Excel Worksheet Example #1 - Combined Summary page - combined view of risks

Risk Matrix		Occurrence Likelihood					
		Remote *[<1% chance of occurrence]*	Highly Unlikely *[1% to 10% chance of occurrence]*	Unlikely [10% to 25% chance of occurrence]	Possible [25% to 70% chance of occurrence]	Likely [70% to 99% chance of occurrence]	Almost Certain [>99% chance of occurrence]
Impact Effect	Catastrophic	6	12	18	24	30	36
	Critical	5	10	15	20	25	30
	Major	4	8	12	16	20	24
	Moderate	3	6	9	12	15	18
	Minor	2	4	6	8	10	12
	Insignificant	1	2	3	4	5	6

Risk Tolerance Threshold (*Moderate Risk*)

INITIAL RISK ASSESSMENT - UNWEIGHTED & AVERAGED - Risk Scoring Range (1 to 36)				
LOW (1-4)	MODERATE (5-11)	HIGH (12-19)	SEVERE (20-29)	EXTREME (30-36)

*Compensating Controls & Control Weighting Convert Risk Score To

FINAL RISK ASSESSMENT - WEIGHTED & AVERAGED - Risk Scoring Range (1 to 180)				
LOW (1-22)	MODERATE (22.1-57)	HIGH (57.1-97)	SEVERE (97.1-147)	EXTREME (147.1-180)

	Initial Risk Assessment	Compensating Factors	Final Risk Assessment
CYBERSECURITY RISK SUMMARY	MODERATE *5* *Raw Value*	→	LOW *13* *Weighted Value*
NATURAL & MAN-MADE RISK SUMMARY	MODERATE *9* *Raw Value*	→	MODERATE *29* *Weighted Value*

Excel Worksheet Example #2 - Combined Summary page - combined view of risks

Risk Component Definitions		
Raw Score	**Occurrence Likelihood** *[under normal business conditions]*	**Impact Effect**
6	**Almost Certain** *[>99% chance of occurrence]* - Event occurrence is virtually certain to occur.	**Catastrophic** - Catastrophic damage, cost or service impact. Financial and reputational damage is enough to ruin the business.
5	**Likely** *[70% to 99% chance of occurrence]* - Event occurrence is reasonably certain to occur, based on current operating environment and controls in place.	**Critical** - Critical damage, cost or service impact. Financial and reputational damage has long-term negative consequences to the business.
4	**Possible** *[25% to 70% chance of occurrence]* - Event occurrence is possible, based on current operating environment and controls in place.	**Major** - Major damage, cost or service impact. Extensive short-term reputational or financial impact, but not enough to ruin the business.
3	**Unlikely** *[10% to 25% chance of occurrence]* - Event occurrence is unlikely, based on current operating environment and controls in place.	**Moderate** - Noticeable damage, cost or service impact. Harmful short-term reputational or financial impact, but not enough to ruin the business.
2	**Highly Unlikely** *[1% to 10% chance of occurrence]* - Event occurrence is possible, but improbable.	**Minor** - Localized or minimal damage, cost or service impact. Minor short-term reputational or financial impact.
1	**Remote** - Theoretically possible *[<1% chance of occurrence]*. Event occurrence could manifest only under exceptional circumstances.	**Insignificant** - Little to no damage, cost or service impact. No reputational or financial impact.

CAPABILITY MATURITY MODEL (CMM) SPECTRUM

IT Security Program Maturity Summary **3**

CMM Level	CMM Level Definitions	Associated Risks
0	Incomplete	There is a few or no identifiable work products or outputs.
1	Performed	Purpose of processes is general achieved. Ad hoc processes are used.
2	Managed	Work products fulfill basic quality expectations within time & resource requirements.
3	Established	Defined processes are used to achieve outcomes. Process is performed & managed.
4	Predictable	Processes are performed consistently. Quantitative understanding through detailed metrics.
5	Optimizing	Defined and standardized processes are dynamically adapted to meet current & future need

Excel Worksheet Example #3 - Appendix B Controls Worksheet - drop-down & fill-in worksheet for natural & man-made risk

