**Notes – How security events could arise in this environment (40‑60 words)**  
Although local crime is low, the bank’s wide digital footprint (120 staff—20 of them remote—and highly public marketing partnerships) greatly expands its cyber‑attack surface. Coastal hurricanes can interrupt cash deliveries and power, while strict U.S. banking regulations mean any loss of funds or customer data would attract heavy fines and reputational damage.

| **Risk** | **Likelihood (1‑3)** | **Severity (1‑3)** | **Priority = L × S** | **Rationale (concise)** |
| --- | --- | --- | --- | --- |
| Business email compromise | **3** | **3** | **9** | Phishing is pervasive and targets finance staff; a successful BEC can trigger fraudulent wire transfers and violate FFIEC/GLBA requirements. |
| Compromised user database | **2** | **3** | **6** | Moderate chance via weak crypto or insider error; exposure of PII/financial data incurs major regulatory penalties and customer attrition. |
| Financial records leak (backup server exposed) | **1** | **3** | **3** | Misconfiguring an off‑site backup is less frequent but would reveal sensitive ledgers, triggering audits and fines. |
| Theft of cash (safe left unlocked) | **1** | **3** | **3** | Robust physical controls and CCTV make occurrence rare, yet any cash loss directly affects reserve requirements and insurance claims. |
| Supply‑chain disruption (cash delivery delayed by storm) | **2** | **2** | **4** | Coastal storms occur periodically; delayed armored‑car deliveries strain daily Fed reserve balances but rarely halt operations completely. |