

INTELLIGENCE SECURITY ASSESSMENT

Can essential work continue without the office?

A sample continuity component of an Intelligence Security Assessment for a hypothetical Southwest Florida service business.

Demonstration, not client work. Business context is hypothetical. Public facts are referenced; judgments and information gaps are stated. This is not a live alert.

Executive assessment

Validate the business's ability to keep essential work moving when its normal office is unavailable. For the assumed business, the immediate research priority is the relationship between premises access, electricity, dispatch communications, and customer records.

A written continuity plan is useful only if its dependencies and recovery arrangements have been checked. No site inspection or test was performed for this sample, so it does not assign a property-specific security rating.

Operating context and public evidence

Assumed context: a Southwest Florida service contractor uses one office for dispatch and customer records, with field crews depending on telephone and internet access. Backup arrangements have not been evidenced. This is a hypothetical scenario, not a finding about a real business.

Public context: NOAA identifies June 1-November 30 as the Atlantic hurricane season and recommends advance planning and a communication plan that remains usable without internet access [1]. The U.S. Department of Energy advises businesses to identify critical utility dependencies, discuss backup options, and test backup systems [2].

Assessment: a disruption affecting several office dependencies could interrupt service even if field equipment remains usable. The business needs evidence of recovery capability before deciding whether additional resilience spending is justified. No current storm, local outage, or imminent threat is asserted.

Illustrative risk register

Provisional priorities for the assumed context; no measured likelihood scores

Exposure	Potential consequence	Priority / evidence gap
Dispatch concentrated at one office	Crews may lose work assignments if the office cannot operate.	Validate first: confirm an alternative dispatch process and its owner.
Power and connectivity dependencies	Phones and business applications may become unavailable.	Validate first: obtain evidence of tested fallback arrangements.
Records accessible only through the normal workflow	Customer commitments and restoration priorities may be unclear.	Validate next: establish whether authorized staff can retrieve essential records.

Priority follows the assumed role of each dependency in keeping the business operating. Event likelihood is unassessed. Consequences are plausible, not observed losses; an overall risk score would imply more evidence than this exercise provides.

Action priorities and ownership

1. Operations lead: identify the smallest set of activities needed to maintain essential service. Name who can authorize the fallback process if the usual manager is unavailable.
2. Office or dispatch lead: document how authorized staff will communicate assignments and customer updates through a tested alternative channel.
3. IT or service provider: demonstrate authorized access to essential records through the agreed recovery arrangement. Record the result, gaps, and responsibility for follow-up.
4. Management: compare the consequences of interruption with the cost and practicality of fixing the evidenced gaps. Obtain qualified utility or technical advice before changing systems.

A useful acceptance criterion is a documented exercise showing that the chosen essential task can be completed when the normal office workflow is unavailable. Management sets the recovery objective; this sample does not invent a suitable time limit.

Confidence and limits

High confidence: the cited agencies publish the preparedness principles summarized here. Moderate confidence: the assumed dependencies deserve validation. Low confidence: any judgment about actual business readiness, because no business records, site conditions, fallback tests, or staff interviews were reviewed.

This is a public-source continuity component of an Intelligence Security Assessment, not a complete all-hazards assessment. It includes no on-site security survey, engineering certification, cybersecurity testing, licensed protective service, or emergency response. Operational decisions during an incident must follow the relevant authorities and qualified service providers.

Indicators for reassessment

Reassess after an office move, a change of dispatch or records provider, a failed recovery exercise, or a material change in the work that the business considers essential. Review relevant official alerts as conditions change. A completed checklist is not evidence that a fallback works.

Source register and method

1. NOAA, Prepare Before Hurricane Season. Preparedness and communication principles; reviewed October 29, 2026.
2. U.S. Department of Energy, Business Owners: Prepare for Utility Disruptions. Business utility dependencies and backup validation; reviewed October 29, 2026.

Rook Vantage's assumed business context, prioritization, and proposed validation steps are original analysis. No agency endorsement is implied. This sample is not a current weather forecast or a location-specific hazard assessment.

Online edition: rookvantage.com/samples/business-continuity-assessment/
Contact: mbardsley@rookvantage.com