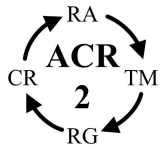




Risk Update Report Sample

Revised 12/01/2006



Date of Report

2-Nov-2005

26-Jul-2006

Threat Source	Vulnerability	Baseline Risk Score	Updated Risk Score	Change in Risk Score
Wind	Roof damage	5	5	0
Fire	Smoke damage	50	25	25
Flood	Facility damage	50	20	30
Power loss	Loss of operations	1	10	9
Power loss	Damage to building	5	1	4
Vehicle collision	Facility damage	1	5	4
Human error	Data acquisition	1	25	24
Human error	Data storage	1	5	4
Human error	Data retrieval	5	5	0
Human error	Data modification	5	5	0
Human error	Data transmission	50	5	45
Human error	System design	25	10	15
Human error	Procedure implementation	5	5	0
Human error	Internal controls	5	5	0
Malicious insider	Data acquisition	5	5	0
Malicious insider	Data storage	5	5	0
Malicious insider	Data retrieval	5	5	0
Malicious insider	Data modification	5	5	0
Malicious insider	Data transmission	50	25	25
Malicious insider	System design	25	50	25
Malicious insider	Procedure implementation	5	5	0
Malicious insider	Internal controls	5	5	0
Malicious outsider	Data acquisition	5	25	20
Malicious outsider	Data storage	1	1	0
Malicious outsider	Data retrieval	25	5	20
Malicious outsider	Data modification	1	1	0
Malicious outsider	Data transmission	50	50	0
Malicious outsider	System design	10	10	0
Malicious outsider	Procedure implementation	1	1	0
Malicious outsider	Internal controls	1	1	0

Risk is a function of the likelihood of a given **threat-source's** exercising a particular vulnerability, and the resulting **impact** of that adverse event (NIST 800-30, p8)

Risk Score - is determined by multiplying the probability of event, Low (0.1), Medium (0.5) or High (1.0) by the impact of the event, Low (0.1), Medium (0.5) or High (1.0). Scores run from 1 to 100, with 50-100 being High, 10-50 being Medium and <10 being Low. For risks labeled High, corrective action must be taken "as soon as possible" (NIST 800-30). For Medium Risks, a correction plan must schedule a "reasonable amount of time", while Low risks may be merely observed.

Baseline Risk Score - the first risk assessment in a given year.

Updated Risk Score - follows the first risk assessment in a given year. Scores may be better or worse, depending on changes in safeguards and safeguard performance.

Change in Risk Score - Risk scores will change with changes in safeguards used and in safeguard performance. For example, use of encryption will dramatically reduce the impact of data retrieval by a malicious outsider. Increases in risk are highlighted in **red**