Crown Jewels Analysis (CJA): Criticality Analysis

Helping Healthcare Address the Threat of Ransomware

Joanne R. Fitzpatrick

3 Feb 2021

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

CJA at a Glance

Crown Jewels Analysis (CJA) *is a MITRE-developed methodology for criticality analysis.*

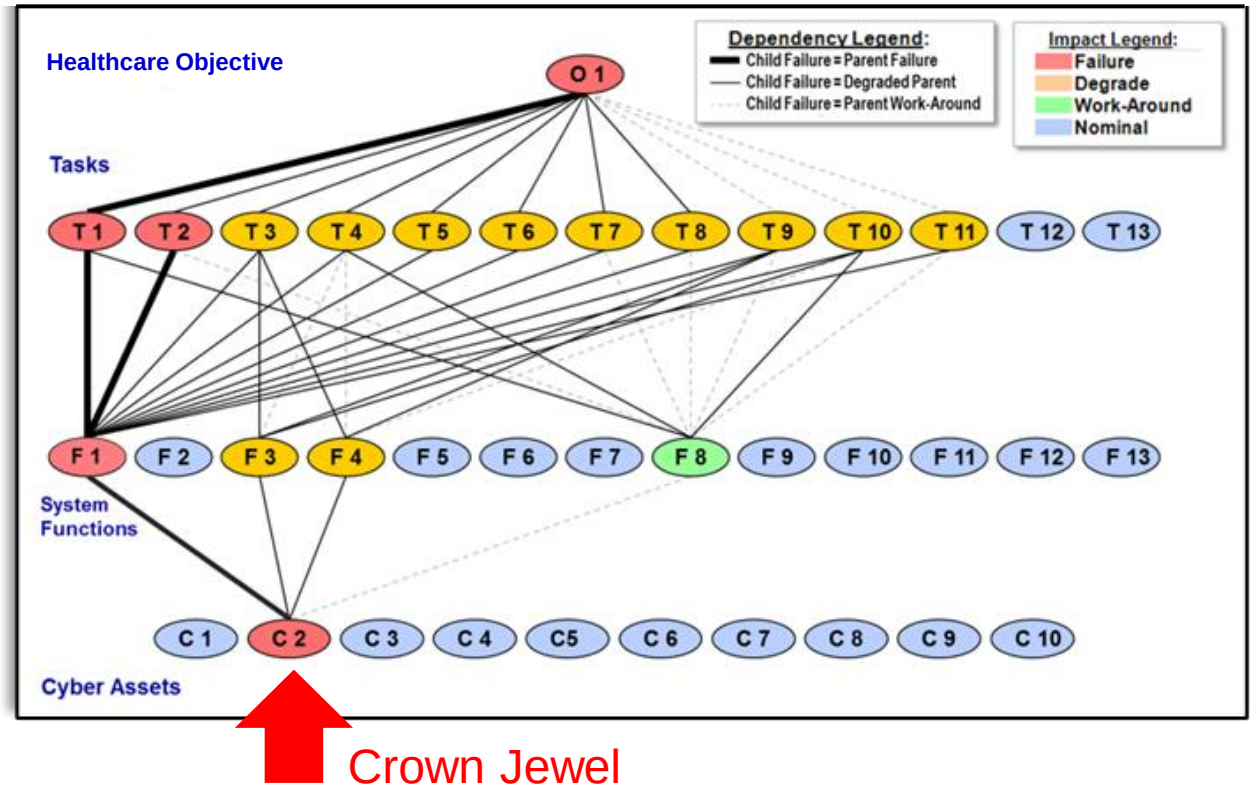
- Identifies an organization's **crown jewels,** those cyber assets most critical to accomplishment of organization's highest objectives.
- Allows healthcare organization to prioritize cyber assets and apply limited resources effectively for **cyber resiliency,** the ability to operate during a major cyber attack, such as ransomware, and still deliver highest objectives in some capacity
- Asks senior management to confirm and prioritize healthcare and organization objectives
- Should be done as part of Risk Management Plan
- Combines expert input from healthcare SMEs with established, analytical techniques applied from engineering fields. CJA in active use for over 12 years with sponsors of all sizes serving in the public trust

Understanding Crown Jewels

CJA identifies an organization's Crown Jewels

- Cyber assets (hardware, software, data) *whose failure, or failure to operate or be accessed as intended,* causes failure of an organization's major objective, e.g., deliver healthcare services
- Are ***most*** critical to the accomplishment of an organization's objectives
- Many are already known by organizations. CJA confirms those known and reveals hidden, unexpected ones.

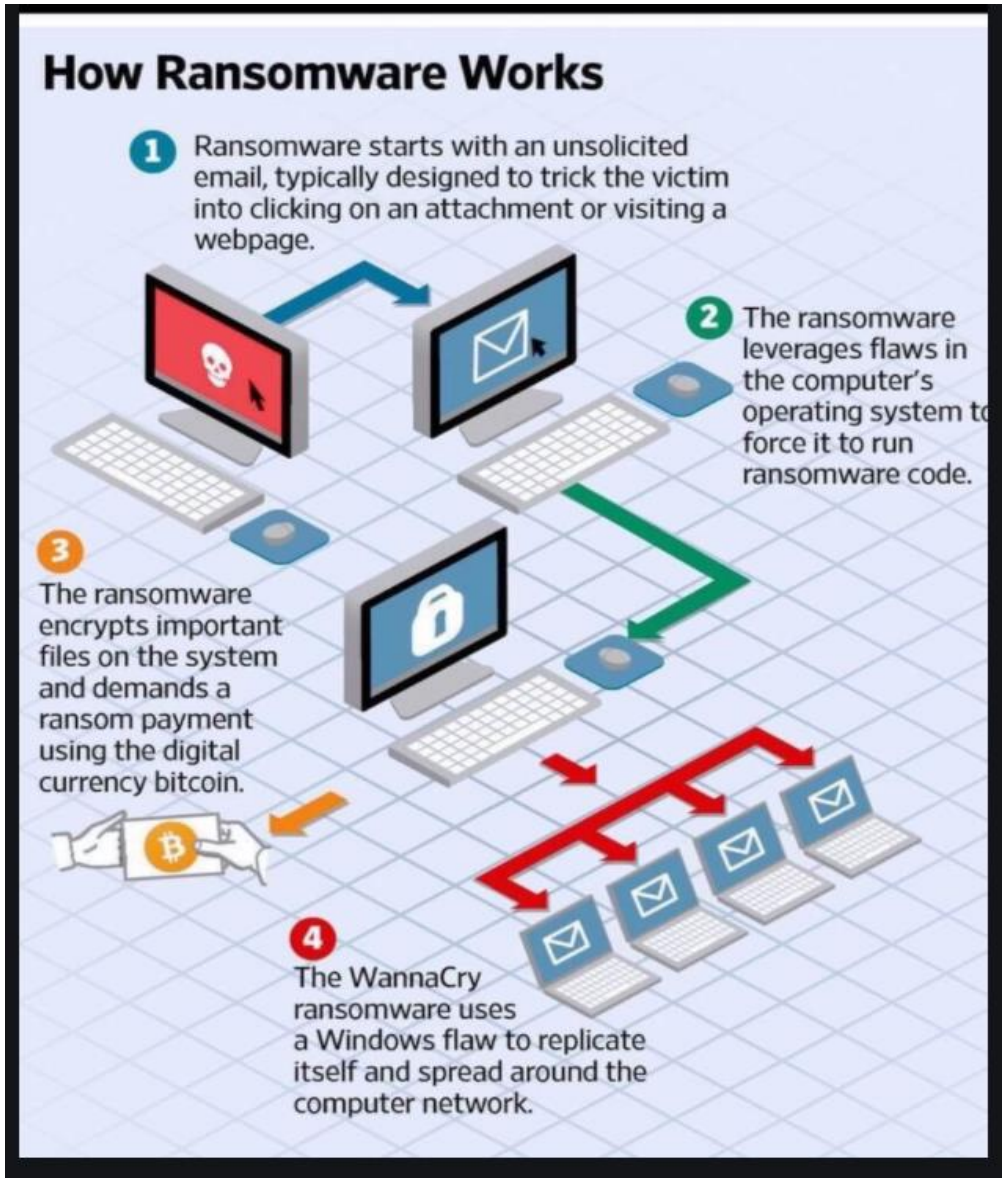
Read Down for Dependency Map.
Read Up for Impact Analysis.



