NETWORK SURVIVABILITY ASSESSMENT METHODOLOGY

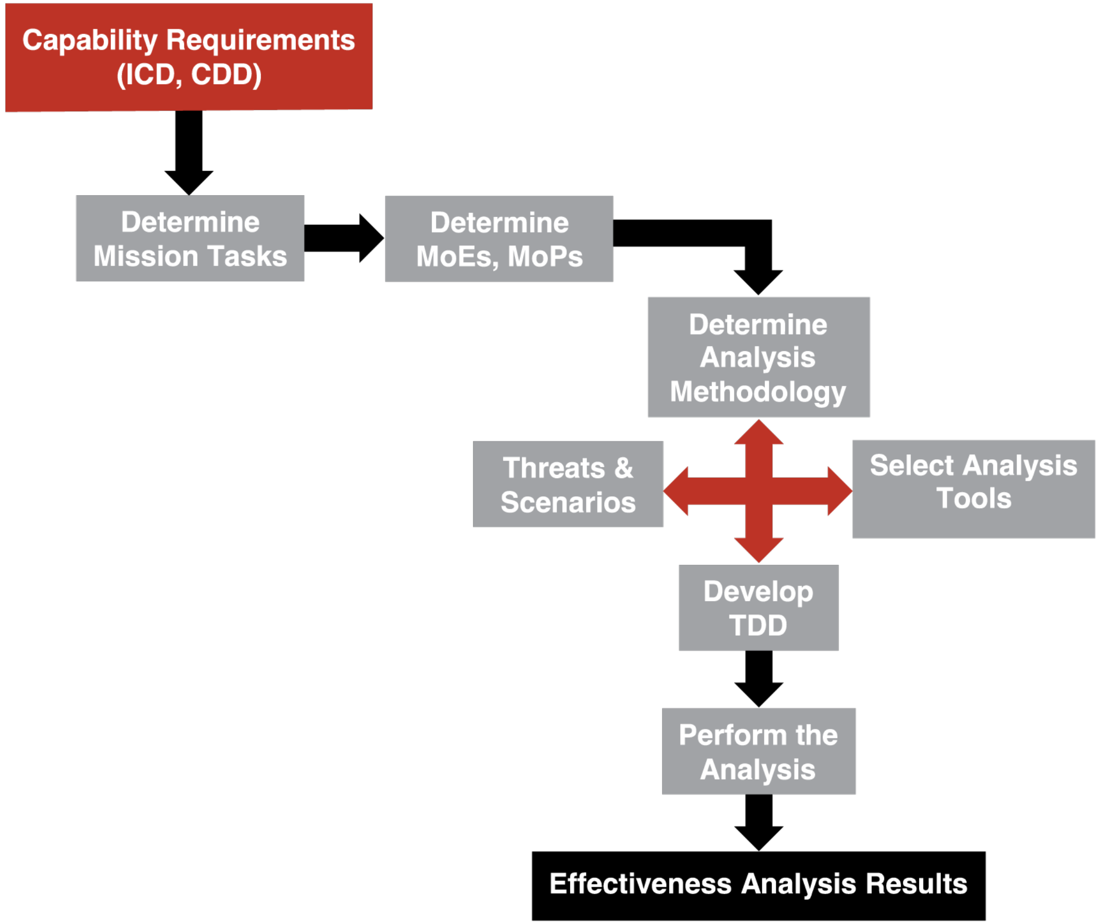
Philip Payne

Cybersecurity & Information Systems Information Analysis Center

Process Outline

1. Identify/Define Mission Sets
2. Identify Key Technologies (KTs)
3. Define Measures of Effectiveness for KTs
4. Identify Threats for each KT
5. Categorize Threats for each KT
   - STRIDE Methodology
6. Compute Risk Score Based on Measures of Effectiveness (MoEs) for each Threat
   - Risk Score = Impact × Likelihood
   - DREAD Methodology
7. Prioritize Threats Based on Mission Sets

Effectiveness Analysis Process



Capability Requirements (ICD, CDD)

