ISO/IEC 13335-2 - Annex D List of possible threat types (informative)

The following list gives examples of typical threats. The list can be used during the threat assessment process. Threats can be caused by one or more of deliberate, accidental or environmental (natural) events. The following list indicates for each threat type where D (deliberate), A (accidental), E (environmental) are relevant. D is used for all deliberate actions aimed at ICT assets, A is used for all human actions which accidentally can damage ICT assets, E is used for all incidents which are not based on human actions. The threats shown as .A., .D. and/or .E. are not in priority order, and are therefore listed alphabetically.

TREAT	Accidental	Deliberate	Environmental
Earthquake			E
Flooding	A	D	E
Hurricane			E
Lightning			E
Industrial Action	A	D	
Bomb attack	A	D	
Use of arms	A	D	
Fire	A	D	
Willful Damage		D	
Failure of power supply	A	D	E
Failure of water supply	A	D	E
Air conditioning failure	A	D	E
Hardware failures	A		
Power fluctuation	A		E
Extremes of temperature and humidity	A	D	E
Dust			E
Electromagnetic radiation	A	D	E
Electrostatic charging			E
Theft		D	
Unauthorized use of storage media		D	
Deterioration of storage media			E
Operational staff error	A	D	
Maintenance error	A	D	
Software Failure	A	D	
Use of software by unauthorized users	A	D	
Use of software in an unauthorized way	A	D	
Masquerading of user identity		D	
Illegal use of software	A	D	
Malicious software	A	D	
Illegal import/export of software	A	D	
Network access by unauthorized users		D	
Use of network facilities in an unauthorized way		D	
Technical failure of network components	A		
Transmission errors	A		
Damage to lines	A	D	
Traffic overloading	A	D	
Eavesdropping		D	
Communications infiltration		D	
Traffic analysis		D	
Misrouting of messages	A		
Rerouting of messages		D	
Repudiation		D	
Failure of communications services (i.e. network services)	A	D	
Staff shortage	A	D	
User errors	A	D	
Misuse of resources	A	D	

ACIB – Afhankelijkheids – en kwetsbaarheidsanalyse / overzicht dreigingen

MENSEN	wegvallen	• voorzienbaar (ontslag, vakantie) • onvoorzienbaar (ziekte, ongeval, staking)
	onopzettelijke foutieve handelingen	• onkunde, slordigheid, stress • foutieve procedures • complexe foutgevoelige bediening • onzorgvuldige omgang met passwords
	opzettelijke foutieve handelingen	• niet in acht nemen voorschriften • fraude of diefstal op eigen initiatief of onder druk van derden • ongeautoriseerde toegang
APPARATUUR	spontaan technisch falen	• veroudering of slijtage • storing • ontwerp-, fabricage-, installatie- of onderhoudsfouten
	technisch falen door externe invloeden	• spanningsschommelingen • te hoge/lage temperatuur of vochtigheid • vuil, stof • elektromagnetische straling • elektrostatische lading
	menselijk handelen	• bedieningsfouten • opzettelijke functieverandering of –toevoeging • beschadiging of vernieling • diefstal • ontbrekende toebehoren
PROGRAMMATUUR	programmatuurfouten	• ontwerp-, programmeer-, implementatie-, onderhoudsfouten • manipulatie voor of na ingebruikname
	programmatuurgebruik	• opzettelijke introductie van virus, e.d. • opzettelijke introductie van virus, e.d., door gebruik van ongescreende programma's • illegaal kopiëren van programmatuur • diefstal of privé-gebruik van programmatuur
GEGEVENS	via gegevensdragers	• diefstal of zoekraken • beschadiging door vuur, water, vochtigheid, ontmagnetisering, verkeerde behandeling • incompatibele formats • foutieve ver- of ontsleuteling • foutieve of vervalste identificatie
	via apparatuur	• fysieke schrijf- of leesfouten • fouten interne geheugens
	via programmatuur	• foutieve of gemanipuleerde programmatuur • doorwerking van virussen • afbreken van verwerking
	via personen	• foutieve gegevensinvoer, -verandering of –verwijdering (wel/niet opzettelijk, wel/niet bevoegd personeel) • illegaal kopiëren van gegevens • meelezen zichtbare invoer en uitvoer (printer, beeldscherm) • uitlezen elektromagnetische straling • onzorgvuldige vernietiging • foutieve bediening