CJA Helps Healthcare Face a Ransomware Attack

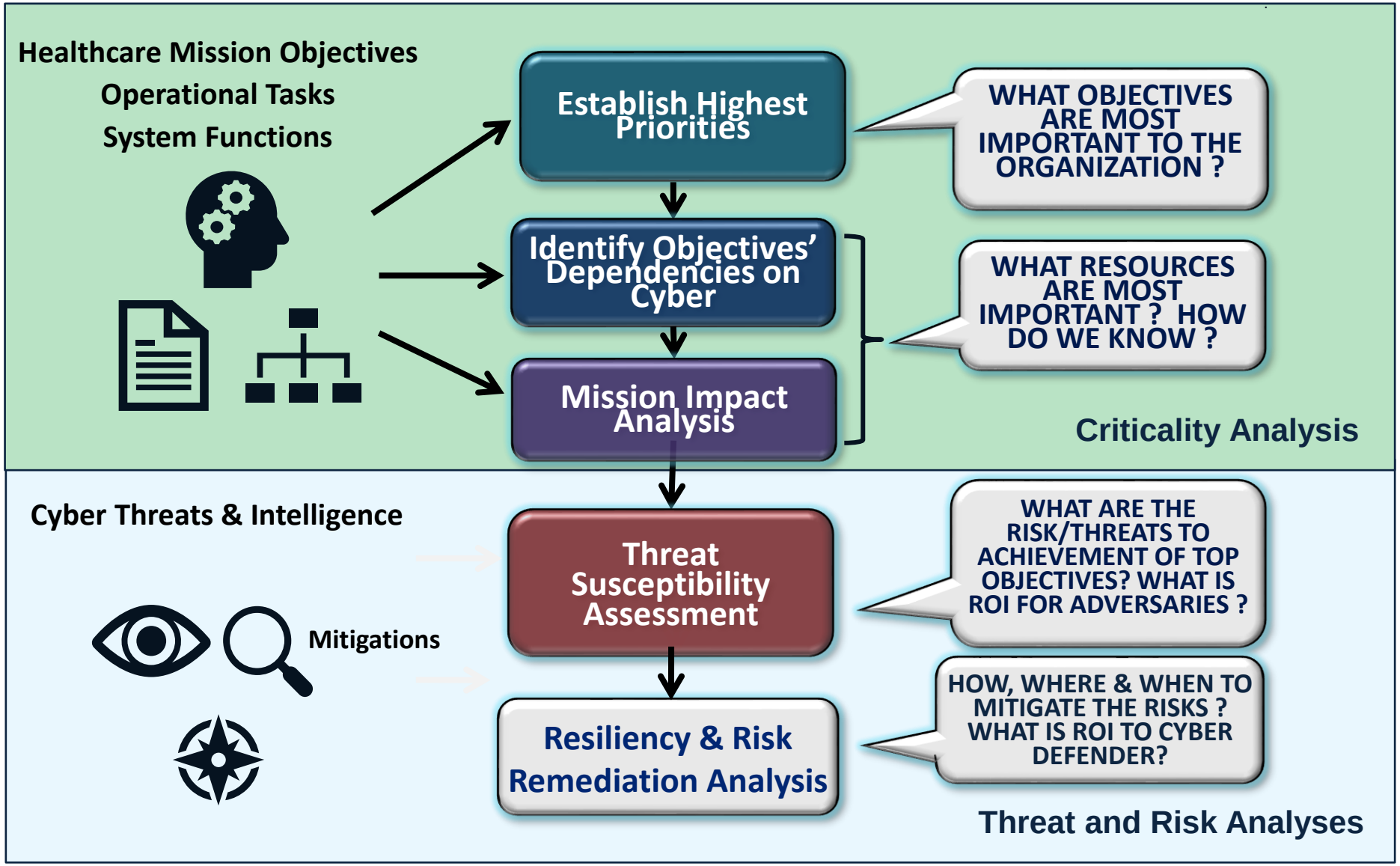
CJA's purpose is not to prevent or detect a ransomware attack. It mitigates the risk posed by such major attacks. CJA serves an organization:

- Before an attack, to better prioritize its cyber mitigations in protecting its most important assets
- During an attack, to more effectively respond in addressing most critical assets first
- During an attack, to know extent and impact of processes and systems affected and their relationship to top healthcare objectives
- After an attack, to provide supplemental protection to critical assets not yet involved in attack



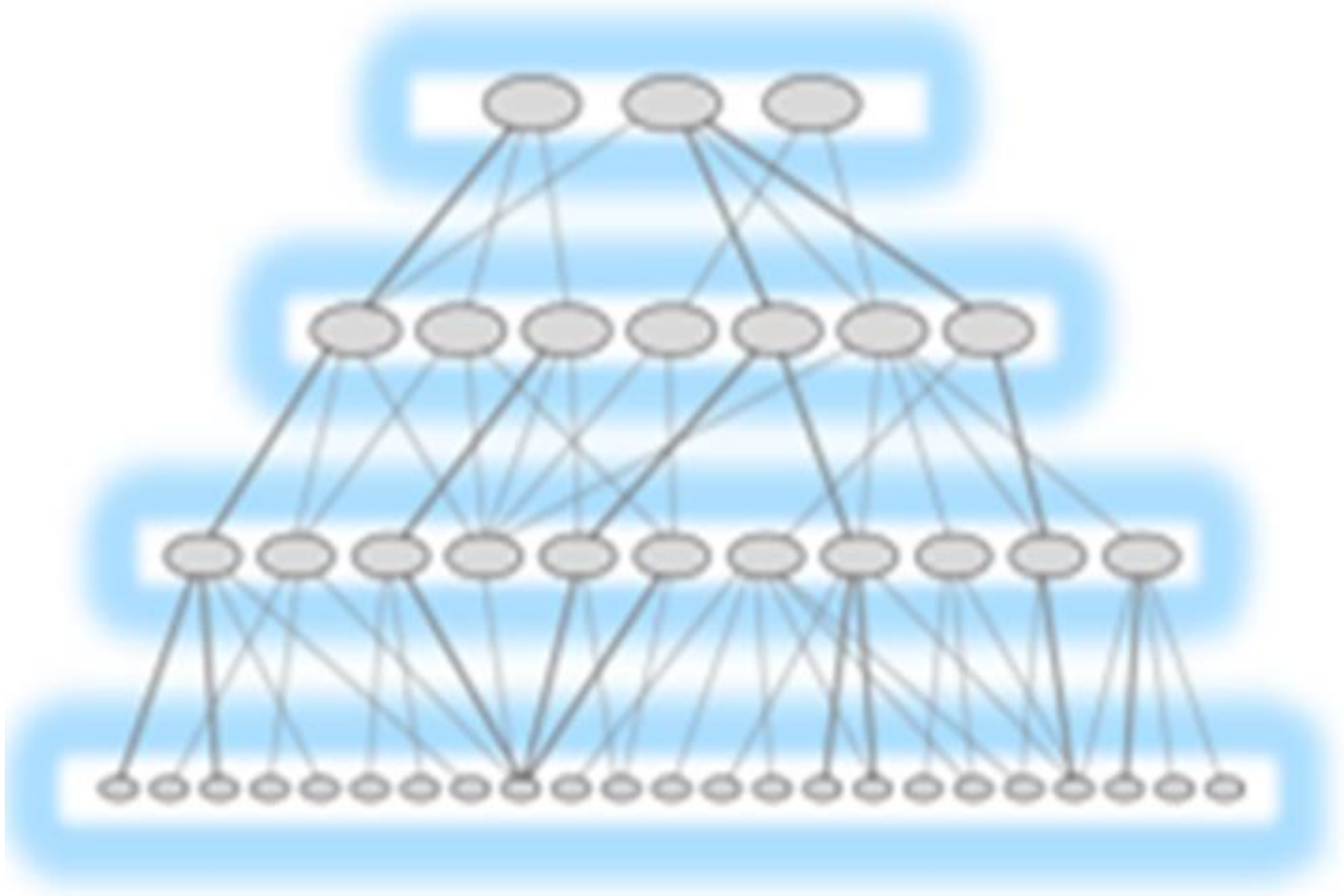
Ref: Wall Street Journal, 2017. Cybersecurity Experts Try to Understand How Ransomware Invaded Networks - WSJ