Threat Category	Threat Type	Threat Description	Occurrence Likelihood	Potential Impact	Compensating Factors	Risk Assessment Notes *(Justification for compensating controls or other factors that need to be explained)*		*Risk Factor (unweighted)*		*Risk Factor (compensated & weighed)*	
NATURAL DISASTERS	Pandemic (Disease) Outbreaks	Due to the wide variety of possible scenarios, consideration should be given both to the magnitude of what can reasonably happen during a pandemic outbreak (e.g., Influenza, SARS, Ebola, etc.) and what actions the business can be taken to help lessen the impact of a pandemic on operations.	Highly Unlikely	Major	Moderate Impact Reduction			*8*	MODERATE	*11*	LOW
	Severe Weather	Severe weather is a broad category of meteorological events that include events that range from damaging winds to hail.	Possible	Minor	Minimal Impact Reduction			*8*	MODERATE	*20*	LOW
	Space Weather	Space weather includes natural events in space that can affect the near-earth environment and satellites. Most commonly, this is associated with solar flares from the Sun. An understanding of how solar flares may impact the business is of critical importance in assessing this threat.	Highly Unlikely	Moderate	None Available			*6*	MODERATE	*18*	LOW
	Thunderstorms & Lightning	Thunderstorms are most prevalent in the spring and summer months and generally occur during the afternoon and evening hours, but they can occur year-round and at all hours. Many hazardous weather events are associated with thunderstorms. Under the right conditions, rainfall from thunderstorms causes flash flooding and lightning is responsible for many fires and fatalities.	Possible	Minor	None Available			*8*	MODERATE	*24*	MODERATE

Excel Worksheet Example #4 - Appendix C Controls Worksheet - drop-down & fill-in worksheet for cybersecurity risk

Control Description	Likelihood of Control NOT Operating Properly	Potential Impact of Control NOT Operating Properly	Compensating Factors *(see Risk Assessment Notes)*	Assessed Level of Maturity for the Capability (Process / Technology)	Risk Assessment Notes *(Explanation of compensating factors to justify reduction in risk)*	Associated Risk from a Control Deficiency (CD)	*Risk Factor (unweighted)*		*Risk Factor (compensated & weighed)*	
Access to information system is limited to authorized users, processes acting on behalf of authorized users, or devices (including other information systems)	Improbable	Major	None Available	High level of maturity - capabilities, processes & documentation are robust and comprehensive.		*Information system access is not limited to authorized users or processes acting on behalf of authorized users or devices. This could allow nefarious activities to occur.*	*4*	LOW	*20*	LOW
Information system access is limited to the types of transactions and functions that authorized users are permitted to execute.	Improbable	Moderate	Moderate Impact Reduction	High level of maturity - capabilities, processes & documentation are robust and comprehensive.	Least access necessary principle deployed.	*Information system access is not limited to the types of transactions and functions that authorized users are permitted to execute. This could allow nefarious activities to occur.*	*3*	LOW	*11*	LOW
The flow of sensitive data is controlled in accordance with approved authorizations.	Improbable	Major	Significant Impact Reduction	High level of maturity - capabilities, processes & documentation are robust and comprehensive.	Encryption Vault deployed	*The flow of sensitive data is uncontrolled and could lead to a loss of sensitive data.*	*4*	LOW	*9*	LOW
Separation the duties for individuals is implemented to reduce the risk of malevolent activity without collusion.	Highly Unlikely	Moderate	Moderate Impact Reduction	High level of maturity - capabilities, processes & documentation are robust and comprehensive.		*Without collusion, individuals could conduct nefarious activities on systems and/or processes under their control.*	*6*	MODERATE	*8*	LOW
The principle of least privilege is employed, including for specific security functions and privileged accounts.	Improbable	Moderate	None Available	Moderate level of maturity - capabilities, processes & documentation are informal or not comprehensive.		*The principle of least privilege is not enforced, allowing users and processes to operate at higher than authorized privileges. This could allow nefarious activities to occur.*	*3*	LOW	*15*	LOW
The use of non-privileged accounts or roles is used when accessing nonsecurity functions.	Improbable	Major	Moderate Impact Reduction	High level of maturity - capabilities, processes & documentation are robust and comprehensive.	Perodic audits are completed to insure lease access necessary	*Privileged users (e.g., administrators) can use their privileged accounts for normal business user, instead of in "run as" or sudo scenarios. This could lead to account and/or system compromise.*	*4*	LOW	*14*	LOW
Non-privileged users are prevented from executing privileged functions and the execution of such functions are audited.	Improbable	Major	Moderate Impact Reduction	High level of maturity - capabilities, processes & documentation are robust and comprehensive.		*Regular users can execute privileged functions on the information system or application. This could allow nefarious activities to occur.*	*4*	LOW	*14*	LOW

Excel Worksheet Example #5 - Control Mapping summary - cybersecurity control mapping for NIST 800-171, NIST 800-53 and ISO 27002

