Risk Management Tables/Charts/Worksheets

This job aid provides examples of each of the tables, charts and worksheets that are referenced in the courseware and are an integral part of the risk management process. This job aid can be used as quick reference material or as a starting point in your own risk management analysis using the blank worksheets located at the end.

Impact/Risk and Threat/Vulnerability Scales

During the analysis process; values are assigned corresponding to the impact of asset loss, threats, and vulnerabilities, and then a resulting risk value is calculated. (See tables below).

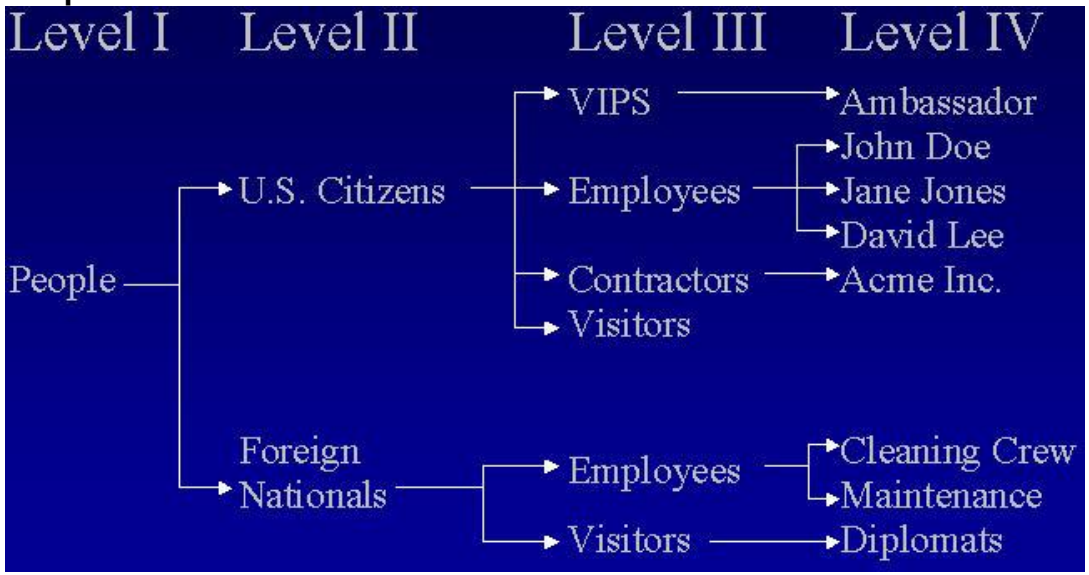
Impact and Risk Scale				
	Low	**Medium**	**High**	**Critical**
Range	0-3	4-13	14-50	51-100
Mid-point	2	8	31	75

Threat and Vulnerability Scale				
Degree of Threat	**Low**	**Medium**	**High**	**Critical**
Range	.01-.24	.25-.49	.50-.74	.75-1.00
Mid-point	.12	.37	.62	.87

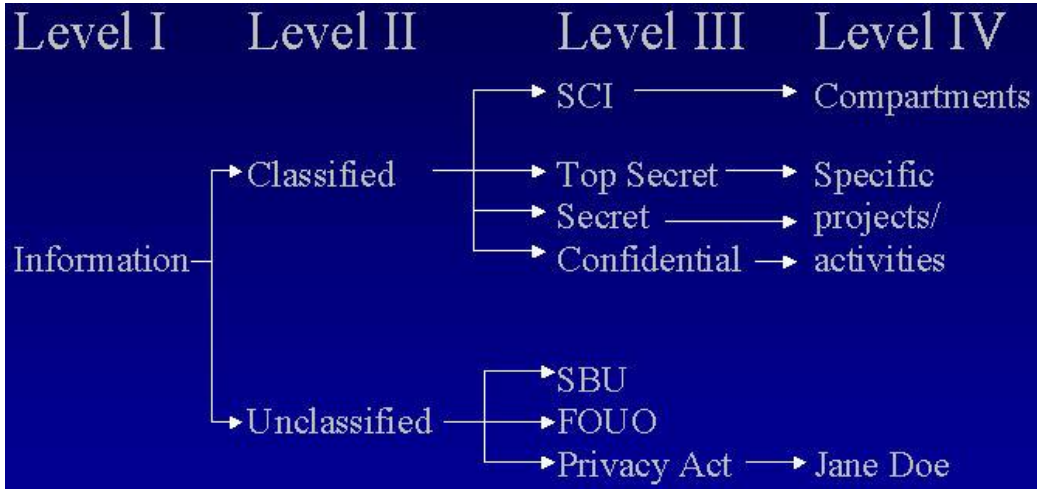
Asset Category Tables

Assets can be assigned to one of five categories: people, information, equipment, facilities, and activities & operations. These can be broken into multiple levels to assist with capturing details about each asset. Each level within the categories is then used during the asset analysis. Asset analysis studies are done at a Level I, II, III, and IV, or deeper as necessary. (See tables below)