CJA Identifies Most Critical Assets



Model Terminology

- **Healthcare Objectives (HO)**
  - Highest tier in model
  - Typical range: 3-6 nodes
  - Matrix 1 in tool
- **Operational Tasks (OT)**
  - Second tier in model
  - Typical range: 20-100 nodes
  - Matrix 2 in tool
- **System Functions (SF)**
  - Third tier in model
  - Typical range: 25-125 nodes
  - Matrix 3 in tool
- **Cyber Assets (CA)**
  - Fourth and lowest tier in model
  - Typical range: 40-200 nodes
  - Matrix 4 in tool



MITRE

CJA: Five Step Process

- Initial analysis using client-provided materials and discussions with senior management
- Outcomes: Agreement on scope of analysis and draft build of model for Matrices 1 & 2

- Best done with senior management for HOs and senior healthcare SMEs for OTs
- Outcomes: Validated build and scoring of Matrices 1 & 2. Leads to draft build of model for Matrices 3 & 4.

- Best done with IT staff and operators for SFs and CAs.
- Outcomes: Builds and scorings of Matrices 3 & 4.
- Leads to Dependency Maps

- Initial deliverables
- Outcomes: Refined and completed model. Completed Dependency Maps.
- Yields Impact Analysis and identifies Crown Jewels.

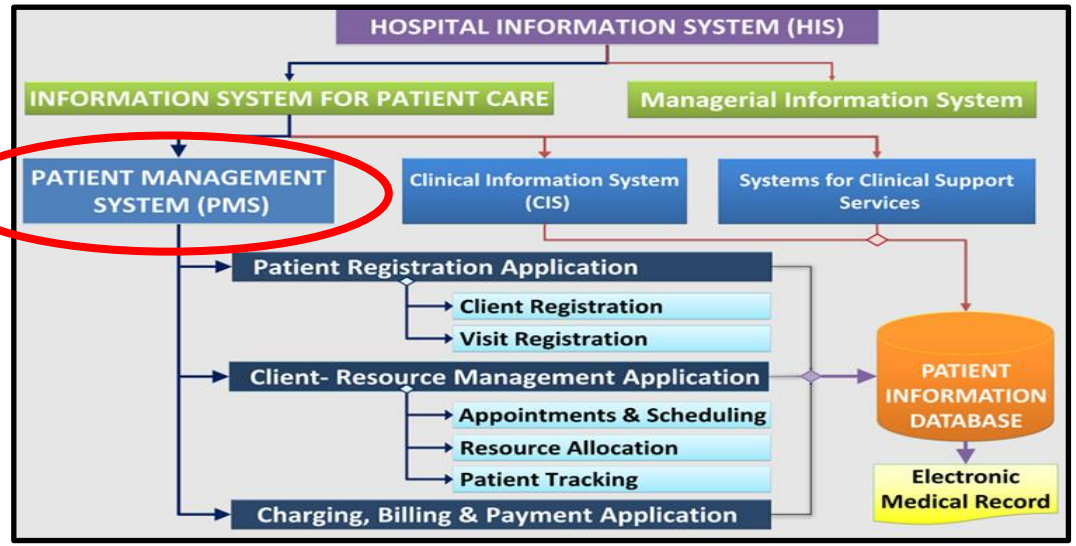
- Best done with senior management (objectives' owners) and system owners
- Outcomes: Explored options. Allows for better resource management through priorities. Provides focus for future risk analyses and mitigation strategies.