Determine Mission Tasks

Determine MoEs, MoPs

Determine Analysis Methodology

Threats & Scenarios

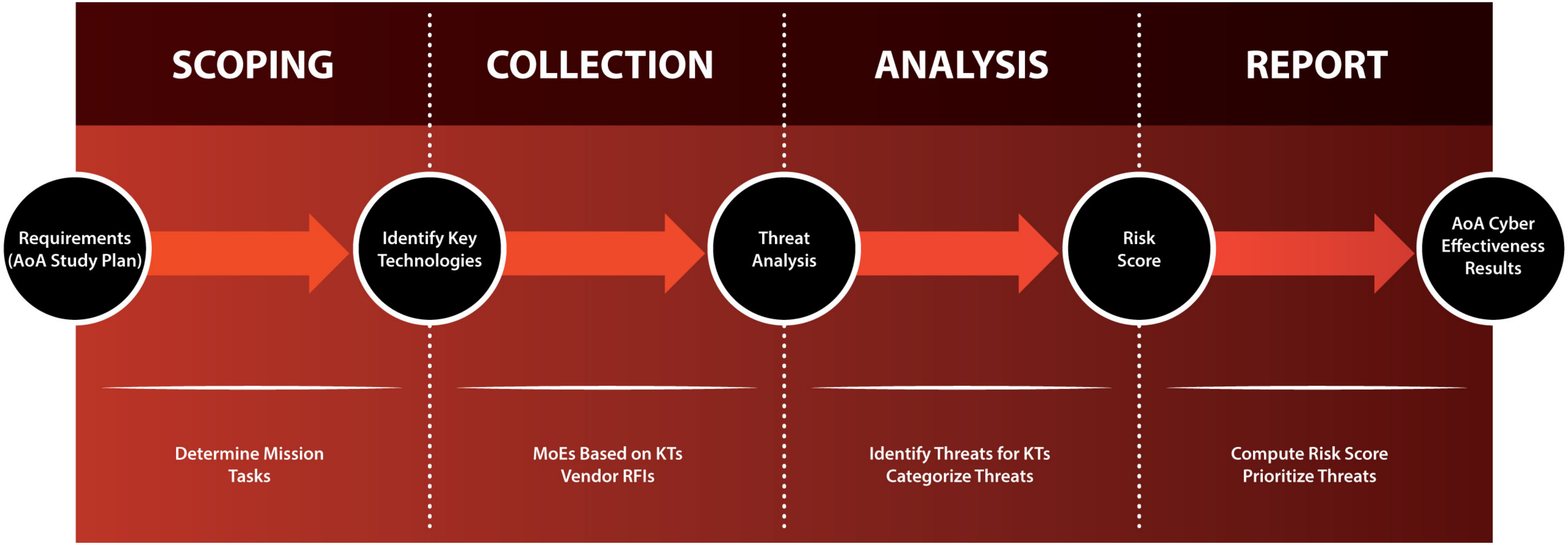
Select Analysis Tools

Develop TDD

Perform the Analysis

Effectiveness Analysis Results

Network Survivability Analysis Process



SCOPING

COLLECTION

ANALYSIS

REPORT

Requirements (AoA Study Plan)

