Disaster Recovery Program

"Maturity Model" for the Checklist

Date: _____

Organization: _____

Strategy	I	II	III	IV	V
___/5 Complete System List *(signed-off BIA, services, components)*	-focus on individual **systems**, in a specific DC or computer room, identified as critical	-DR for a **standalone DC with a specific exposure to** systems running there	-**BIA** performed (BCP may not have been done) -focus on most demanding customers & their applications -limited to particular geography and/or DC	-**separate BIA & BCP** initiatives, that supply a systems list - **critical 3rd party (outsourced) services** included	-Fully **integrated BC** initiative for all business units (all jurisdictions, locations, services) -includes critical outsourced & SAAS applications & services -identifies important IT processes & services for customers – in all sites
___/5 Tiered Services *(tier definitions / SLAs, criticality factors)*	-critical systems identified, but no documentation of rationale or tiers or ranking within tiers	- tiers & critical systems identified -criticality factors identified	-tiers & ranking documented -RTO & RPO's defined	-widely-published list -recovery commitments are consistent with SLAs	-all IT service activity is driven via Tier structure (importance & funding) -active "customer" involvement in prioritization & SLAs -based on relevant internal & external (regulatory, investor, customer) drivers
___/10 Recovery Strategy *(interconnections, tech. alternatives, costs, speed of recovery)*	-unique approach for each critical application	-consolidation of recovery approaches for most critical applications	-use of proven recovery tools and approaches to rapidly recover all critical applications and enable faster recovery of lower priority applications	-proven recovery tools in place for all applications - infrastructure components, applications & services for all Tiers are accommodated	-applications migrated to DR-friendly technology (e.g. highly –portable due to virtualization & replication of processing & storage)
___/5 Site Selection *(threats, evaluation factors)*	-potential site(s) identified that may be available for use aToD – may be exposed to same threats	-pre-arranged recovery site	-optimal pre-arranged recovery site that accommodated staff & key suppliers from common threats & vulnerabilities	-contracted site, accessible to staff, with additional recovery resources	-fully-provisioned recovery site, with little or no exposure to common threats -accessible & able to accommodate BC team
___/5 Approvals *(budget, people allocation, pgm. def'n)*	-little / no operating or capital budget for DR	-DR plans funded out of existing IT operating budget & staff	- DR plan development funded through specific IT operating & capital budget	-DR plans funded via overall DR program funding for specialized people, facilities, methods & technology	-DR plans funded through a mix of explicit and imbedded investments by customers
___/30 **Sub-total Strategy**					