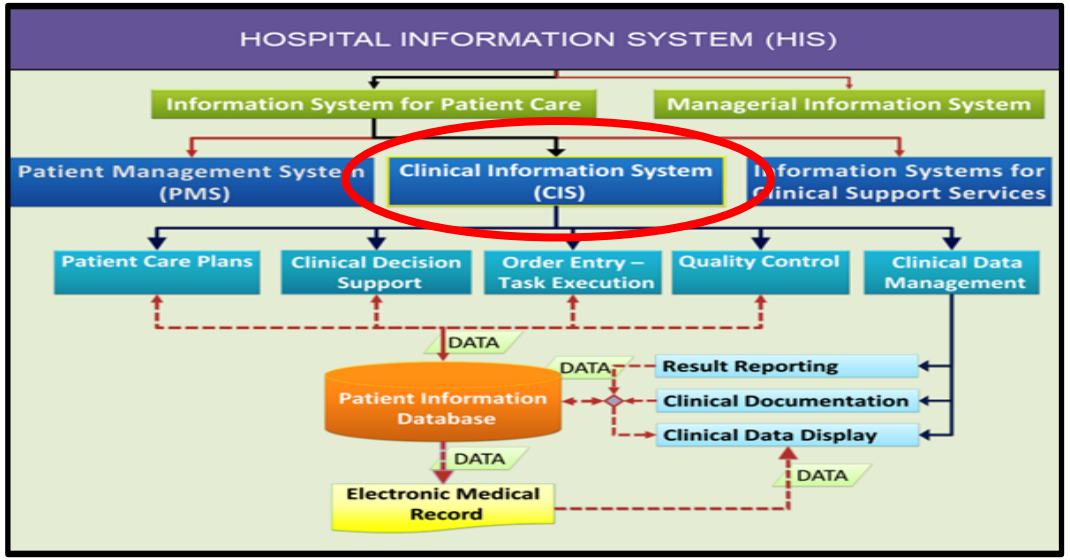
Functional Decomposition

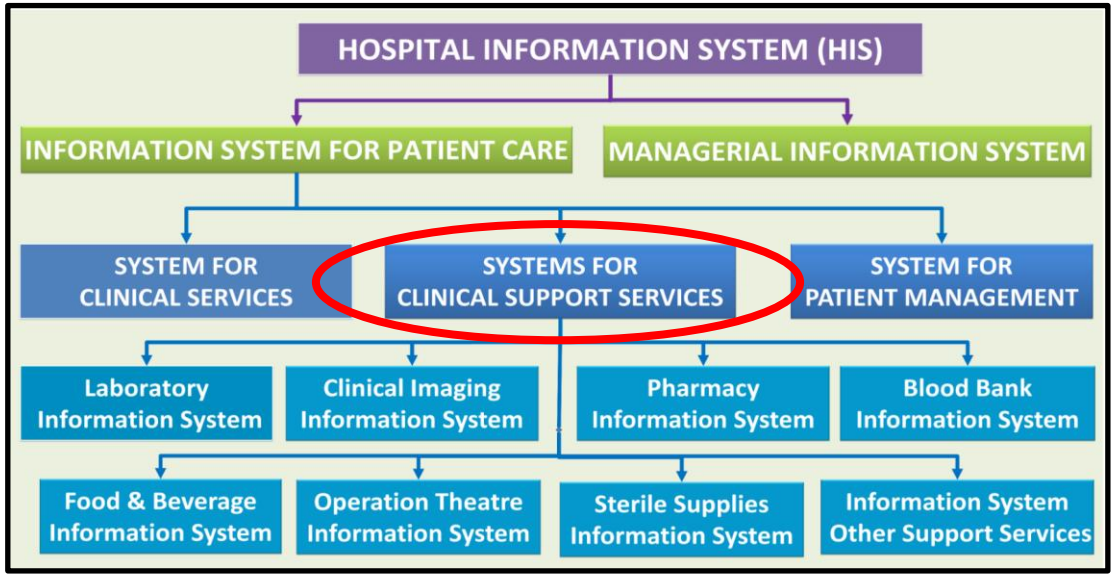
- CJA determines its dependency mappings and ultimate impact analysis by performing decomposition of healthcare IS modules
- Healthcare IS broadly divided into two major areas: **Patient Care IS** and **Managerial IS.** Both are comprised of numerous, likely targets for attacks
- **Patient Care IS** of particular importance. Likely contains **most** crown jewels. Notionally, comprised of:
  - **Patient Mgt System (PMS)** – e.g., registration, appointments and scheduling, charging and billing
  - **Clinical Information System (CIS)** – e.g., patient care plans, clinical decisions, medical order entry, clinical data management
  - **Clinical Support Systems (CSS)** – e.g., labs, imaging, pharmacy, blood bank, operating room schedules

Ref: Dr. Dollah, 2019 https://drdollah.com/hospital-information-system-his/Information Systems in Health Care | Health Care Service Delivery (drdollah.com)

Patient Care IS Breakout

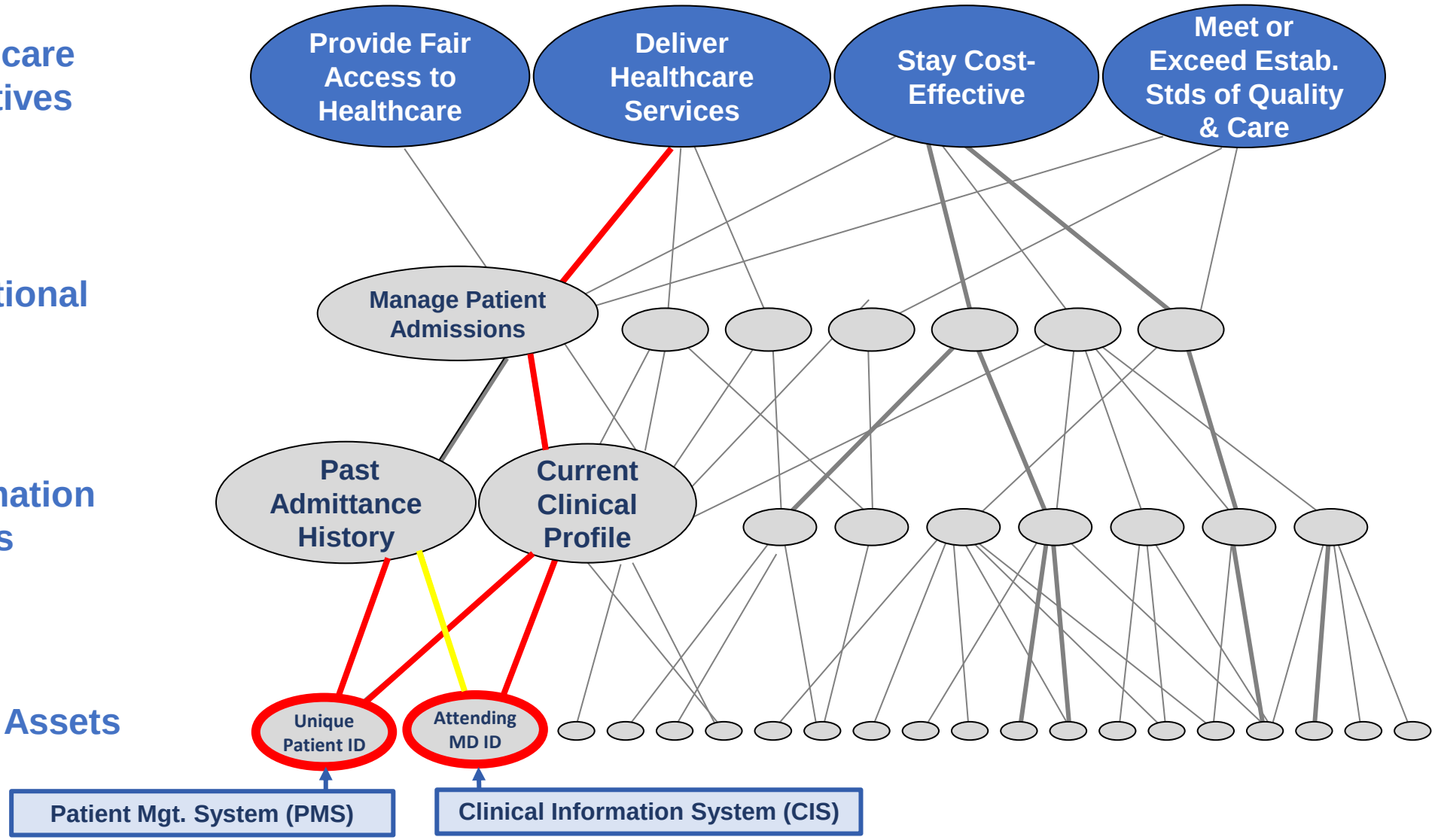




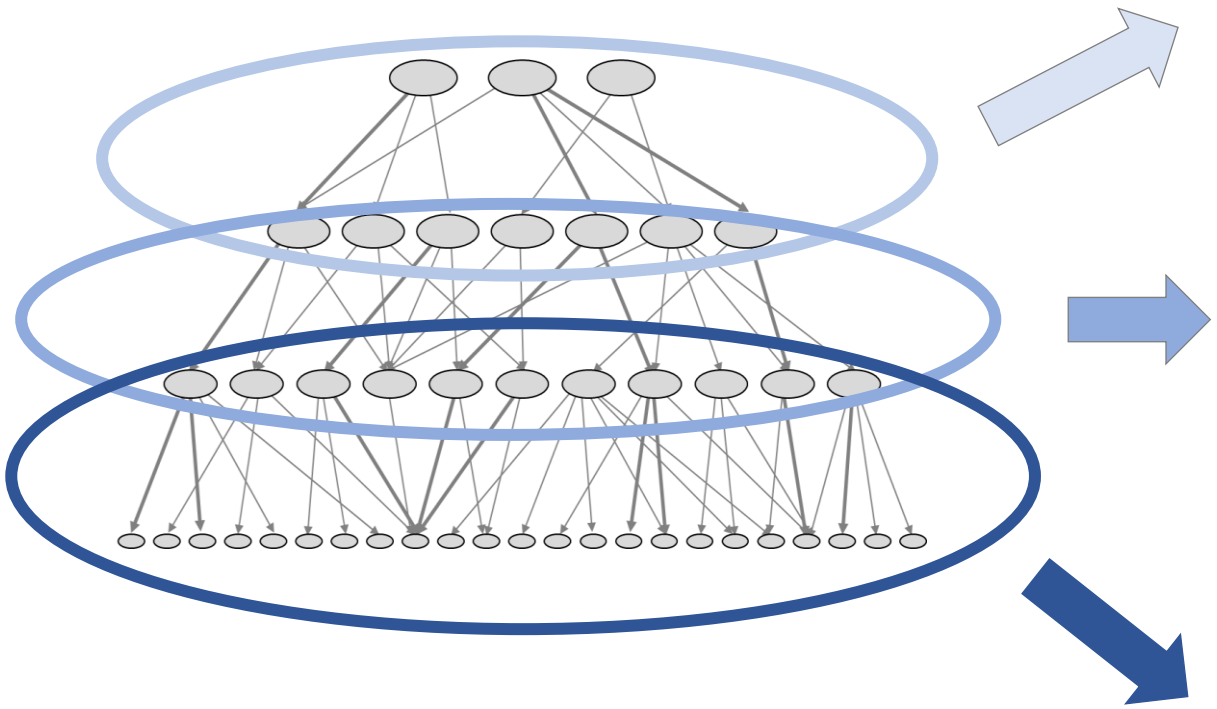


Ref: Dr. Dollah, 2019
https://drdollah.com/hospital-information-system-his/Information Systems in Health Care | Health Care Service Delivery (drdollah.com)

