PREPARE OF ASSESSMENT NIST, ENISA E ITSRM2

Prenderefamiliaritàcon NIST SP 800-30, creandouno schema relazionaletratuttele tabellepresentinella pubblicazione. https://csrc.nist.gov/pubs/sp/800/30/r1/final

TIER1 :ORGANIZZAZIONE TIER 2:PROCESSO AZIENDALE TIER 3: SISTEMA INFORMATIVO

1) IDENTIFICARE SORGENTI DI INFORMAZIONI PER THREAT, VULNERABILITÀE IMPATTIDA UTILIZZARE NELLA VALUTAZIONE DEL RISCHIO (TABELLE D-1, E-1, F-1, H-1, I-1). AD ESEMPIO SVOLGENDO UN RA PER IL TIER 3, IL TIER 3 SI ASPETTA INFORMAZIONI DI LIVELLO TIER 1-2 DA TIER 2 (TIER 1 FORNISCE INFORMAZIONE DIRETTAMENTE A TIER 3 SE NON GIA' FORNITE DA TIER 2) E INFORMAZIONI DA ALTRI TIER 3 TRAMITE PEER SHARING. TIER 3, A SUA VOLTA CONDIVIDERÀ INFORMAZIONI A TIER 1-2 TRAMITE RAR E TIER 3 TRAMITE PEER SHARING

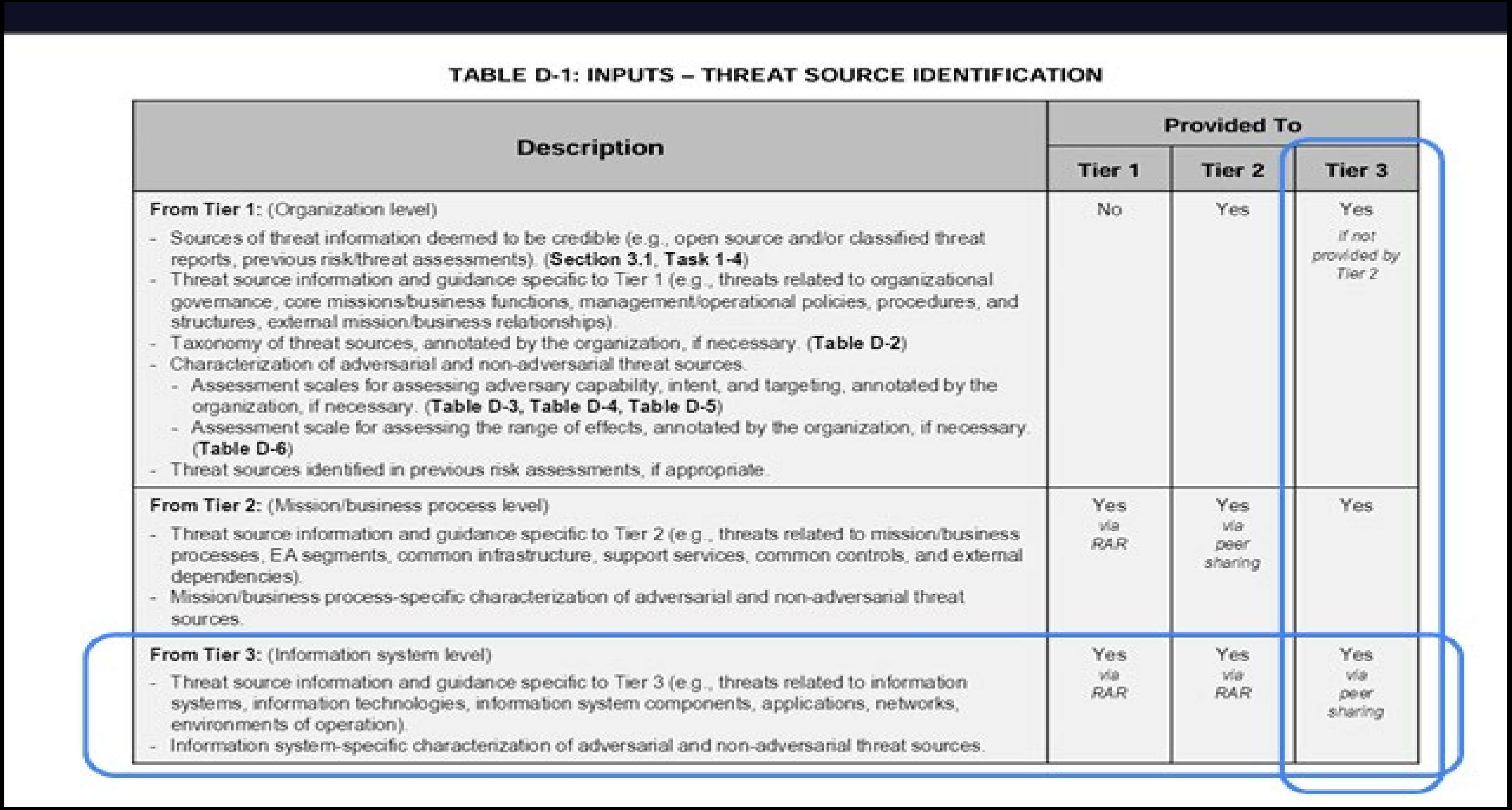
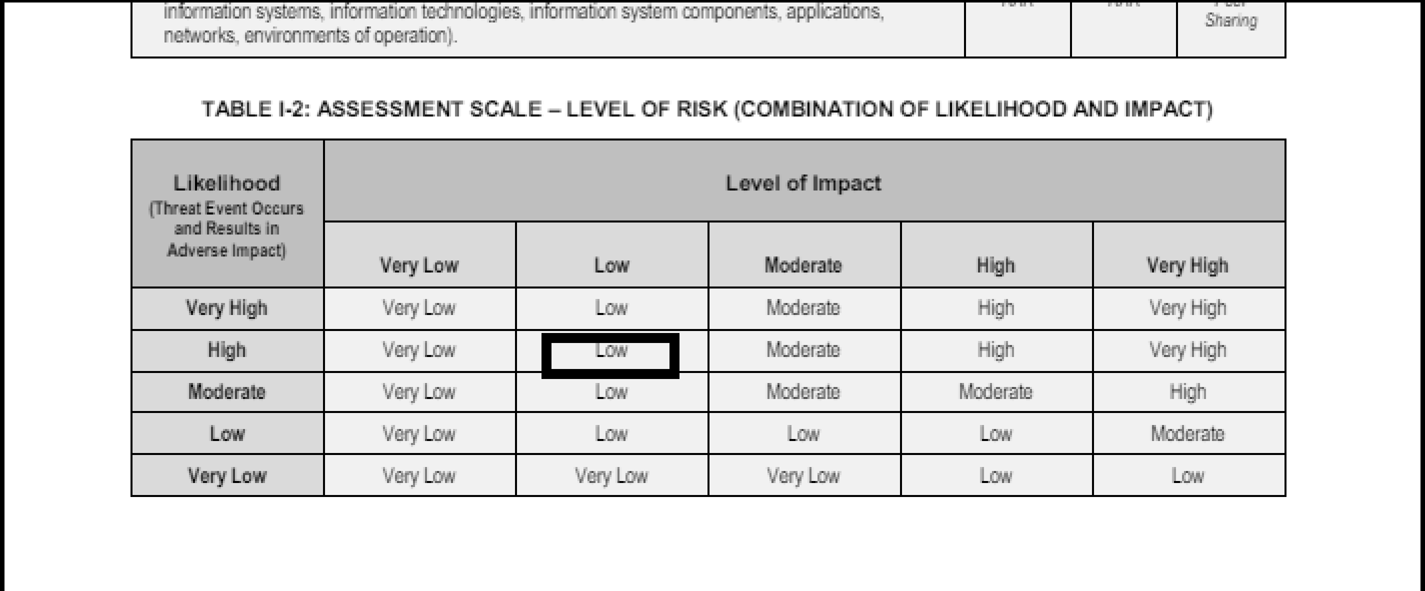