Identify Key Technologies

Threat Analysis

Risk Score

AoA Cyber Effectiveness Results

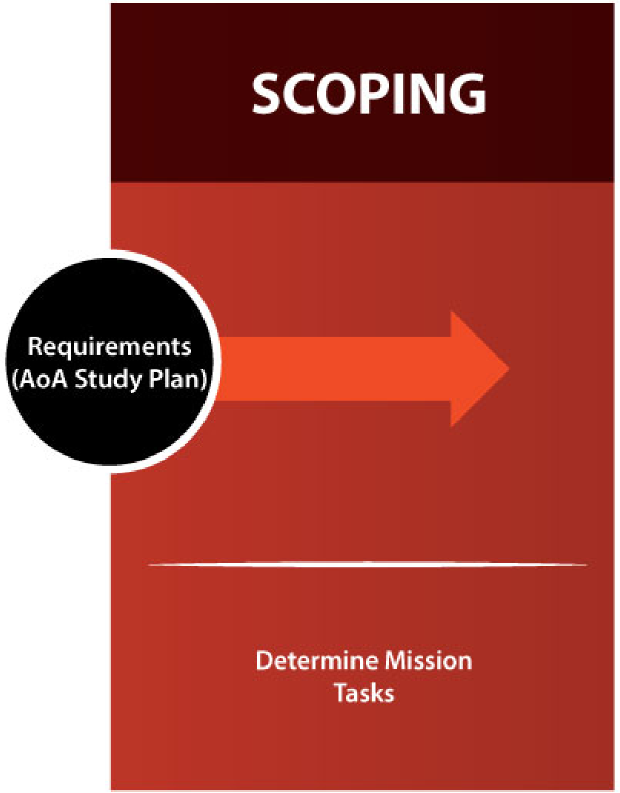
Determine Mission Tasks

MoEs Based on KTs
Vendor RFIs

Identify Threats for KTs
Categorize Threats

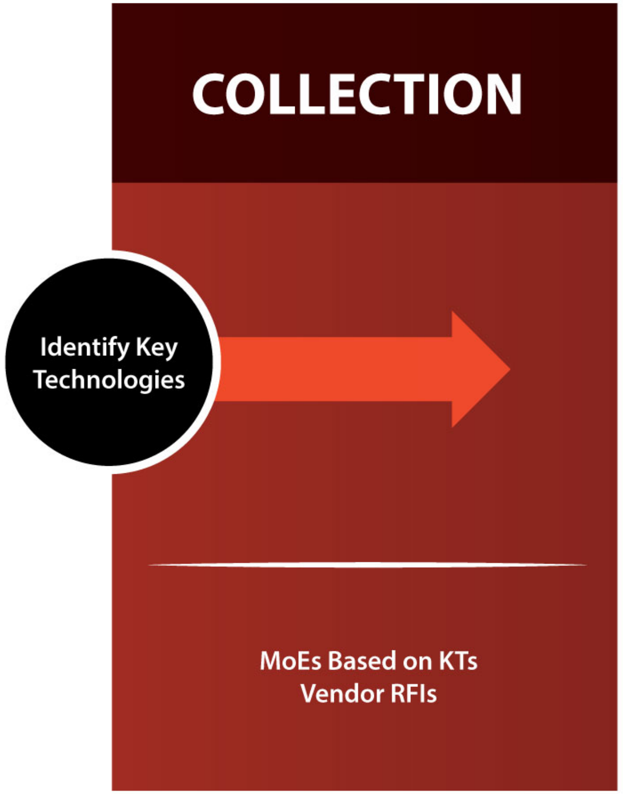
Compute Risk Score
Prioritize Threats

Network Survivability Scoping Process



The Network Survivability Assessment Scoping Process consists of examining the Analysis of Alternatives (AoA) study plan to identify the cybersecurity requirements (if any), the overall mission task, as well as generic effectiveness measures by which we can define cyber measures of effectiveness.