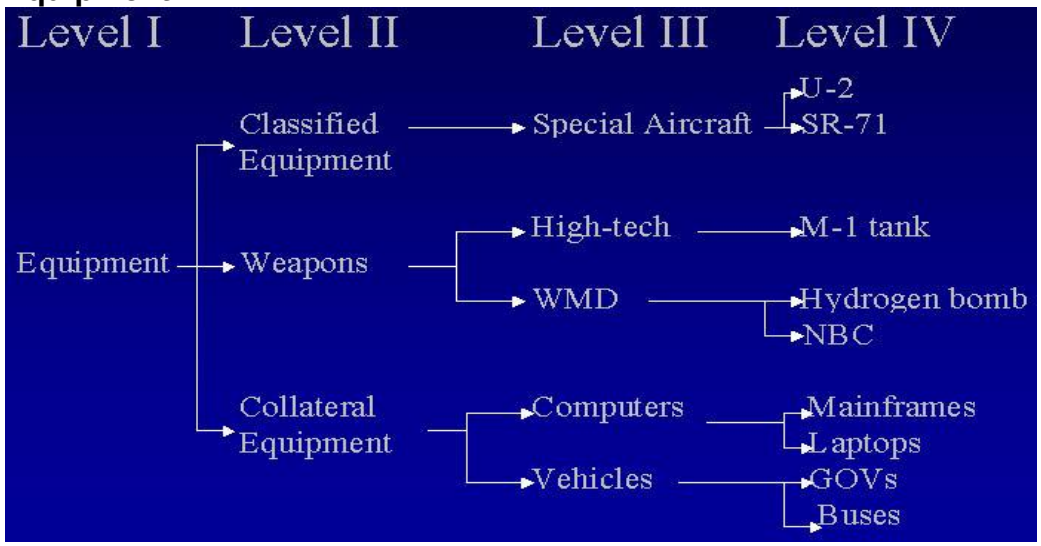
People



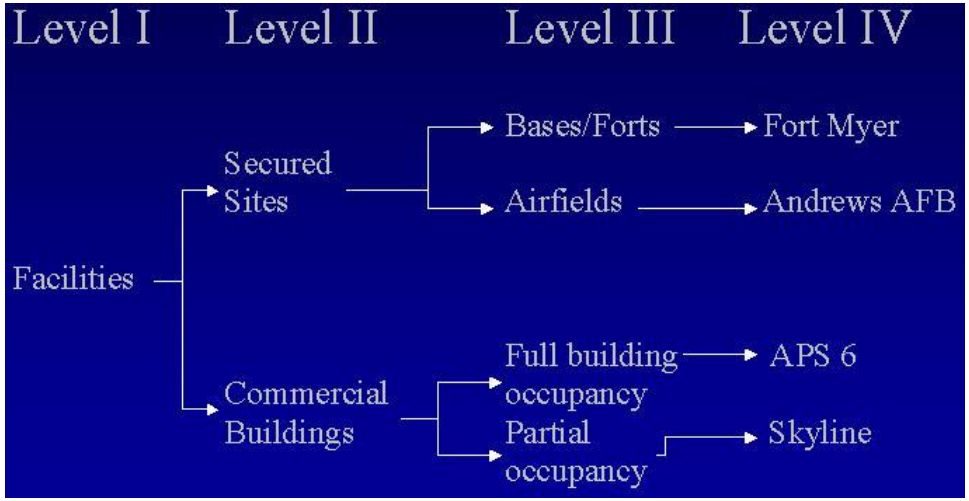
Information



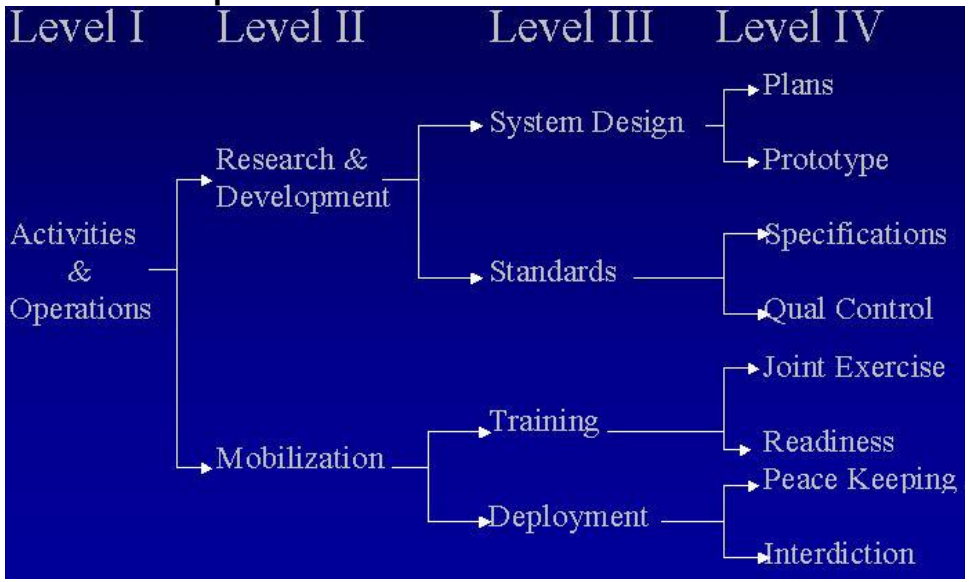
Equipment



Facilities



Activities & Operations



Adversary Categories

Group the identified adversaries into categories to help in the analysis and organization of your assessment. Examples of categories include individuals, groups & organizations and governments. (See tables below)

INDIVIDUALS			
Categories	**Adversaries**	**Goals**	**Strategies**
Common Criminals	• Muggers • Burglars • Petty thieves • Vandals	• Survival • Excitement	• Steal money or valuables for sale • Do destructive, but exciting things
Insiders	• Spies • Saboteurs • Problem employees	• Live better • Exact revenge • Excitement	• Sell secrets • Sabotage equipment • Cause bad public relations • Act violently
Disturbed Individuals	• Assassins • Stalkers • Harmless individuals	• Gain attention • Get relief • Respond to delusions • Suicide	• Harm or kill very important people (VIPs) • Approach VIPs or select organizations to obtain help • Express beliefs/ideas • Commit suicide

GROUPS & ORGANIZATIONS			
Categories	**Adversaries**	**Goals**	**Strategies**
Terrorists	• Hezbollah • HAMAS • Nov. 17th • Others	• Force change • Gain publicity for cause	• Steal money or valuables for sale • Do destructive but exciting things
Corporate Competitors	• Any foreign or domestic competitor	• Capture market share • Gain advantage • Make money	• Gather proprietary info legally • Gather proprietary info illegally • Exploit competitor info
Narco-traffickers	• Cali Cartel • Medellin Cartel • Others	• Continue business • Stay out of jail • Make money	• Intimidate politicians and law enforcement • Co-opt key politicians and law enforcers

