Freddie Mac
SINGLE-FAMILY

Preparing for Cybersecurity Risk Assessment

Freddie Mac Information Security conducts third-party risk assessments to ensure the integrity and security of our operations. This assessment benefits your organization by providing a structured framework for identifying and mitigating potential risks, as well as fostering a transparent and secure business environment.

To prepare for the Freddie Mac Information Security cybersecurity risk assessment, you can take a series of practical, proactive steps to prepare you for your assessment and ensure the process goes smoothly and yields meaningful results:

1. **Engage Stakeholders and Assign Responsibilities**
   - Notify relevant teams about the upcoming assessment.
   - Assign a point of contact to coordinate with the cyber examiner.

2. **Gather and Organize Documentation**
   - Prepare up-to-date network diagrams, asset inventories and lists of applications.
   - Compile security policies, procedures, incident response plans and previous audit reports.

3. **Review and Update Security Controls**
   - Ensure technical controls (firewalls, antivirus, access controls) are active and documented.
   - Review physical and administrative controls for completeness.

4. **Address Regulatory and Business Requirements**
   - Compile documentation on compliance with relevant standards (e.g., NIST, ISO).
   - Highlight critical business processes and sensitive data.

5. **Prepare for Interviews and Data Collection**
   - Schedule meetings between assessors and key personnel.
   - Inform staff about the assessment and encourage transparency.

6. **Document Known Risks and Past Incidents**
   - Create a summary of previously identified risks, vulnerabilities and privacy and security incidents.

7. **Provide Necessary Access**
   - Arrange for secure, temporary access to systems, applications and physical locations as needed.

8. **Communicate with Staff**
   - Explain the purpose and importance of the assessment to all involved.
   - Encourage cooperation and honest feedback.

9. **Plan for Remediation and Follow-Up**
   - Be ready to address any findings and recommendations from the assessment.
   - Establish a process for ongoing risk management and improvement.

We intend for this proactive approach to build your trust and confidence, ensure smoother collaboration and reduce the likelihood of disruptions.

For Freddie Mac, the assessment helps us maintain regulatory compliance and safeguard sensitive information, which is vital for maintaining trust with our stakeholders and the broader market.

By proactively managing third-party risks, Freddie Mac enhances its ability to make informed decisions, ensuring that its business relationships meet regulatory expectations and align with strategic objectives and risk tolerance levels.