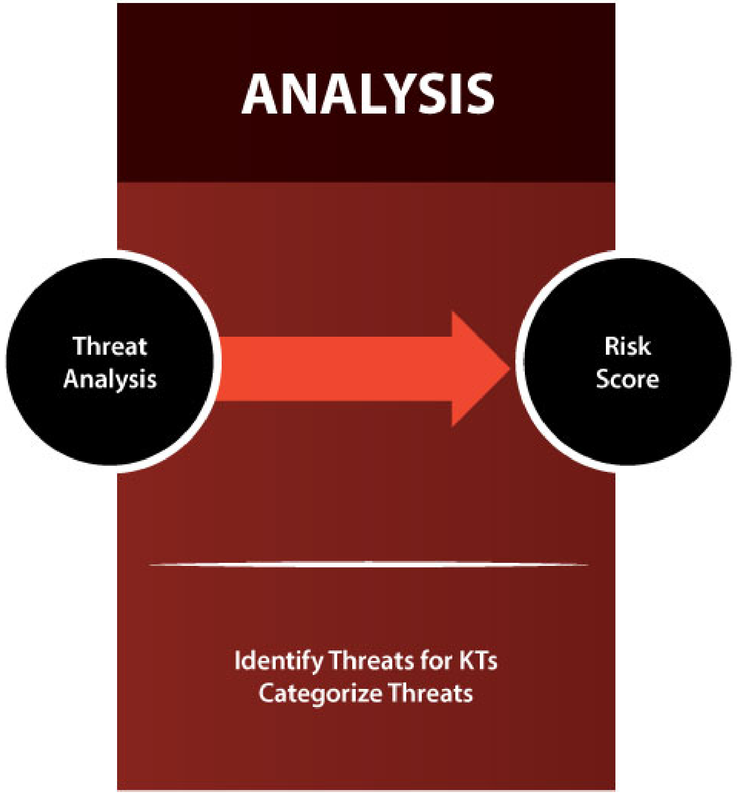
Network Survivability Collection Process



The Network Survivability Assessment Collection Process begins with an identification of the key technologies required to perform each mission task or function. Once identified, the cyber measures of effectiveness (based on confidentiality, integrity, availability, authentication, and nonrepudiation) are defined. Vendor requests for information (RFIs) are subsequently distributed based on MoEs.

Network Survivability Analysis Process

The Network Survivability Assessment Analysis Process seeks to identify and categorize cyber threats to the key technologies previously identified. We leverage the STRIDE methodology to categorize the threats based on the type of potential attack (e.g., spoofing or denial of service). Risk scoring is performed by conducting a DREAD analysis.



Network Survivability Analysis Process

The Network Survivability Assessment Reporting Process aggregates the results into a tabular format where the MoEs are evaluated for each alternative. The risk scores are presented from the previous phase in a color-coded format based on the level of risk to the mission tasks.

REPORT

AoA Cyber Effectiveness Results

Compute Risk Score
Prioritize Threats

Network Survivability Assessment Resulting Table

	MT 1			MT 2			MT 3		
	MoE 1-1	MoE 1-2	MoE 1-3	MoE 2-1	MoE 2-2	MoE 2-3	MoE 3-1	MoE 3-2	MoE 3-3
Alternative 1	🟥	🟩	🟥	🟨	🟥	🟩	🟥	🟨	🟥
Alternative 2	🟩	🟩	🟨	🟩	🟥	🟩	🟨	🟩	🟨
Alternative 3	🟩	🟩	🟩	🟩	🟨	🟩	🟨	🟩	🟩

The Network Survivability Assessment Resulting Table is an aggregation of all cyber-based results produced for an AoA, with N number of alternatives to evaluate. It provides a summary of the overall risk(s) associated with the selection of a particular alternative.

SAMPLE ANALYSIS (ENTERPRISE ANTI-VIRUS SOFTWARE)

Scoping

Requirement(s)

Perform cyber risk assessment of anti-virus (AV) software running on Defense Information Systems Agency (DISA) enterprise information systems to aid in the selection of AV software