GOVERNMENTS			
Categories	**Adversaries**	**Goals**	**Strategies**
Foreign Intelligence Entities	• SVRR • DGI	Multiple	Multiple
Foreign Militaries	• N. Korean Army • Iraqi Rev. Guard • Cuban Brigades • Russian GRU	To further political, economic, military, ethnic or religious agendas as defined by national leaders	• HUMINIT • SIGINT • IMINT • MASINT • OSINT • Other technical collection attacks • Conventional warfare • Information Operations • Terrorism
State-sponsored Entities	• Hezbollah • MITI • Others		

Intent Assessment Chart

Once you have grouped the adversaries, create an Intent Assessment Chart to summarize the data. Use “yes” or “no” responses for knowledge of an asset, need and each adversary’s demonstrated interest level. This is generally the weakest link in the overall risk management process because access to this type of information is often limited.

Based on the number of “yes” responses, assign a high, medium, or low intent level for each adversary. Typically, three “yes” responses equate to a high intent level, two “yes” responses translate to a medium, and one “yes” response indicates a low overall intent level.

Intent Assessment Chart				
Adversary	**Intent**			
Insider, Terrorist, FIE, Criminal	**Knowledge of Asset**	**Need**	**Demonstrated Interest**	**Overall Intent Level**
Adversary 1	Yes	Yes	Yes	High
Adversary 2	Yes	Yes	No	Medium
Adversary 3	Yes	No	No	Low

Collection Capability Assessment Chart

Use the Collection Capability Assessment Chart to record findings when researching an adversary's capabilities. Adversaries may use overt or covert methods/activities to collect information. Some of these may include: SIGINT, HUMINT, IMINT, MASINT and OSINT.

