۳-۸- تمهیدات مقابله با بحران

در بانک ملت آزمون‌های بحران (stress test) در بخشهای مختلف فناوری اطلاعات صورت می‌گیرد. در بخش مدیریت امنیت اطلاعات آزمون‌های دوره‌ای نفوذ پذیری بر روی وب سایتهای حساس بانک به صورت دوره‌ای و موردی انجام می‌پذیرد. در بخش مراکز داده به ایجاد سایت پشتیبان به منظور پشتیبانی از سایت اصلی بانک و ایجاد سایت بحران به منظور جایگزین شدن برای سایت اصلی در زمان بحران اقدام شده است. شرایط عملیاتی سایت پشتیبان و بحران در مانورهای دوره‌ای تست و اصلاح می‌گردد. در بخش سیستم‌های اطلاعاتی آزمونهای مرتبط با ظرفیت و عملکرد سیستم-های اطلاعاتی مبتنی بر تغییر متغیرهای مرتبط با امنیت و افزایش بار به صورت دوره‌ای صورت می‌گیرد. در این بخش برخی از اقدامات انجام شده برای مقابله با بحران تشریح می‌گردد:

الف)تحلیل سناریو و انجام آزمون‌های نفوذ پذیری وب سایتها و سیستم‌های بانک: در این بخش سیستمهای اطلاعاتی و نرم افزاری حساس بانک به منظور بررسی وضعیت امنیتی بصورت دوره‌ای مورد آزمونهای بحران قرار می‌گیرند. تحلیل سناریو انجام آزمونهای نفوذپذیری وب سایت‌های حساس بانک، آزمون سرویس **Active Directory** و سایر سرویس-های وابسته و آزمون نفوذپذیری برروی کلیه سامانه‌ها قبل از عملیاتی شدن در محیط اصلی مبتنی بر وب از اهم اقدامات صورت گرفته می‌باشند.

ب)آزمون‌های مرتبط با ظرفیت و عملکرد سیستم‌های اطلاعاتی: در این بخش متغیرهای مرتبط با امنیت و افزایش صحت عملکرد سیستم‌ها، سرویس‌ها و سامانه‌های بانک مورد آزمون قرار می‌گیرد. بررسی صحت عملکرد سیستم پشتیبان سامانه اتوماسیون اداری در سایت بحران، آزمون سرویس **Active Directory** و سایر سرویس‌های وابسته و آزمون سامانه ضد ویروس مرکزی از مهمترین اقدامات این بخش می‌باشند.

ج)آزمون‌های مرتبط با عملکرد منابع سخت افزار و رویه‌های امنیتی: در این بخش تجهیزات سخت افزاری و همچنین رویه-های امنیتی تدوین شده به منظور صحت عملکرد مورد آزمون قرار گرفته است. اهم اقدامات صورت گرفته بدین شرح است: مانور قطع برق جهت تست عملکرد تاسیسات و تجهیزات در سایتهای بانک، ارزیابی‌های امنیتی شبکه‌های ارتباطی بانک و بازدیدهای دوره‌ای امنیتی ازمدیریت شعب استانها و شعب تابعه.