TABLE D-1: INPUTS – THREAT SOURCE IDENTIFICATION

Description	Provided To		
	Tier 1	Tier 2	Tier 3
From Tier 1: (Organization level) - Sources of threat information deemed to be credible (e.g., open source and/or classified threat reports, previous risk/threat assessments). (**Section 3.1, Task 1-4**) - Threat source information and guidance specific to Tier 1 (e.g., threats related to organizational governance, core missions/business functions, management/operational policies, procedures, and structures, external mission/business relationships). - Taxonomy of threat sources, annotated by the organization, if necessary. (**Table D-2**) - Characterization of adversarial and non-adversarial threat sources. - Assessment scales for assessing adversary capability, intent, and targeting, annotated by the organization, if necessary. (**Table D-3, Table D-4, Table D-5**) - Assessment scale for assessing the range of effects, annotated by the organization, if necessary. (**Table D-6**) - Threat sources identified in previous risk assessments, if appropriate.	No	Yes	Yes *if not provided by Tier 2*
From Tier 2: (Mission/business process level) - Threat source information and guidance specific to Tier 2 (e.g., threats related to mission/business processes, EA segments, common infrastructure, support services, common controls, and external dependencies). - Mission/business process-specific characterization of adversarial and non-adversarial threat sources.	Yes *via RAR*	Yes *via peer sharing*	Yes
From Tier 3: (Information system level) - Threat source information and guidance specific to Tier 3 (e.g., threats related to information systems, information technologies, information system components, applications, networks, environments of operation). - Information system-specific characterization of adversarial and non-adversarial threat sources.	Yes *via RAR*	Yes *via RAR*	Yes *via peer sharing*

NELLA TABELLA I-2 SONO ANDATO A SELEZIONARE IL LIVELLO DI RISCHIO NEL LIVELLO DI LIKELIHOOD (HIGH E LEVEL IMPACT LOW) RIFERENDOMI ALLA TABELLA NELLA SLIDE PRECENDE RELATIVA AL TIER 3 PROCESSO INFORMATICO



information systems, information technologies, information system components, applications, networks, environments of operation).			Sharing