Collection Capability Assessment Chart						
Adversary **Insider, Terrorist, FIE, Criminal**	**Collection Capabilities**					
	HUMINT	**SIGINT**	**IMINT**	**MASINT**	**OSINT**	**Overall Capability Level**
Adversary 1	High	High	Medium	Medium	High	High
Adversary 2	High	Medium	Low	Medium	High	Medium
Adversary 3	Medium	Medium	Low	Low	Medium	Medium

History Assessment Chart

Use the History Assessment Chart to document an adversary's history with regards to suspected, attempted, or successful incidents.

History Assessment Chart			
Adversary **Insider, Terrorist, FIE, Criminal**	**History**		
	Suspected Incidents	**Attempted Incidents**	**Successful Incidents**
Adversary 1	2 technical devices found	2 attempted forced entries	Unknown
Adversary 2	5 alarm activations; adversary sighted in area	2 attempted forced entries	Unknown
Adversary 3	None	None	None

Threat Assessment Summary Chart

Use the Threat Assessment Summary Chart to summarize intent (from Intent Assessment Chart), capability (from Collection Capability Assessment Chart), and history (from History Assessment Chart) and assign an overall threat level rating. The intent and capability columns are populated with high, medium, or low ratings and the history column is populated with a "yes" or "no" response.

Threat Assessment Summary Chart				
Adversary **Insider, Terrorist, FIE, Criminal**	**Intent (Interest/Need)**	**Capability (Methods)**	**History (Incidents/Indicators)**	**Overall Threat Level**
Adversary 1	High	High	Yes	High
Adversary 2	Medium	Medium	Yes	Medium
Adversary 3	Low	Medium	No	Low

Threat Level Decision Matrix

Once the overall threat level is determined, create a second chart, the Threat Level Decision Matrix. Assign "yes" or "no" ratings for each adversary's intent, capability, and history. A threat level is assigned based on the number of "yes" ratings. The greater number of "yes" ratings, the higher the threat level.

For example,

yes + yes + yes = critical,
no + no + no = low.

Threat Level Decision Matrix			
Intent (Interest/Need)	**Capability (Methods)**	**History (Incidents/Indicators)**	**Threat Level**
Yes	Yes	Yes	Critical
Yes	Yes	No	High
Yes	No	Yes/No	Medium
No	Yes	No	Medium
No	No	No	Low

Countermeasure Classification Chart

Countermeasures are classified according to their implementation requirements. Countermeasures can be procedural, involve equipment/devices, and involve personnel.

Countermeasure Classification Chart		
Procedures	**Equipment (Physical/Technical)**	**Manpower**
• Security Policies • Security Procedures • Training • Awareness Programs • Legal Prosecution • Security Investigations • Polygraph • Disclosure Statements • Personnel Transfer • Contingency/Emergency Response Planning • OPSEC Procedures • Cover Procedures	• Locking Mechanism • Window Bars • Doors • Fences • Alarms/Sensors • Hardware/Software • Badges • Lighting • TEMPEST Devices • Paper Shredder • Weapons • Closed-circuit TV • Safe Haven/Vault	• Contractor Guard Force • Special Police Officers • Local Guards • Military Guards

Countermeasure Worksheet

Use the Countermeasure Worksheet to categorize projected vulnerability-reducing countermeasures along with estimated costs.

Countermeasure Worksheet			
Undesirable Events	**Procedures**	**Equipment**	**Manpower**
Surreptitious Entry	Procedures to secure facilities after hours Cost: moderately inconvenient	Doors, locks, bars - $5000 IDS - $20,000	Contractor Guards - $100K SPOs - $250K Military Guards - $250K
Kidnapping an Official	Vary travel route Cost: moderately inconvenient Relocate official - $10000	Doors, locks, bars - $5000 IDS - $20,000 Bullet proof car - $40K Residential: CCTV - $170K	Contractor Guards - $100K SPOs - $250K
Compromised Documents	Security awareness briefing Cost: negligible Strict control procedures Costs: moderately inconvenient	System audit trail - $125K Password/user ID software - $50K	N/A

Countermeasure Effectiveness Table

This table can be used for tracking countermeasure effectiveness against potential threats of undesirable events. A ten-point scale is used to indicate the relative level of effectiveness for each countermeasure with 1 being extremely low and 10 being highly effective.