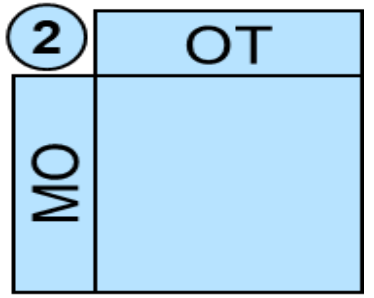
Sample, Partial Healthcare Decomposition



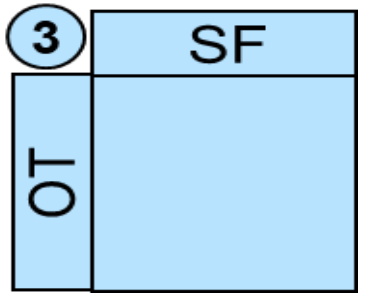
How Dependency Tree Relates to CJA Matrices for Scoring (1 of 2)



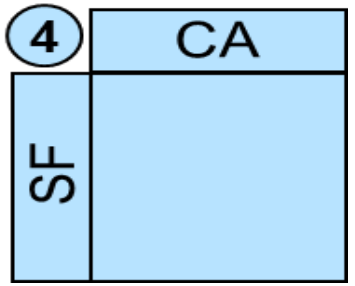
Matrix 2 captures HO/MO (parent) to OT (child) relationships.



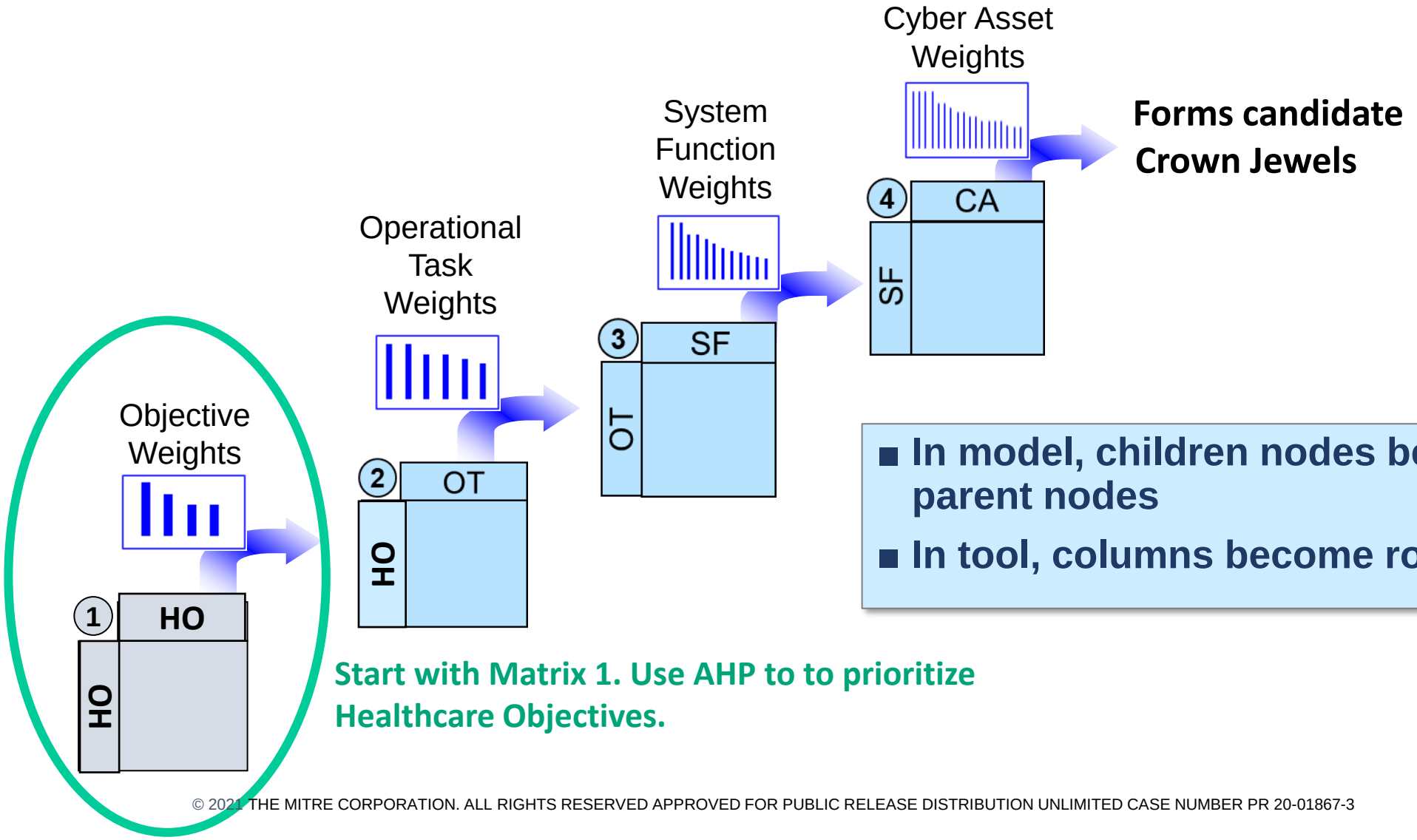
Matrix 3 captures OT (parent) to SF (child) relationships.



Matrix 4 captures SF (parent) to CA (child) relationships.



How Dependency Tree Relates to CJA Matrices for Scoring (2 of 2)



- In model, children nodes become parent nodes
- In tool, columns become rows

Start with Matrix 1. Use AHP to to prioritize Healthcare Objectives.

Healthcare Objectives:

What Might Matrix 1 Look Like?

Notional

SCALE:

1 = Row is EQUALLY IMPORTANT to Column

2 = Row is SLIGHTLY MORE IMPORTANT than Column

4 = Row is SIGNIFICANTLY MORE IMPORTANT than Column

8 = Row is FAR MORE IMPORTANT than Column

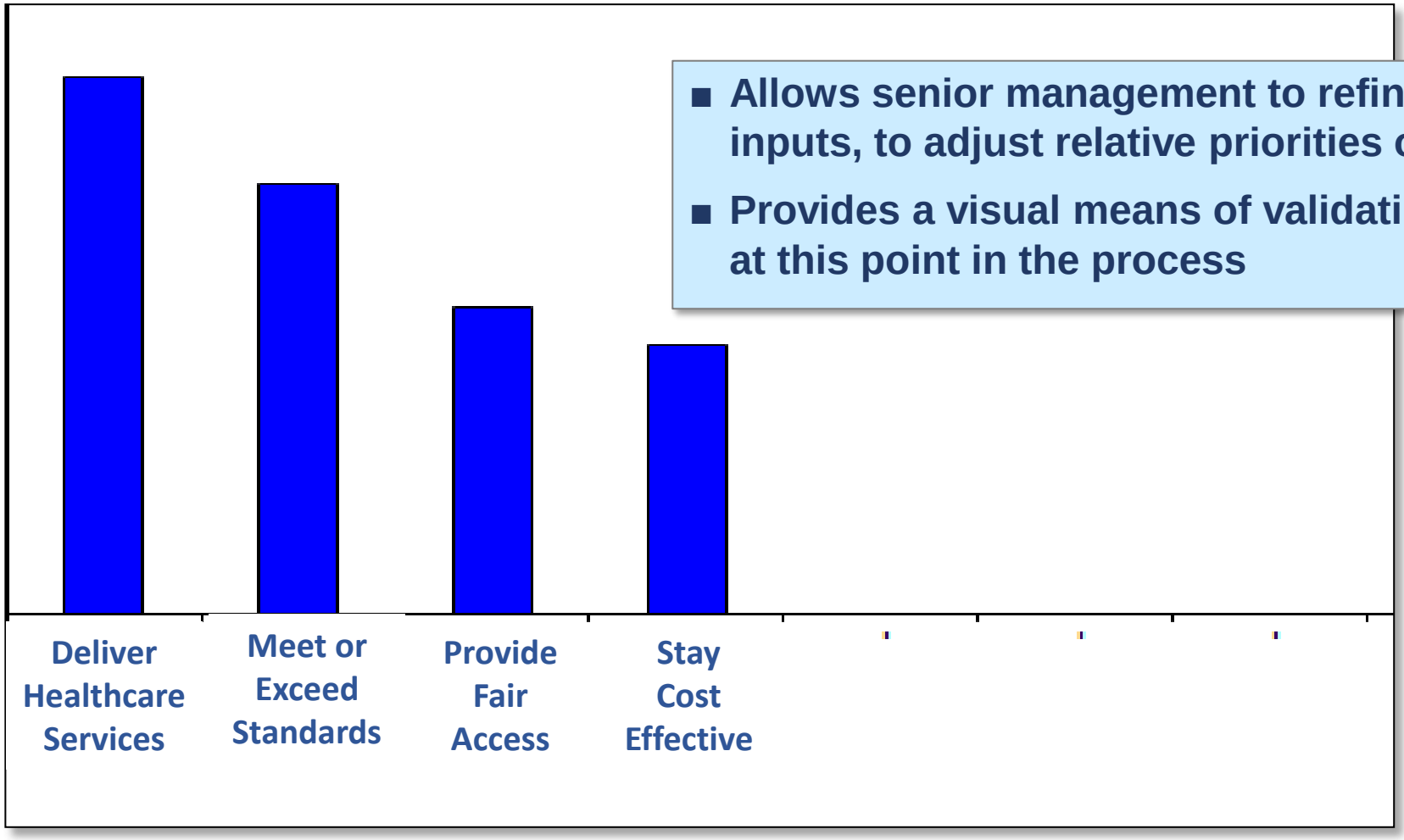
(Use reciprocals for LESS IMPORTANT cases)

		Deliver Healthcare Srvcs	Meet/Exceed Standards	Provide Fair Access	Stay Cost Effective	Sums	Normalized Relative Weights
1	Deliver Healthcare Srvcs	1	1.25	1.75	2	6.000	0.348
2	Meet/Exceed Standards	0.8	1	1.4	1.6	4.800	0.279
3	Provide Fair Access	0.571	0.714	1	1.14	3.429	0.199
4	Stay Cost Effective	0.5	0.625	0.875	1	3.000	0.174
5	-						
					Total >>	17.229	1.000

- **Based on the Analytic Hierarchy Process (AHP)**
- **Inputs only required in the white cells – all others auto-calculated**
- **Result is a set of normalized Relative Weights**

Healthcare Objectives: Sorted by Relative Weights

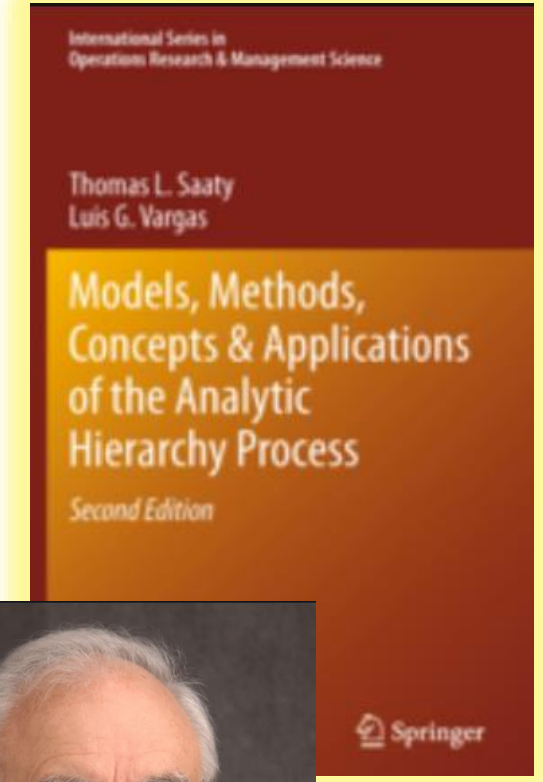
Notional

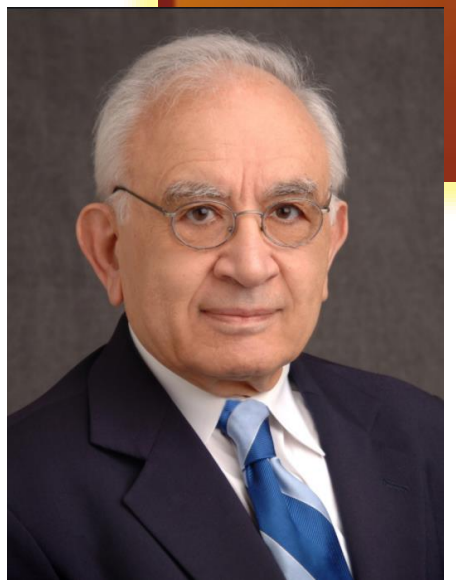


- Allows senior management to refine their inputs, to adjust relative priorities of objectives
- Provides a visual means of validating the model at this point in the process

Healthcare Objectives and AHP

- **Analytical Hierarchy Process (AHP) determines relative importance among healthcare objectives and used to form CJA Matrix 1**
- **Provides a means of measuring *intangible* properties, e.g., importance of objectives to senior management, when no direct measurement scale is possible**
  - Employs pairwise comparisons using a fundamental scale
  - Comparison values are summed up and the sums normalized
  - Result is a set of relative weights
- **Developed by Thomas L. Saaty (1926 - 2017)**
  - Very-well respected approach used across numerous domains
  - The Analytic Hierarchy Process: Planning, Setting Priorities, Resource Allocation," 1980
  - "Decision Making with the Analytic Hierarchy Process," 2008





MITRE

Healthcare Objectives:

Matrix 1 Relationships

	Objective 1	Objective 2	Objective 3	Sum of Row	Relative Weights
Objective 1	1	m_{12}	m_{13}	$1+m_{12}+m_{13}$	$\mathbf{Wmo_1}$
Objective 2	$\frac{1}{m_{12}}$	1	$\frac{m_{13}}{m_{12}}$	$\frac{1+m_{12}+m_{13}}{m_{12}}$	$\mathbf{Wmo_2}$
Objective 3	$\frac{1}{m_{13}}$	$\frac{m_{12}}{m_{13}}$	1	$\frac{1+m_{12}+m_{13}}{m_{13}}$	$\mathbf{Wmo_3}$
			Total:	$\frac{(1+m_{12}+m_{13})(m_{12}+m_{13}+m_{12}m_{13})}{m_{12}m_{13}}$	$\mathbf{Wmo_1}+\mathbf{Wmo_2}+\mathbf{Wmo_3}=1.0$

Ref: J. Watters, "The Risk-to-Mission Assessment Process (RiskMAP): A Sensitivity Analysis and an Extension to Treat Confidentiality Issues (I3P Research Report #15, MITRE PR 09-2994)," The MITRE Corporation, 2009.

