بسم الله الرحمن الرحيم

مؤسسة النقد العربي السعودي

إدارة التفتيش البنكي — المركز الرئيسي

الرقم: ...../م ا ت/ ٢٥٥١٤

المرفقات: ٢

تعميم عاجل

سعادة/ المحترم

البنك/

بعد التحية

الموضوع: إجراء تقييم لأنظمة الحماية وأمن المعلومات لجميع البنوك العاملة في المملكة.

انطلاقاً من حرص المؤسسة على تطوير البنوك العاملة في المملكة بنيتها الأساسية لأنظمة الحماية وأمن المعلومات، وتطوير أنظمة وخطط استمرارية العمل (Business Continuity Plan) ومراجعتها واختبارها بشكل دوري. وحث البنوك على الالتزام الكامل بالأنظمة والتعليمات الصادرة من المؤسسة في مجال أمن المعلومات وأتباع أفضل الممارسات العالمية (Best Practice) في هذا المجال، وتطبيق التوصيات الصادرة من اللجنة المصرفية لأمن المعلومات (BCIS) لتحقيق أعلى مستويات الأمان لتلك لأنظمة.

ونظراً لأهمية التحقق من قوة وسلامة وجاهزية تلك الأنظمة بشكل مستمر، نأمل تكليف إحدى الشركات العالمية المتخصصة في مجال أمن المعلومات لتنفيذ برنامج تقييم شامل لأنظمة الحماية وأمن المعلومات وخطط استمرارية العمل القائمة لدى البنك، وأن يتضمن برنامج التقييم العناصر الإرشادية الواردة في البيان المرافق. ومن ثم إعداد تقرير تفصيلي يتضمن تقييماً للوضع الحالي لتلك الأنظمة القائمة وتحديد أهم الملاحظات في شأنها والتوصيات المقترحة لتطويرها، وإعداد تقرير مفصل بالنتائج والملاحظات والتوصيات وإرساله للمؤسسة في موعد أقصاه نهاية شهر يناير ٢٠١٣م.

وفي حال وجود أي استفسار بهذا الخصوص يمكن التواصل مع رئيس وحدة فحص البنوك المحلية بإدارة التفتيش البنكي الأستاذ/ تركي الجمعة على هاتف رقم (٤٦٣٣٠٠٠) تحويلة رقم (٥٣٢١) أو المفتش البنكي/ مروان اللحيدان على هاتف رقم (٤٦٣٣٠٠٠) تحويلة رقم (٥٨١٨).

وتقبلوا تحياتي ،،،

وكيل المحافظ للشئون الفنية

عبدالرحمن بن عبدالمحسن الخلف

مراقبة البنوك

النطاق

- البنوك العاملة في المملكة

Minimum Requirements for IT Evaluation Program

1- Evaluate the adequacy of all aspects of IT security governance in the bank including update of IT security policy, effectiveness of reporting line of head of IT security.

2- Do Risk assessment of all IT infrastructure, database, networks and various operating systems safeguard controls are in place for protection of these information and IT related infrastructure. Includes consideration of information security risks from malicious external threats and internal vulnerabilities to the Bank's IT and communication infrastructure.

3- Do External Penetration Test through Certified Ethical hacker :

- Black Box
- White Box

4- Evaluate the protection systems against new Kind of Malwares (whether from inside and outside)

5- Review the security configuration of the routers, firewalls, IPS, IDS

6- Test efficiency of Network Segmentation against spreading malware if part of network affected.

7- Evaluate DDoS attack mitigation solutions

8- Test Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures are implemented

9- Review Antivirus signature and it is up to date on all machines and it is monitored effectively.

10- Review Intrusion Detection System & Intrusion Prevention System and how are these response if there is suspicious activity (and Evaluate their location in the network). Also make sure the log reviewed in daily basis at least.

11- Test Incident management response through test scenario.

12- Evaluate and test Business Continuity Plan and Data Recovery Plan and Confirm that BCP and DRP also cover information security related incidents caused from both the external threats and internal sources.

13- Check the Segregation of Duties in IT Security, IT Operation Roles.

14- Verify there is adequate procedure for scanning attachment that coming by Email against Trojans and malware.

15- Verify that there are adequate and strict procedure for using removable media.

16- Verify that there are updated policies and secure procedures in place for remote access to the organization's networks

17- Confirm that security risks have been considered for each component of IT infrastructure, perimeter security has been considered in the network design and network segments with high security risk have been identified.

18- Evaluate process and functions for SOC (Security Operation Center) and NOC (Network Operation Center).

19- Evaluate the outsourced security functions

20- Evaluate how adequate the adopted IS awareness campaign (internally and externally).

21- Verify that there are logging activities in place for all systems and check how these logs are reviewed.