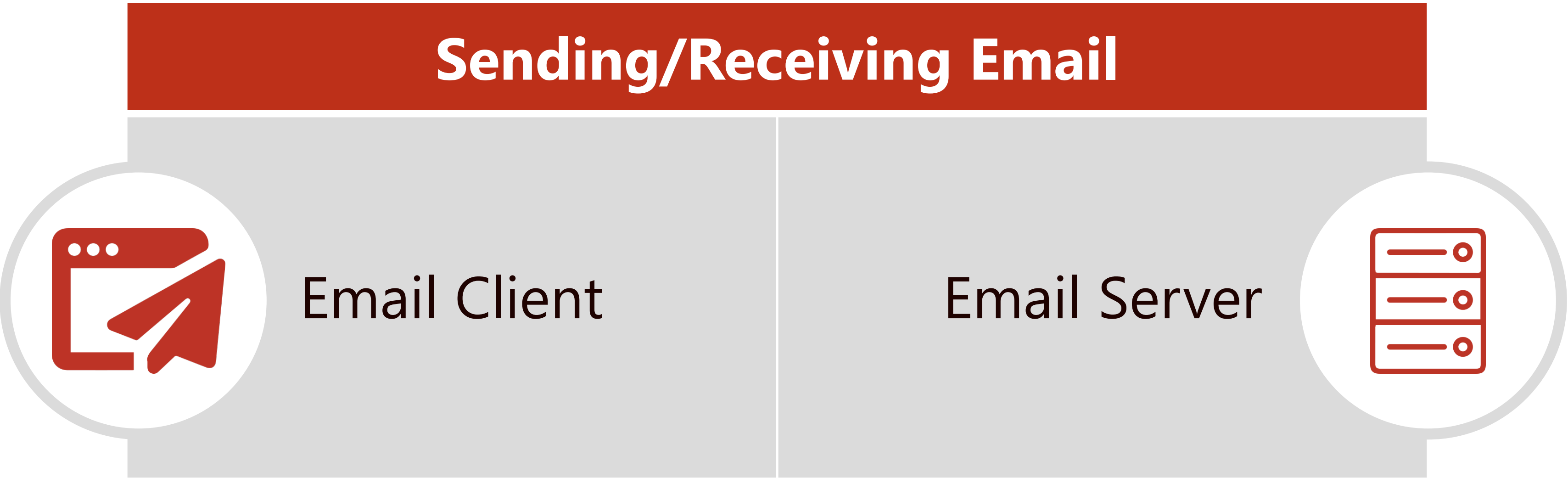
Mission Tasks

Sending/ receiving email

Overall Question

What security features does AV provide when sending/receiving email?

Identify Software-Based KTs



Sending/Receiving Email

Email Client

Email Server

Define Measures of Effectiveness for Sending/Receiving Email KTs

Key Technology	Outgoing Email Protection	Inbound Email Protection	Anti-phishing	Email Attachments
Email client	Scans outgoing email for viruses (1-1)	Scans incoming email for viruses (1-2)	Scans incoming email for phishing characteristics (1-3)	Scans outgoing attachments for viruses (1-4)
Email server	Scans outgoing email for viruses (2-1)	Scans incoming email for viruses (2-2)	Scans incoming/outgoing email for phishing characteristics (2-3)	Scans incoming/outgoing attachments for viruses (2-4)

Vendor RFI

SOFTWARE SPECIFICATIONS

- AV (Initial) Policy
- AV Configuration
- AV Signature Database
- AV Scanning Documentation *(AV email scanning)*
- AV Update Process

Identify Threats for KTs

Mission: Sending/Receiving Email				
Key Technology	**Outgoing Email Protection**	**Inbound Email Protection**	**Anti-Phishing**	**Email Attachments**
Email client	Scans outgoing email for viruses	Scans incoming email for viruses	Scans incoming email for phishing characteristics	Scans outgoing attachments for viruses
Threats	Email-based virus	Email-based virus	Phishing mail	Attachment virus
Email server	Scans outgoing email for viruses	Scans incoming email for viruses	Scans incoming/outgoing email for phishing characteristics	Scans incoming/outgoing attachments for viruses
Threats	Email-based virus	Email-based virus	Phishing email	Attachment virus

Categorize Threats Based on KTs

MoE	Threats	Spoofing Identity	Tampering With Data	Repudiation	Information Disclosure	Denial of Service	Privilege Escalation
1-1	Email-based virus (client outgoing)	X	X	X	X	X	X
1-2	Email-based virus (client incoming)	X	X	X	X	X	X
2-1	Email-based virus (server outgoing)	X	X	X	X	X	X
2-2	Email-based virus (server incoming)	X	X	X	X	X	X
1-3	Phishing email (client)	X	X	X	X	X	
2-3	Phishing email (server)	X	X	X	X	X	
1-4	Attachment virus (client)		X		X	X	
2-4	Attachment virus (server)		X		X	X	