Operational Tasks - Matrix 2

Notional

- Purpose: to determine IMPACT of each task failure on each Healthcare Objective (HO)
- Sample question and answer: **What is the impact on the HO Deliver Healthcare Services if Task 1 fails, or fails to operate as intended?**
- The shadings of orange provide a quick visual cue to the highest values on the screen

Healthcare Objective Impact of Task Failure/Degradation

0 = No Impact on HO achievement

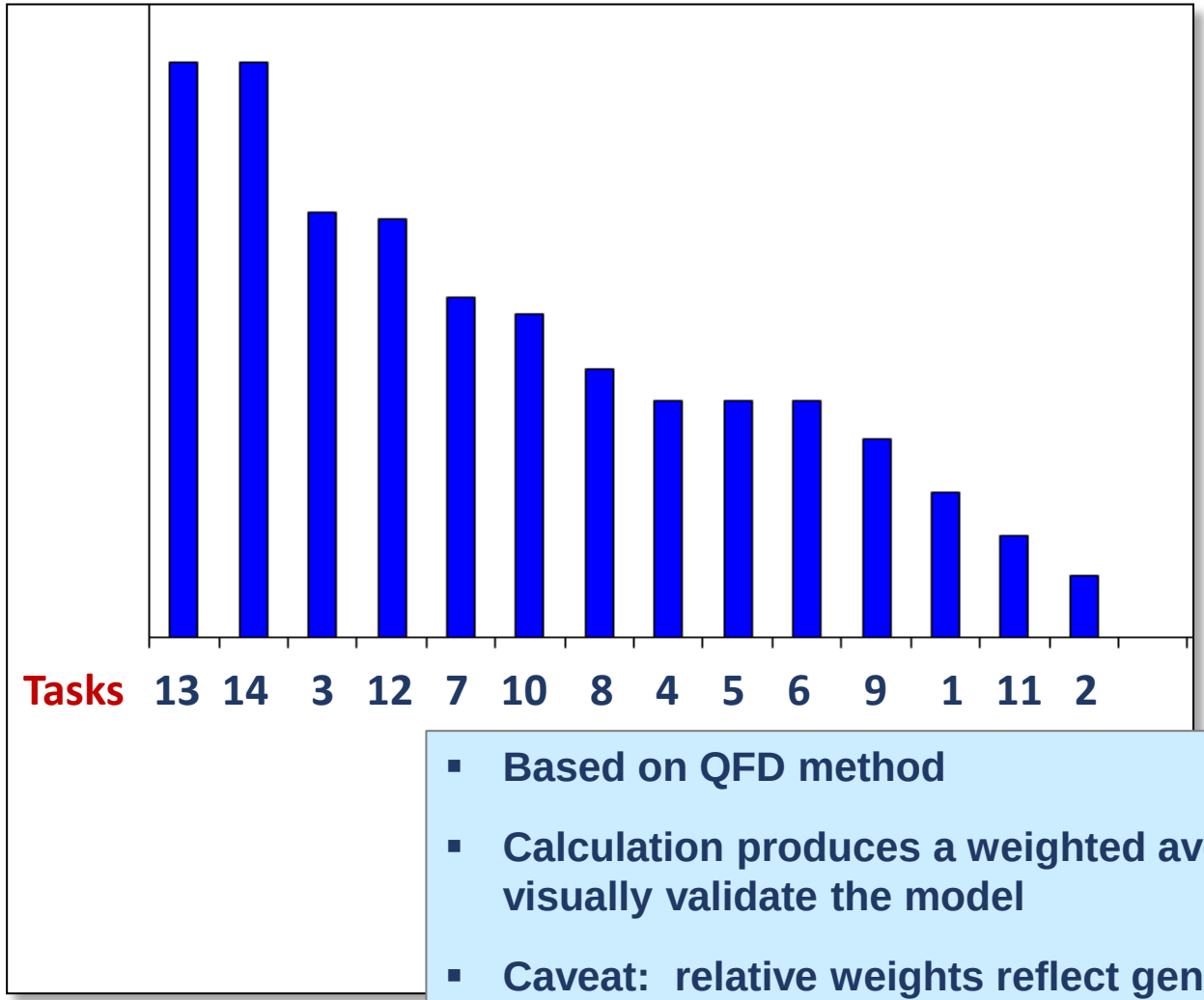
30 = HO is achievable using a documented work around

75 = HO is degraded even using a work-around

95 = HO is not achievable at all

No.	Healthcare Objective (HO)	MO Rel Wt	Task	1	2	3	4	5	6	7	8	9	10	11	12	13	14
			Task Rel Wt	19.55	8.36	56.87	31.69	31.69	31.69	45.62	36.04	26.52	43.28	13.58	56.07	76.97	76.97
			Task	Task 1	Task 2	Task 3	Task 4	Task 5	Task 6	Task 7	Task 8	Task 9	Task 10	Task 11	Task 12	Task 13	Task 14
				Task Criticality to Healthcare Objective													
1	Deliver Healthcare Services	0.348			70								70		30	70	70
2	Meet of Exceed Standards	0.279		30	30	30	70	70	70	70	70	30		30	70	95	95
3	Provide Fair Access	0.199		30		95				70		30	95		70	70	70
4	Stay Cost Effective	0.174		30		30	70	70	70	70	95	70		30	70	70	70

Operational Tasks - Pareto View

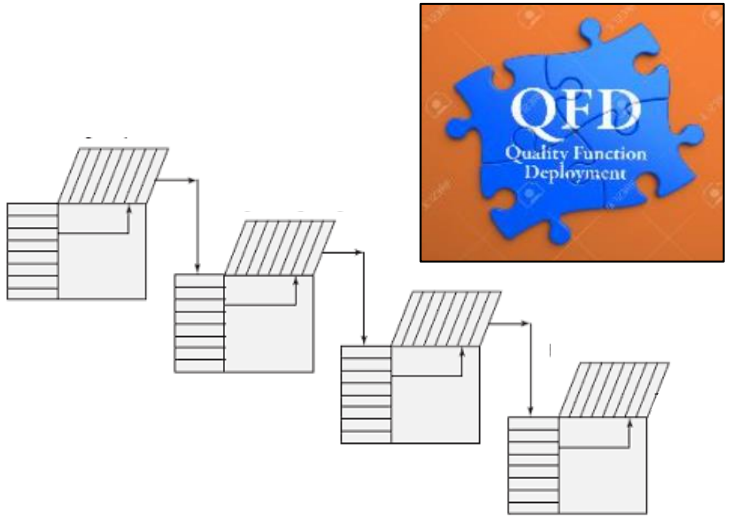


- Based on QFD method
- Calculation produces a weighted average. Relative Weights provide a quick means to visually validate the model
- Caveat: relative weights reflect general importance but do not constitute impact on their own

MITRE

Operational Tasks, System Functions, Cyber Assets and QFD

- **Quality Function Deployment (QFD) used to form CJA Matrices 2 - 4**
  - Uses series of matrices rather than single “House of Quality”
  - Adds cardinal scale for developing relative weights
- **Decomposes top-level product requirements into underlying qualities and functions. Used to identifies dependencies.**
- **Originally intended for manufacturing setting**
- **Developed by Dr. Yoji Akao (1928 - 2016)**
  - Original work appeared in the 1960’s shipyards in Japan. Brought to U.S. by Don Clausing of MIT
  - “Development History of Quality Function Deployment. The Customer Driven Approach to Quality Planning and Deployment,” 1994

