

Aspect	Weaknesses Before Migration	Strengths After Migration
Security Management	<p>No centralized security department</p> <p>No security policies, standards, or procedures</p>	<p>Centralized security department established</p> <p>Security standards, procedures, and guidelines developed and documented</p>
Access Controls	<p>Limited to online Applications</p> <p>No facility for users to change passwords</p> <p>No lockout for unsuccessful password attempts</p> <p>Account IDs and passwords stored unencrypted</p>	<p>Password-controlled access with expiration, limited re-use, lockout, and hashing.</p> <p>Data objects protected by default</p>
Data Protection	<p>No protection for objects from access outside of online applications</p> <p>Production downtime due to accidental testing parameters</p>	<p>Data objects protected by default</p> <p>Production downtime eliminated</p>
Monitoring and Reporting	<p>No facility to discover or record sign-on failure attempts</p> <p>No security manual or documentation of procedures</p>	<p>Suspicious and/or unusual activity recorded and reviewed</p> <p>Comprehensive security documentation created</p>

User Training and Support	No formal training or support structure for users	<p>Training documentation created</p> <p>Mini boot camps conducted for training</p> <p>Additional staff recruited for user support</p>
Technological Infrastructure	Operating in a 1980s technology environment with no LANs or WANs	<p>Migration to the most current mainframe hardware and operating system</p> <p>Implementation of LAN providing an intranet site</p>