Disaster Recovery Program

"Maturity Model" for the Checklist

Date: _____

Organization: _____

Implementation	**I**	**II**	**III**	**IV**	**V**
___/5 I1. Services Arrangements *(recovery site, recovery services)*	-simple arrangements to provide "cold / standby" site capability	-arrangements include shared or "warm" site capabilities	-contracted "hot" site capability	-"hot & warm" site capabilities	-covers all Tiers -contractual SLA's -familiar with facilities & tools to assist & accommodate tests -change flexibility -optional recovery support
___/5 I2. Communications *(primary - recovery site, remote access)*	-little/no supplemental DR arrangements (e.g. reliance on internet access aToD)	-ability to activate temporary connections to facilitate team and remote user access	-"reduced service" permanent PROD-DR connections at recovery site	-flexible capacity at DR site to expand permanent if required	-fully-expandable capacity for users & remote support staff -fully-meshed, expandable network capacity
___/10 I3. Technology *(recovery equipment, config. & test)*	-standard back-up & restoration systems in place	-some virtualization & replication in place	-specialized hardware & software for recovery & remote access	-recovery management system in place	-DR-friendly technology only -self-aware, self-monitoring & alerting (specialized DR team notification tools)
___/5 I4. As Built Documentation *(settings / configuration, steps)*	-totally reliant on access to 3RD party materials	-possess original vendor documentation	-original configuration documentation available -relationships between applications & technical components well-documented		-fully-referenced in DR Plan -written at appropriate level -complete map of applications by tier to technology (e.g. server names)
___/5 I5. Documented Plan *(stages, activities, roles, references)*	-plan may have gaps, with inconsistent format & terminology	-documentation covers all stages of recovery -consistent use of terms	-documentation outlines roles, as well as, sequential work steps -includes definitions	-documentation includes references to supplemental details & procedures -simple, unambiguous language	-Consistent format, single document, multiple sections -complete declaration, decision-making guidance, consistent with incident mgmt.
___/5 I6. Organization *(governance, steering, DRC, recovery team, support)*	-operations responsibility -DR role not well defined / imbedded in staff profiles -recovery team – not pre-defined (as available)	-recovery leader identified -"unofficial" recovery team responsibilities	-identified recovery team members -identified management escalation, declarers & decision-makers	-DR responsibilities added to job profiles	-top stakeholder -permanent + back-up DRC's -recovery team training & awareness
___/5 I7. Technical Test *(by appl'n / infrastructure component)*	-simple recovery technology testing of infrastructure components	-testing of individual applications in isolation	-integrated applications recovery testing	-successful multi-level testing of applications and infrastructure components	-verifiable (3rd party), successful testing of individual application services & components
___/**40** **Sub-total Implementation**					

Disaster Recovery Program

"Maturity Model" for the Checklist

Date: _____

Organization: _____

Maintenance		**I**	**II**	**III**	**IV**	**V**
___/5	M1. Failover & Failback Tests *(lessons learned, performance)*	-able to test failover to DR (in parallel to live PROD)	-able to failover to DR & shut-down PROD	-able to failover to DR & failback to PROD (no transaction processing)	-successful failover & failback testing with users	-successful failover & failback testing with typical user volumes -prompt issue resolution
___/5	M2. Accessible Plan *(distribution, electronic access)*	Hardcopy master only	Maintained, written plan, at sites	Central electronic version, distributed to sites	Portable plan downloaded designated individuals when updated	**Anytime, anywhere role-based access to all potential users (int. / ext.)** **Resilient hosting** of electronic version
___/5	M3. Live Test *(user involvement)*	**-PROD disconnected** -**preplanned off-hours testing** (little / no risk to users)	-Users connected to DR -Users validate failover	-**User testing of DR integration, integrity, security & performance** (i.e. data entry)	-**Planned failover during business hours** (full client remote access) -**Failback to PROD off-hours**	**-Unannounced failover during business hours** -Critical applications-Failback to PROD
___/5	M4. Current As Built Documentation *(reflects changes)*	Tacit knowledge only	Configuration information recorded for initial installations	Updates to configuration information for new systems	Updates to configuration information for historical systems	Automatic updates to configuration information
___/5	M5. Maintained Plan *(updates, people information)*	-updated annually for compliance reasons, or whenever DR site is relocated	-updated as recovery staff change	-updated when there are significant changes to recovery or underlying technology	-updated when recovery process and procedures change	-continuous validation/refresh, especially when there are changes to the applications
___/5	M6. On-going Program *(integrated change processes, verification, funding)*	-overall objectives & policy statement in place	-well-defined program scope	-organization & responsibilities identified	-published program overview -annual program funding -methods identified (e.g. DR gate for projects, enhancements & changes)	-permanent position(s) -DR imbedded in regular practices (e.g. operations & development processes) -regular audits
___/30	**Sub-total Maintenance**					
___/100	**Total Score** (<50 – "still building"; 50-69 – "work-in-progress"; 70-89 –"good"; 90+ - "mature")	**Minimal**	**Basic Recovery**	**Technical Recovery**	**Advanced DR**	**Business Recovery**
		0-20	**21-40**	**41-60**	**61-80**	**81-100**

Note: aToD = "at Time of Disaster"