*Notional Example Only

Risk Score for Each Threat

MoE	Threats	Damage Potential	Reproducibility	Exploitability	Affected Users	Discoverability	Risk DREAD
1-1	Email-based virus (client outgoing)	5	8	6	5	7	6.2
1-2	Email-based virus (client incoming)	5	8	6	5	7	6.2
2-1	Email-based virus (server outgoing)	5	8	6	10	7	7.2
2-2	Email-based virus (server incoming)	5	8	6	10	7	7.2
1-3	Phishing email (client)	5	10	10	5	2	6.4
2-3	Phishing email (server)	5	10	10	10	2	7.4
1-4	Attachment virus (client)	5	4	2	5	3	3.8
2-4	Attachment virus (server)	5	4	2	10	4	5

Key

High (7-10) Med (4-7) Low (1-3)

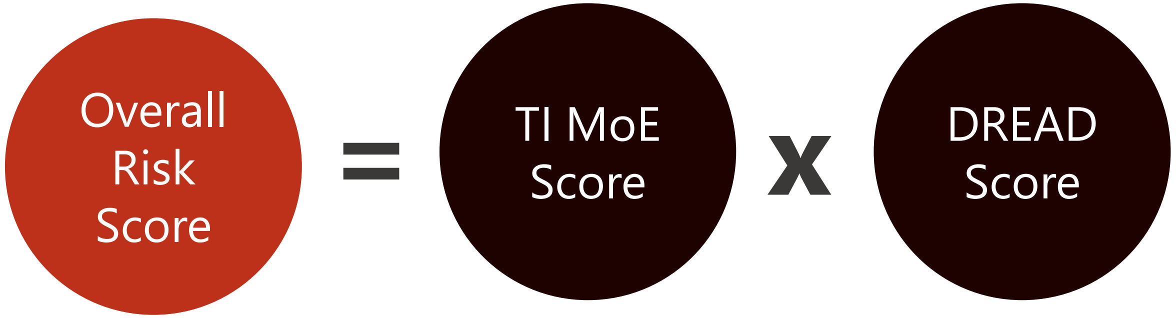
*Notional Example Only

Compute Risk Score

TECHNICAL IMPLEMENTATION (TI) SCORING

An analysis of the mechanism(s) of a KT meeting an MoE *(in the context of a threat)*

- **Substantially Implemented = 1**
  (e.g., all email scanned, blocks >75% of known viruses)
- **Minimally Implemented = 2**
  (e.g., some email scanned, blocks >25% of known viruses)
- **Insufficiently Implemented (or Not Implemented) = 3**
  (e.g., no email scanned, blocks <25% of known viruses)



Overall Risk Score = TI MoE Score x DREAD Score

Network Survivability Assessment Resulting Table

Alternatives	Sending/Receiving Email (Client)				Sending/Receiving Email (Server)			
	MoE 1-1	MoE 1-2	MoE 1-3	MoE 1-4	MoE 2-1	MoE 2-2	MoE 2-3	MoE 2-4
ALT #1	🟩	🟩	🟨	🟨	🟩	🟩	🟨	🟨
ALT #2	🟩	🟩	🟩	🟨	🟩	🟩	🟩	🟨
ALT #3	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
ALT #4	🟥	🟥	🟨	🟥	🟥	🟥	🟨	🟥
ALT #5	🟩	🟩	🟨	🟥	🟩	🟩	🟨	🟥

Key

🟥 High (20-30)	🟨 Med (10-19)	🟩 Low (0-9)

*Notional Example Only

References

AoA Handbook

(Practical Guide to AoAs – Office of Aerospace Studies)

Qualitative Risk Analysis With DREAD Model

http://resources.infosecinstitute.com/qualitative-risk-analysis-dread-model/#gref

The STRIDE Threat Model

https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx