) are not used in this report and are omitted from the table for brevity.

Statements in this report are classified as **assessed** (judgement grounded in evidence and analytic reasoning), **inferred** (drawn from environmental patterns, not validated inside target properties), or **unverified** (would require site access or operator-side records to confirm). This document assesses exposure feasibility, not confirmed compromise.

Source Reliability and Limits

Source	Reliability	Principal limitation
Public-source enumeration	High	Surfaces external exposure; does not validate internal property topology
Wi-Fi proximity survey	High	Indicators reflect plausible district-level conditions, not asset-level validation
CNDP and official publications	High	Public enforcement record is incomplete by definition
Field visit and environmental observation	Moderate	Limited to observable surface; no authenticated access or prolonged deployment

Information Gaps

The assessment does not attempt to confirm the internal topology of any target property. It does not establish whether surveillance, guest Wi-Fi, payment systems, and management devices share a flat network inside those buildings. It does not confirm active compromise, default credentials in use, or the current state of firmware on the properties themselves. Those points would require site access.

3. Operating Environment

3.1 Hospitality Context

Morocco's hospitality sector continues to expand, driven by strong tourism growth, continued European demand, and sustained investment attention in Fez, Marrakech, and Casablanca. For an acquirer, that growth brings two parallel effects. More demand supports revenue. More digital dependency raises the cost of weak local practices that might previously have passed without consequence.

At the small-property end of the market, hospitality operations are rarely built around a security-first design. Devices and processes usually accumulate over time through router replacements, cameras added in stages, staff coordination moving into WhatsApp, and booking or payment workflows shaped more by local convenience than by a controlled model.

3.2 Infrastructure Pattern

Across the three cities under review, consumer and prosumer networking equipment remains common in the small-business layer. In Fez and Marrakech especially, the medina environment creates conditions in which technical infrastructure often grows around the building rather than from a planned building-wide design. Cable runs, rooftop visibility, shared walls, inherited lines, mixed residential-commercial use,

and ad hoc router placement all matter here. None of that proves weakness inside a specific riad, but it does mean the buyer should start from a more cautious baseline than the building exterior or the listing presentation might suggest.

The Casablanca district reviewed for this assessment showed a more modern baseline, greater vendor diversity, stronger adoption of current Wi-Fi standards, and lower prevalence of legacy convenience settings. Even there, the observed pattern still points to uneven control quality in the small and mid-market hospitality layer.

3.3 Regulatory Context

Morocco's data-protection framework is centred on Law 09-08 and CNDP oversight. In formal terms, the framework is developed enough to matter. In practical terms, smaller operators often lag behind what a European owner would regard as acceptable data governance. The immediate acquisition question is not whether Moroccan law exists. It is whether inherited operating practice, once reviewed by a European group, insurer, platform partner, or payment stakeholder, will prove operationally acceptable without remediation.

In hospitality terms, the most relevant issues are guest identity documents, cross-border transfer of guest data, video surveillance practice, retention discipline, and the use of unmanaged staff channels for operational information.

4. Threat Landscape Relevant to Acquisition

4.1 External Threat Actors

Actor type	Primary aim	Likely route into this environment	Relevance
Fraud operators	Monetise brand confusion and booking identity	Cloned listings, copied imagery, off-platform payment requests, spoofed communications	High
Opportunistic local attackers	Gain network access or harvest locally exposed data	Weak Wi-Fi controls, default router settings, exposed surveillance access, proximity advantage	High
Access brokers and low-end intrusion operators	Obtain footholds for resale or reuse	Exposed internet-facing services, reused credentials, unmanaged remote access	Medium

Actor type	Primary aim	Likely route into this environment	Relevance
Targeted collectors	Persistent low-noise collection on people and routines	Camera access, environmental visibility, weak segmentation, known guest patterns	Low to medium; higher for properties serving high-profile clientele

4.2 Threat Scenarios That Matter Most

Brand impersonation and duplicate-listing fraud. This is the most straightforward post-acquisition scenario because it does not require deep technical access. Public imagery, address information, and property descriptions are available by design, and the attacker mainly needs timing, copied presentation, and a way to move payment off platform. The opportunity is simple, but the business effect can spread quickly through refund disputes, support load, review damage, and weakened platform trust.

Inherited technical debt with security consequences. Ownership change does not reset routers, cameras, admin credentials, staff habits, or ad hoc remote access. If weak settings or unmanaged external exposure exist before acquisition, they usually persist into the first operating phase unless explicitly audited out.

Insider-enabled data leakage. At smaller properties, guest names, arrival details, and service coordination often circulate through informal staff channels, so the more likely problem is weak offboarding, shared devices, screenshots, and access that survives role change rather than anything technically sophisticated.

