

# Fraud Prevention Checklist



As a leader of your organization, your role is pivotal in determining strategy, awareness, and response to the threats of fraud facing your business.

According to [www.CISA.gov](http://www.CISA.gov), managing cyber risks requires building a culture of cyber readiness. You should focus on these essential elements:



• **Yourself** – be aware of the basics and drive fraud prevention strategy, investment, and culture



• **Your Surroundings** – ensure only those who belong on your digital workplace have access to your assets and critical applications



• **Your Staff** – develop cyber security awareness and vigilance



• **Your Data** – regularly back up critical data



• **Your Systems** – protect your critical assets and applications



• **Your Crisis Response** – be prepared with a plan to limit damage and restore operations

Here are three important suggestions and considerations:

## 1 Conduct an overall Fraud and Cyber Security Review



- A.** Engage a third party partner, or leverage the CISA Toolkits
- B.** Evaluate firewall software & update schedule
- C.** Implement email screening software to identify and alert for external senders
- D.** Implement controls and protocols governing validation of requests submitted by email
- E.** Implement malware detection software & regularly apply updates
- F.** Establish & Audit internal controls
  - i.** role-based data access
  - ii.** multi-factor authentication & password management
  - iii.** dual authorization
  - iv.** personal device & wi-fi security
  - v.** daily account reconciliation
- G.** Review data & system backup schedules, storage, and security
- H.** Review cyber insurance coverage

## 2

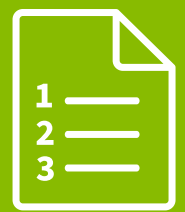
### Develop an ongoing Employee education and awareness program



- A.** Provide education on phishing, smishing, and social engineering campaigns
- B.** Educate on Business Email Compromise
- C.** Conduct regular testing and audit results
- D.** Train employees on basic security practices like strong passwords & internet security
- E.** Create a culture of risk awareness

## 3

### Establish a Fraud & Risk Governance Plan



- A.** Include an Incident Response Plan
  - i.** Know who to call, how to reach them, and individual roles
  - ii.** Conduct regular cyber security assessments
  - iii.** Include a ransomware event in plan
- B.** Identify and document risk tolerance
  - i.** Ensure risk tolerance is consistent with cyber insurance coverage
- C.** Create a robust vendor management program
- D.** Obtain Executive and Board level approval

The information presented is general in nature and should not be considered, legal, accounting or tax advice. Regions reminds its customers that they should be vigilant about fraud and security and that they are responsible for taking action to protect their computer systems. Fraud prevention requires a continuous review of your policies and practices, as the threat evolves daily. There is no guarantee that all fraudulent transactions will be prevented or that related financial losses will not occur. Visit [regions.com/STOPFRAUD](http://regions.com/STOPFRAUD), or speak with your Banker for further information on how you can help prevent fraud.