**Module 3 Architecture & Design**

**3.8 Resiliency**

**Automation/Scripting**

* Reduces risk through repeatable processes & automated courses of action
* Leveraging sophisticated monitors & sensors/continuous monitoring
* Configuration validation
* OS scripting languages

1. Linux shells – Bash, Ksh
2. Windows – PowerShell

**Frameworks & Templates**

* See section 3.1 for common frameworks (NIST, ISO, PCI-DSS)
* System baselines using standard templates
* Compare current state against desired state

**Master Image**

* AKA “Gold” Image
* Creating model OS verified as “clean”
* Used for system restores
* Needs to be secured

**Managing Cloud Risk**

* Non-persistence – temporary system images. Snapshot of known, good state
* Elasticity/scalability – adjusting resources as needed
* High Availability (HA) – measures such as redundancy, failover & mirroring used to keep services & systems operational
* Redundancy – replicating systems usually at multiple sites. Associated with failover
* Distributive allocation/Load balancing – distributing burden across multiple systems

**Fault Tolerance**

* Ability of system to sustain operations in event of component failure
* 2 key components – spare parts & electrical power
* Power protection

1. Surge power
2. Uninterruptible Power Supply (UPS)
3. Backup power/generators

**RAID (Redundant Array of Inexpensive Disks) Storage**

* Focuses on availability of data
* RAID Types

1. 0 – disk striping
2. 1 – disk mirroring
3. 3 – disk striping with parity disk
4. 5 – disk striping with parity