Compliance exposure triggered by external review. Problems of this type are often discovered only when a parent group standard, insurer questionnaire, payment requirement, or customer complaint forces the issue. The operational burden then lands at once rather than in sequence.

5. Property-Level Findings

The following sections combine district-level wireless indicators, structured public-source enumeration, and a short field visit around each asset, including a brief review of visible devices and the apparent network arrangement where that would be observable during a limited property visit. The sections should be read as environmental risk analysis around a target property rather than as a substitute for a site audit.

5.1 Fez, Traditional Riad, Medina

The Fez asset sits in a dense medina corridor where residential, commercial, and hospitality use overlap closely. In this setting, physical adjacency matters. Shared walls, rooftop continuity, legacy cabling paths, and piecemeal infrastructure upgrades make clean separation between one property's digital boundary and the next less likely.

District baseline. Fez presents the weakest wireless environment in this comparison, reflecting the kind of dense medina conditions in which legacy hardware, weak controls, and convenience-led infrastructure are most likely to accumulate. The district dataset reflects roughly 3,200 unique access points.

Indicator	Approx. count	Approx. share
WPS enabled	~2,200	~70%
Mixed WPA/WPA2 security mode	~830	~26%
Open / unencrypted	~70	~2%
2.4 GHz only	~2,300	~72%
Wi-Fi 6E / 6 GHz	0	0%
Arcadyan / Maroc Telecom	~1,080	~34%

Assessment. Fez presents the weakest local wireless baseline of the three environments reviewed here. High WPS prevalence, heavy dependence on legacy hardware profiles, and medina-specific building conditions increase the likelihood that a small hospitality operator is running a fragile setup. That does not establish that the target riad uses a flat network or exposed surveillance access, but it does justify treating both as live possibilities that require validation before acquisition.

Implication for the asset. In Fez, the digital diligence question is not simply whether the router is old. It is whether the property's network and camera setup have been shaped over time by convenience, neighbour relationships, inherited installer decisions, and unmanaged staff practice.

5.2 Marrakech, Riad-Hotel, Mouassine Quarter

The Marrakech asset sits in a mature hospitality zone with heavier exposure to international tourism and a somewhat stronger likelihood of partial upgrades driven by renovation cycles. That produces a mixed picture: more signs of improvement than Fez, without evidence of a consistently controlled baseline.

District baseline. The Marrakech district presents a mixed hospitality environment with partial renovation effects but persistent reliance on unevenly administered consumer and prosumer infrastructure. The district dataset reflects roughly 2,900 unique access points.

Indicator	Approx. count	Approx. share
WPS enabled	~1,800	~64%
Mixed WPA/WPA2 security mode	~690	~24%

Indicator	Approx. count	Approx. share
Open / unencrypted	~50	~2%
2.4 GHz only	~1,950	~68%
5 GHz dual-band	~290	~10%
Wi-Fi 6E / 6 GHz	0	0%
Arcadyan / Maroc Telecom	~830	~29%
TP-Link / aftermarket	~370	~13%

Assessment. Marrakech appears marginally stronger than Fez, mainly because the surrounding district shows limited signs of more recent hardware refresh and a broader vendor mix. That is still not a robust baseline. Weak wireless controls remain common, and the medina's built environment still favours incremental, convenience-led infrastructure over disciplined separation of systems.

Implication for the asset. In Marrakech, the more likely acquisition risk is false reassurance. A property that looks polished, renovated, and commercially mature may still be running on an improvised technical base.

5.3 Casablanca, Boutique Hotel, Gauthier District

The Casablanca asset differs from the two medina properties in architecture, clientele, and surrounding infrastructure profile. The district is commercial, more vertically built, and more likely to include newer networking equipment.

District baseline. The Casablanca district presents the strongest of the three baselines, with greater hardware diversity, more dual-band deployment, and lower prevalence of legacy convenience settings. The district dataset reflects roughly 1,500 unique access points.

Indicator	Approx. count	Approx. share
WPS enabled	~670	~45%
WPA2 only	~810	~55%
Open / unencrypted	~40	~3%
2.4 GHz only	~725	~49%
5 GHz dual-band	~590	~40%

Indicator	Approx. count	Approx. share
Wi-Fi 6E / 6 GHz	~20	~1%
Arcadyan / Maroc Telecom	~310	~21%
Diverse vendors	~550	~37%

Assessment. Casablanca shows the best technical baseline in this comparison. Even so, the data supports only a relative judgement, not a clean bill of health. Better district-level indicators still do not answer the questions that matter for acquisition: how the building is segmented, how cameras are administered, whether remote access is controlled, how staff devices are handled, and what operational data moves across informal channels.