ACIB – Afhankelijkheids – en kwetsbaarheidsanalyse / overzicht dreigingen

OMGEVING	buitengebeuren	• natuurgeweld (overstroming, blikseminslag, storm, aardbeving, etc.) • overig geweld (oorlog, terrorisme, brandstichting, inbraak, neerstortend vliegtuig) • rest (blokkade, staking)
	nutsvoorzieningen	• uitval van elektriciteit, water, telefoon • wateroverlast door lekkage, bluswater • uitval van licht-, klimaat-, sprinklerinstallatie
	huisvesting	• brand, trilling, ontploffingen • gebreken in ruimtes, inbraakgevoeligheid • belending • locatie
ORGANISATIE	gebruikersorganisatie	• mismanagement • gebrekkige toedeling van taken, bevoegdheden, verantwoordelijkheden • geen werkprocedures/gedragscodes • geen handboeken, systeemdocumentatie, gebruikinstructies • geen interne controle • geen toetsing op naleving richtlijnen • geen input validatie (gegevensuitwisselingsovereenkomst) • geen contractbeheer, DAP's, SLA's • geen kwaliteitsborging • gebrekkige capaciteitsverwerving/-benutting • gebrekkige doel/middelen beheersing

	beheersorganisatie	• gebrekkig beleid rond systeembeheer
		• geen kwaliteitsborging
		• wanbeheer, slordigheden in beheersactiviteiten
		  • release management
		  • configuratiemanagement
		  • change management
		  • problem management
		  • onderhoudsmanagement
		• geen inspecties

	systeemontwikkelings-organisatie	• geen projectmanagement • geen ontwikkelrichtlijnen/-procedures • geen methoden/technieken • geen ontwikkeltools

CRAMM versie 5 - Threats

In de bijlage F van de user manual van CRAMM versie 5 (Dutch) zijn de 'threats' opgenomen gekoppeld aan asset groups en impact. Onderstaand volgt het overzicht van de threats.

Threats
Masquerading of User Identity by Insiders
Masquerading of User Identity by Contracted Service Providers
Masquerading of User Identity by Outsiders
Unauthorised Use of an Application
Introduction of Damaging or Disruptive Software
Misuse of System Resources
Communications Infiltration
Communications Interception
Communications Manipulation
Repudiation
Communications Failure
Embedding of Malicious Code
Accidental Mis-Routing
Technical Failure of Host
Technical Failure of Workstation
Technical Failure of Storage Device
Technical Failure of Print Facilities
Technical Failure of Network Distribution Component
Technical Failure of Network Management / Service Host
Technical Failure of Network Interface
Technical Failure of Network Services
Power Failure
Air Conditioning Failure
System or Network Software Failure
Application Software Failure
Operations Error
Hardware Maintenance Error
Software Maintenance Error
User Error
Fire
Water Damage
Natural Disaster
Staff Shortage
Theft by Insiders
Theft by Outsiders
Wilful Damage by Insiders
Wilful Damage by Outsiders
Terrorism

Nabrander

CRAMM onderkent de volgende impacts. Volledigheidshalve zijn deze hieronder opgenomen. Doel hiervan is om aan te geven hoe ‘immature’ het vakgebied is. Het hiervoor aangehaalde ISO-dcument noemt bijvoordeel ‘mis-routing’ een dreiging.

AFKORTING	IMPACT
P	Physical destruction
15 M	Unavailability - 15 minutes
1 Hr	Unavailability - 1 hour
3 Hr	Unavailability - 3 hours
12 Hr	Unavailability - 12 hours
1 Dy	Unavailability - 1 day
2 Dy	Unavailability - 2 days
1 W	Unavailability - 1 week
2 W	Unavailability - 2 weeks
1 M	Unavailability - 1 month
2 M	Unavailability - 2 months
B	Loss of data since last back-up
T	Total loss of all data
I	Unauthorised disclosure to insiders
C	Unauthorised disclosure to contracted third parties
O	Unauthorised disclosure to outsiders
S E/T	Small-scale errors (for example, keying errors)/small-scale errors in transmission
W E/T	Widespread errors (for example, programming errors)/widespread errors in transmission
D S/T	Deliberate modification of stored data/deliberate modification of data in transit
Or	Repudiation of origin
Rc	Repudiation of receipt
Nd	Non-delivery
Rp	Replay
Mr	Mis-routing
Tm	Traffic monitoring
Os	Out-of-sequence
In	Insertion of false message