Countermeasure Effectiveness Table				
Countermeasures	**Surreptitious Entry**	**Kidnapping**	**Documents Stolen**	**Terrorist Attack**
Doors, Locks, Bars	4			
Alarms, Sensors	5			
Contractor Guards	6			
Special Police Officers	9			
Military Guards	9			
Vary Travel Routes		5		
Relocate Official		8		
Residence Locks, Bars		4		
Residence Alarms		5		
Residence Sensors		5		
Bullet-proof Car		4		
Residence CCTV		7		
Security Awareness			7	
Strict Media Controls			6	
System Audit Trail			6	
Passwords			6	
Defensive Driving				4
Vehicle Checks				7

Emergency Procedures				4
Metal Detectors				5
Fences, Barriers				5

Countermeasure Analysis Chart

The Countermeasure Analysis Chart is used to determine appropriate countermeasures for mitigating an asset's vulnerabilities. All the information acquired to this point in the risk management process will be used in conducting a countermeasure analysis.

Countermeasure Analysis Chart						
Undesirable Events (1)	**Existing Risk (2)**	**Related Vulnerability Level & Vulnerability (3)**	**Countermeasure (4)**	**Cost (5)**	**New Vulnerability Level (6)**	**New Risk Level (7)**
Motorcade Attack – assassination of VIP	75.27 (Critical)	.80 – Cars not inspected	Car inspection program	$5,000	.40 (Medium)	37.6 (High)
Information Loss – Mission Failure	46.03 (High)	.65 – Ineffective document control	Document control system	$8,000	.15 (Low)	10.6 (Medium)
Existing Risk =>	**60.7**		**Total Cost = >**	**$13,000**	**New Risk Level =>**	**24.1 (High)**

Risk Formula

The three risk factors are incorporated in the formula below to determine a more precise risk rating:

Risk = Impact x (Threat x Vulnerability) or (R = I [T x V])

"Impact" represents the consequence of the asset loss to the asset owner.

The "Threat x Vulnerability" value represents the probability of the undesirable event occurring.

Risk Assessment Worksheet

Once the impact of an undesirable event is defined, create a worksheet for organizing and later analyzing the information. Columns are completed during each step of the risk management process. (See below for an example of a completed worksheet).

Risk Assessment Worksheet										
Asset	**Undesirable Event/Impact**	**Ling. Value (Impact)**	**Num. Rating (Impact)**	**Threat Category**	**Ling. Value (Threat)**	**Num. Rating (Threat)**	**Vulnerability Category**	**Ling. Value (Vuln)**	**Num. Rating (Vuln)**	**Risk Rating**
People	Motorcade attack -> assassination of VIP	H/C	97	Terrorist	H/C	.97	Cars not inspected	C	.80	75.27
	Criminal activity -> employee kidnapping	L/C	51	Terrorist	L/H	.50				
Information	Loss -> mission failure	H/C	97	FIE/Insider	H/H	.73	Ineffective document control	H	.65	46.03
	Unauthorized release-> capability disclosures	H/M	13	Insider	M/M	.37				
Equipment	Theft->loss of computers	H/H	48	Criminal	L/M	.30	No IDS System	H	.55	7.92
	Implant -> compromise information	L/M	4	FIE	H/H	.70				
Facilities	Mail bomb -> destruction of property	M/H	25	Terrorist	L/M	.25	No patrols at building	M	.35	2.19
	Technical attack -> loss of information	L	3	Terrorist	H/H	.74				
Activities & Operations	Disrupt R&D -> schedule attack	M/M	10	FIE/Insider	L	.12	No backup power supply	M	.40	,48
	Poor OPSEC-> operational disclosure	L/H	15	Militant	M/M	.37				

Sample Asset Assessment Worksheet (Step 1)

Critical Asset	Potential Undesirable Event	Impacts	Impact Rating
Activities/Operations			
Equipment			
Facilities			
Information			
People			

Sample Threat Assessment Worksheet (Step 2)

Critical Asset	Potential Undesirable Event	Threat/ Adversary	Impact Rating
Activities/Operations			
Equipment			
Facilities			
Information			
People			

Sample Risk Assessment Worksheet (Step 4)

Asset	Undesirable Event/Impact	Ling. Value (Impact)	Num. Rating (Impact)	Threat Category	Ling. Value (Threat)	Num. Rating (Threat)	Vulnerability Category	Ling. Value (Vuln)	Num. Rating (Vuln)	Risk Rating
People										
Information										
Equipment										
Facilities										
Activities & Operations										

Sample Cost-Benefit Analysis Worksheet (Step 5)

Undesirable Events	Countermeasures	Risk Level Reduced		Cost	Comments
		From	To		