TABLE I-2: ASSESSMENT SCALE – LEVEL OF RISK (COMBINATION OF LIKELIHOOD AND IMPACT)

Likelihood (Threat Event Occurs and Results in Adverse Impact)	Level of Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

DOPO AVER DETERMINATO IL RISCHI DI ENTRAMBE LE TABELLE ANDIAMO A RIPORTA SU QUELLA FINALE (I-5)

- Determinare il metodoappropriato (ad esempio, briefing esecutivo, rapporto di valutazione del rischio o dashboard) per comunicare i risultati della valutazione del rischio. • Comunicare i risultatidel risk assessment agli stakeholder organizzativi designati. • Condividere i risultati del risk assessmente le evidenzea supporto in conformità con le politiche e le linee guida dell'organizzazione

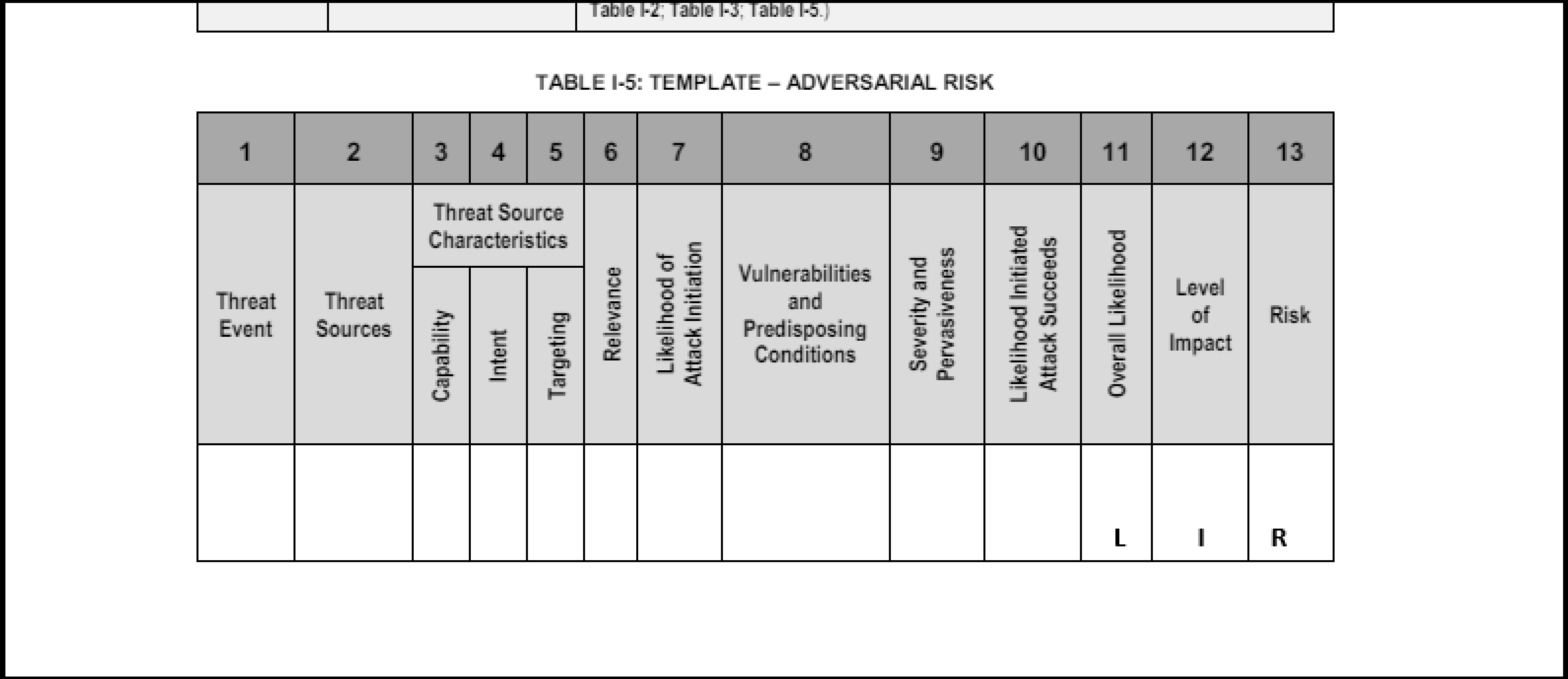


Table I-2; Table I-3; Table I-5.)

TABLE I-5: TEMPLATE – ADVERSARIAL RISK

1	2	3	4	5	6	7	8	9	10	11	12	13
Threat Event	Threat Sources	Threat Source Characteristics			Relevance	Likelihood of Attack Initiation	Vulnerabilities and Predisposing Conditions	Severity and Pervasiveness	Likelihood Initiated Attack Succeeds	Overall Likelihood	Level of Impact	Risk
		Capability	Intent	Targeting								
										L	I	R