Control #	Control Description	Relevant Security Controls				
		NIST SP 800-171	NIST SP 800-53 rev4		ISO/IEC 27002:2013	
ACCESS CONTROL (AC) CONTROLS						
C-AC-1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	3.1.1	AC-2	Account Management	9.2.1	User registration and de-registration
					9.2.2	User access provisioning
					9.2.3	Management of privileged access rights
					9.2.5	Review of user access rights
					9.2.6	Removal or adjustment of access rights
			AC-3	Access Enforcement	6.2.2	Teleworking
					9.1.2	Access to networks and network services
					9.4.1	Information access restriction
					9.4.4	Use of privileged utility programs
					9.4.5	Access control to program source code
					13.1.1	Network controls
					14.1.2	Securing application services on public networks
					14.1.3	Protecting application services transactions
					18.1.3	Protection of records
			AC-17	Remote Access	6.2.1	Mobile device policy
					6.2.2	Teleworking
					13.1.1	Network controls
					13.2.1	Information transfer policies and procedures
					14.1.2	Securing application services on public networks
C-AC-2	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	3.1.2	AC-2	Account Management	9.2.1	User registration and de-registration
					9.2.2	User access provisioning
					9.2.3	Management of privileged access rights
					9.2.5	Review of user access rights
					9.2.6	Removal or adjustment of access rights
			AC-3	Access Enforcement	6.2.2	Teleworking
					9.1.2	Access to networks and network services
					9.4.1	Information access restriction
					9.4.4	Use of privileged utility programs
					9.4.5	Access control to program source code
					13.1.1	Network controls
					14.1.2	Securing application services on public networks
					14.1.3	Protecting application services transactions
					18.1.3	Protection of records
					6.2.1	Mobile device policy

Excel Worksheet Example #6 - Weighting – Natural & Man-Made Risk - editable weighting for natural & man-made risks

Threat Category	Threat Type	Control Weight
NATURAL DISASTERS	Drought & Water Shortage	1
	Earthquakes	5
	Fire & Wildfires	4
	Floods	5
	Hurricanes & Tropical Storms	4
	Landslides & Debris Flow	3
	Pandemic (Disease) Outbreaks	2
	Severe Weather	3
	Space Weather	3
	Thunderstorms & Lightning	3
	Tornadoes	5
	Tsunamis	4
	Volcanoes	4
	Winter Storms & Extreme Cold	3
MAN-MADE DISASTERS	Civil or Political Unrest	3
	Hacking & Other Cybersecurity Crimes	5
	Hazardous Materials Emergencies	2
	Nuclear, Biological and Chemical (NBC) Weapons	4

Excel Worksheet Example #7 - Weighting – Cybersecurity Risk - editable weighting for cybersecurity risks

Control Category	Control #	Control Description	Control Type	Control Execution	Control Weight
	C-PE-5	Physical access devices are controlled and managed.	Preventative	Manual	3
	C-PE-6	Safeguarding measures for sensitive data are enforced at alternate work sites (e.g., telework sites).	Preventative	Automatic	3
RISK ASSESSMENT	C-RA-1	The risk to organizational operations, processes, assets, and individuals, is periodically assessed.	Detective	Manual	5
	C-RA-2	Vulnerabilities in the information system and applications are scanned for periodically.	Detective	Automatic	5
	C-RA-3	Vulnerabilities are remediated in accordance with assessments of risk.	Corrective	Manual	5
SECURITY ASSESSMENT	C-CA-1	The security controls in information systems are periodically assessed to determine if the controls are effective in their application.	Detective	Manual	5
	C-CA-2	Plans of action designed to correct deficiencies are developed and implemented to reduce or eliminate vulnerabilities in information systems.	Corrective	Manual	5
	C-CA-3	Information system security controls are monitored on an ongoing basis to ensure the continued effectiveness of the controls.	Detective	Manual	5
	C-CA-4	Develop, document, periodically update, and implement system security plans for organizational information systems that describe the security requirements in place or planned for the systems.	Detective	Manual	4
	C-SC-1	Organizational communications at the external boundaries and key internal boundaries of the information systems are monitored, controlled and protected.	Preventative	Automatic	4
	C-SC-2	Secure architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems are employed.	Preventative	Manual	5
	C-SC-3	User functionality is separated from information system management functionality (e.g., privileged user functions).	Preventative	Automatic	5
	C-SC-4	Controls to prevent the unauthorized and unintended information transfer via shared system resources is implemented.	Preventative	Automatic	4
	C-SC-5	Subnetworks for publicly accessible system components are implemented that are physically or logically separated from internal networks.	Preventative	Automatic	4
	C-SC-6	Network communications traffic is denied by default and network communications traffic by exception is allowed (e.g., deny all, permit by exception).	Preventative	Automatic	5
	C-SC-7	Dual homing is prevented, where remote devices are prevented from simultaneously establishing non-remote connections and communicating via some other connection to resources in external networks.	Preventative	Automatic	3