Implication for the asset. Casablanca is the least concerning of the three properties on present evidence, but the probable business sensitivity of the clientele there raises the cost of being wrong.

6. Judgements, Decision Points, and Risk Scenarios

Confidence here reflects the amount of environmental support behind each judgement. It should not be mistaken for property-level validation.

6.1 Cross-Portfolio Judgements

Judgement	Confidence
Fez carries the highest structural exposure in this portfolio.	High
Marrakech follows closely and shows only limited signs of stronger infrastructure maturity.	High
Casablanca offers a materially better baseline, but still requires direct technical validation.	High
The strongest transaction-stage concern is inherited weakness, not proven hostile presence.	High
The strongest early operating-phase concern is external fraud against the new brand.	Medium
The most likely source of internal leakage is routine operational informality rather than sophisticated intrusion.	Low

The priority order used here is simple. Risks rise to the top when they combine accessible attack paths, early operational impact after acquisition, and a tendency to remain invisible until they become expensive to unwind.

6.2 Risk Scenarios

Scenario A, inherited exposure discovered late. The acquirer completes the transaction, rebrands the properties, and only then learns that one or more sites rely on default or reused router and camera credentials, ad hoc remote access, or a flat network that mixes guest, staff, and surveillance traffic. The access path is not sophisticated. The damage comes from inheriting weak architecture and having to remediate it during live operations, under time pressure and with immediate cost.

Scenario B, duplicate listing and deposit fraud. A hostile actor copies photography and listing details from a newly branded property, recreates the identity on a second platform or lookalike site, and directs guests toward off-platform payment. The barrier to entry is low because the brand assets are public and the transition period creates uncertainty. The effect lands first on trust, then on operations through complaint handling, refund pressure, platform friction, and review damage.

Scenario C, staff-channel leakage. Guest names, arrival times, room assignments, and identity documents circulate through informal messaging channels used for operational convenience. The exposure here comes from routine handling rather than advanced intrusion. A former staff member, shared handset, or screenshot chain later becomes the source of targeted social engineering, guest complaint, or reputational friction.

Scenario D, compliance issue triggered by group integration. The acquirer tries to connect the new properties into parent systems, central reporting, or cross-border guest-data workflows and discovers that current practice is not properly documented, segmented, or governed. The weakness may have been tolerated locally, but integration makes it visible. The result is delay, procurement pressure, urgent process redesign, and avoidable management attention at the worst moment.

6.3 Transaction Decision Points

The following questions define the collection priorities that close diligence uncertainty before commitment. Each would be answered through a property-level technical review. If those answers are unavailable at signing, the digital operating environment of the asset has not been assessed.

1. What devices and systems appear to be present at the property, and which of them are confirmed to sit on the local network?
2. Are guest Wi-Fi, surveillance, administration, and payment functions separated at a high level?
3. Who holds administrative credentials for routers, cameras, recorders, and booking systems?
4. What staff channels are used for guest operations, and how are departures handled?
5. Where do passport scans, camera footage, and booking records reside, and under what retention practice?

7. Recommendations

Priority should go first to review steps that identify cheap access paths, inherited external dependencies, and gaps between formal control boundaries and the way technology is actually administered in practice.

7.1 Pre-Acquisition

Conduct a short-form technical review at each target property before commitment. The review should establish network topology, device inventory, remote access pathways, credential ownership, surveillance configuration, and operational data flow, with specific attention to informal infrastructure extensions, apparent control boundaries, third-party installer dependency, inherited remote access, and equipment added incrementally without central oversight.

Add digital infrastructure explicitly to the diligence checklist alongside legal, financial, and building-condition review. For this portfolio, the digital question is already material enough to justify that status.

Review how surveillance, networking, and access-control equipment were procured, installed, and maintained, including any retained vendor or installer access, undocumented maintenance arrangements, and passwords or updates still tied to external technicians.

Build an immediate external brand-protection plan before public relaunch, covering duplicate-listing checks, image reuse monitoring, lookalike domain review, and a clear process for guest verification when payment disputes arise.

7.2 First 90 Days After Acquisition

Replace or reconfigure routers and access points that cannot support a controlled baseline. Rotate administrative credentials across all network, surveillance, booking, and payment-adjacent systems. Review all remote access settings and remove any exposure that cannot be justified, especially where administration appears to depend on legacy installer arrangements, convenience-led exceptions, or undocumented third-party support.

Map how guest operations are actually coordinated in practice, including shared phones, informal messaging groups, screenshots, and role overlap, then remove guest-sensitive activity from unmanaged channels and align offboarding with those real workflows rather than with nominal job titles alone.

Review guest identity handling, camera retention practice, and cross-border data movement against the owner's legal and operational standard rather than against local custom alone.

7.3 Medium-Term Remediation

Implement proper separation between guest access, management traffic, surveillance systems, and payment-related functions. Replace legacy devices that cannot be administered safely. Introduce documented ownership for administrative credentials, updates, retention settings, and vendor access. Repeat a small-scope validation survey after remediation to confirm the new baseline.

8. Risk Matrix

Exposure	Likely effect on operations	Priority
Weak local wireless controls in surrounding districts	Increases plausibility of unauthorised local access attempts and weakens confidence in inherited setups	High
Unverified surveillance administration and remote access	Risk of inherited exposure, privacy issues, and delayed remediation burden	High
Informal staff communication channels	Leakage of guest and operational data, weak offboarding, screenshot circulation	High
Publicly available brand assets and booking identity	Duplicate listings, payment diversion, guest confusion, review damage	High
Unclear data-handling and retention practice	Compliance friction, insurer or partner scrutiny, integration delays	High
Consumer-grade device estate with mixed vendor quality	Patch inconsistency, weak administration, fragmented support responsibility	Medium

9. Appendix A. Evidence Notes

Wireless indicators. Produced via passive WiGLE-methodology wardriving in the district immediately surrounding each target property. BSSIDs deduplicated across multiple passes; the reported count reflects unique hardware identifiers after deduplication. Vendor attribution derives from IEEE hardware identifier prefix analysis on anonymised hardware identifiers; no device-level geolocation is retained. WPS-enabled status is observable passively from beacon frames; actual exploitability depends on router model and firmware configuration. Dual-band capability is inferred from 5 GHz BSSID presence; devices emitting on both bands are counted as two BSSIDs but one physical access point. The absence of Wi-Fi 6E is confirmed by the absence of 6 GHz band BSSIDs in the survey.

Surveillance exposure indicators. Produced via Shodan and Censys enumeration of RTSP-exposed endpoints (port 554) and HTTP/HTTPS administration interfaces (ports 80, 443, 8080, 8443) attributed to city-area IP ranges via ISP-level ASN filtering. Results deduplicated by IP and port composite key. NAT-based shared networks cause structural under-representation: device counts behind shared public IPs are not visible to passive enumeration and actual device populations are likely higher than enumerated totals. Firmware version metadata is available only for endpoints that expose banner information; the versioned subset is not a statistically representative sample of the full population.

Comparative positioning. The relative risk positioning of Fez, Marrakech, and Casablanca is calibrated against published patterns of informal digital infrastructure in MENA heritage cities and against documented contrasts between dense medina environments and modern commercial districts in Moroccan urban areas. District-level indicators do not establish what is true inside any given building; the diligence questions in Section 6.3 mark the boundary between environmental assessment and property-level validation.

10. Appendix B. Selected Technical Terms

RTSP: protocol commonly used to stream video from surveillance devices.

NVR: network video recorder used to manage and store camera footage.

WPS: Wi-Fi Protected Setup, a convenience feature that can materially weaken local access control when left enabled.

CNDP: Morocco's data-protection authority.

11. Appendix C. Source Base

Regulatory and policy references. Royaume du Maroc, Loi 09-08 (2009): primary Moroccan data protection legislation. Royaume du Maroc, Loi 05-20 (2020): national cybersecurity framework and critical infrastructure obligations. CNDP (Commission Nationale de contrôle de la Protection des Données à caractère Personnel): public guidance and enforcement publications. DGSSI (Direction Générale de la Sécurité des Systèmes d'Information): public advisories and national cybersecurity guidance.

Methodology references. Office of the Director of National Intelligence: Intelligence Community Directive 203 (ICD-203), Analytic Standards. Shodan and Censys: passive enumeration methodology for internet-facing surveillance infrastructure. WiGLE (Wireless Geographic Logging Engine): wardriving methodology and vendor cross-reference for wireless proximity surveys. IEEE OUI Registry: hardware vendor identification via MAC address prefix attribution.

Market and demographic context. Haut-Commissariat au Plan (HCP), Morocco: urban planning and demographic data for Moroccan cities and Medina population estimates. UNESCO World Heritage Centre: documentation on Moroccan medinas as designated heritage sites. Secondary OSINT on Moroccan tourism density, riad accommodation distribution, and hospitality market structure, drawn from publicly available tourism industry reporting.

Comparative environment references. Published academic and policy literature on informal digital infrastructure in MENA and comparable heritage urban environments, used to support the comparative reasoning underpinning the cross-portfolio judgements in Section 6.1.