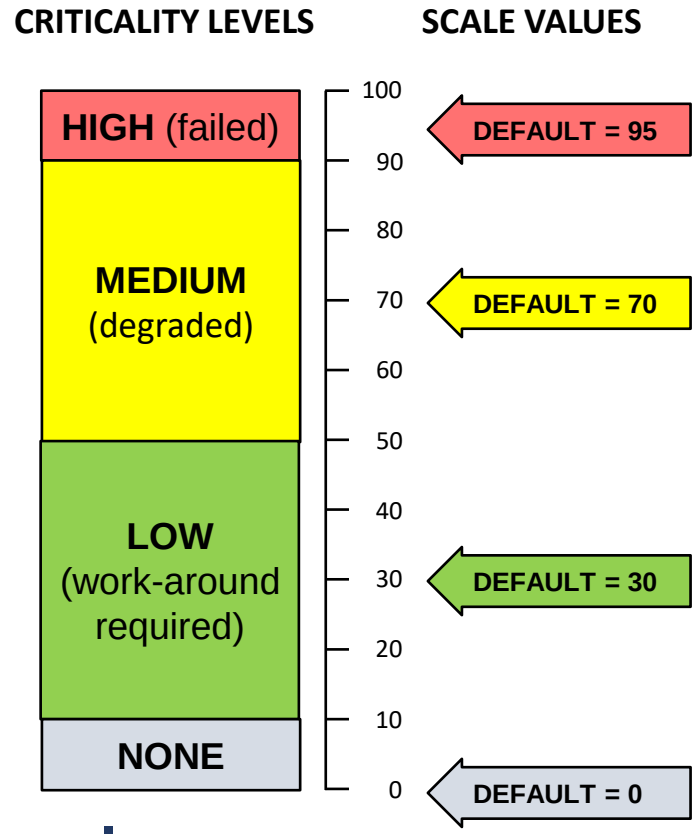


Waterfall Relationship of QFD Matrices used by CJA

MITRE

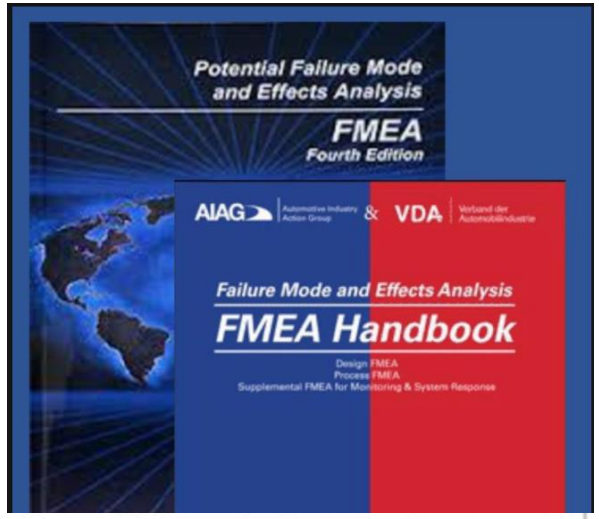
Values in CJA Matrices 2 - 4

- **Represent criticality. Four levels.**
  - High (failure). Default is 95.
  - Medium (degradation, even with work-around implemented). Default is 70.
  - Low (a documented, trained-to work-around is required). Default is 30.
  - None (no impact). Default is 0.
- **Used to calculate relative weights**
- **Provide a sense of placement within each matrix level**



Failure Modes and Effects Analysis (FMEA)

- **CJA uses FMEA-like approach to predict impacts to objectives due to failures in system "components"**
  - System or information dependencies identified through system decomposition
  - Impacts of failures predicted during Impact Analysis (IA)
  - Comes from reliability discipline within engineering
- **Tied to Failure Modes, Effects and Criticality Analysis (FMECA)**
  - FMECA extends FMEA by introducing likelihood of failure
  - Prescribed in military standards where loss of life is highest risk. Adopted by NASA and as US/European airworthiness standards

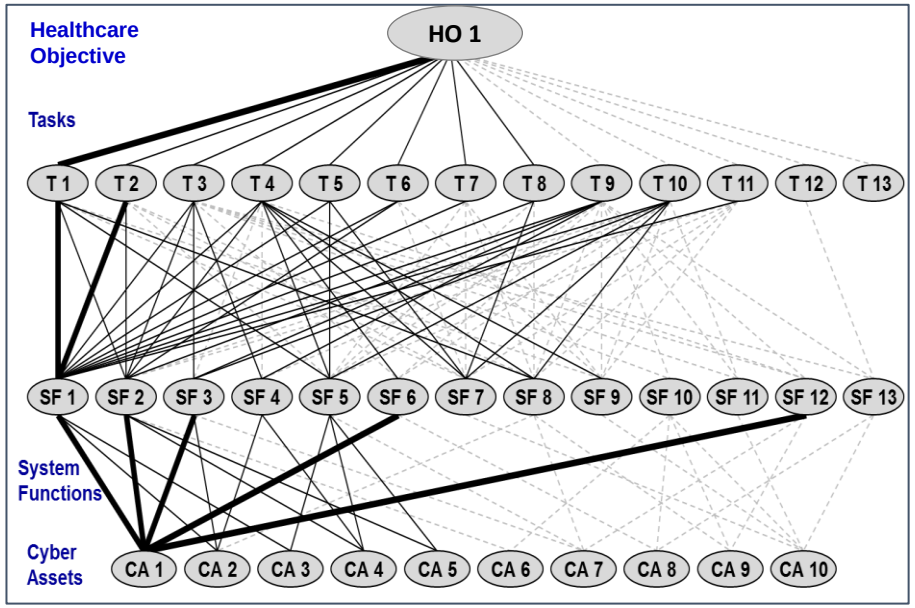


Failure Modes Criticality Matrix (Quantity for Internal Causes only)

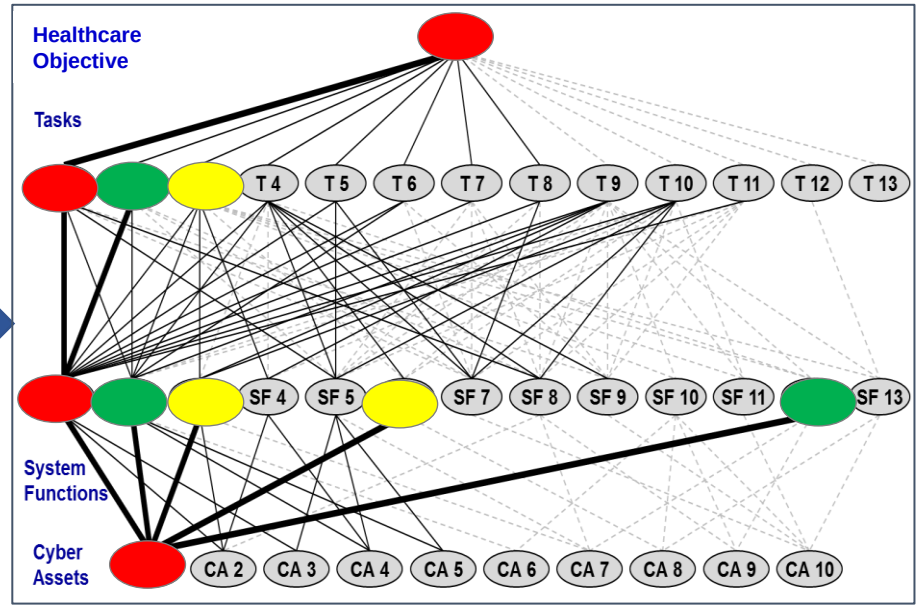
CRITICALITY		SEVERITY				
Group	Range	V	IV	III	II	I
a	b	d				
A	0.2 - Infinity	0	0	0	0	0
B	0.1 - 0.2	0	0	0	0	0
C	0.01 - 0.1	0	0	3	2	2
D	0.001 - 0.01	0	0	3	1	1
E	0 - 0.001	0	0	1	0	1

Impact Analysis (IA)

- Occurs after model is built, data is entered, and matrices are scored
- Performed by encoded algorithms in CJA tool. Uses what-if technique to sequentially fail each cyber asset for each healthcare objective
- Results in simulated impacts percolating upwards



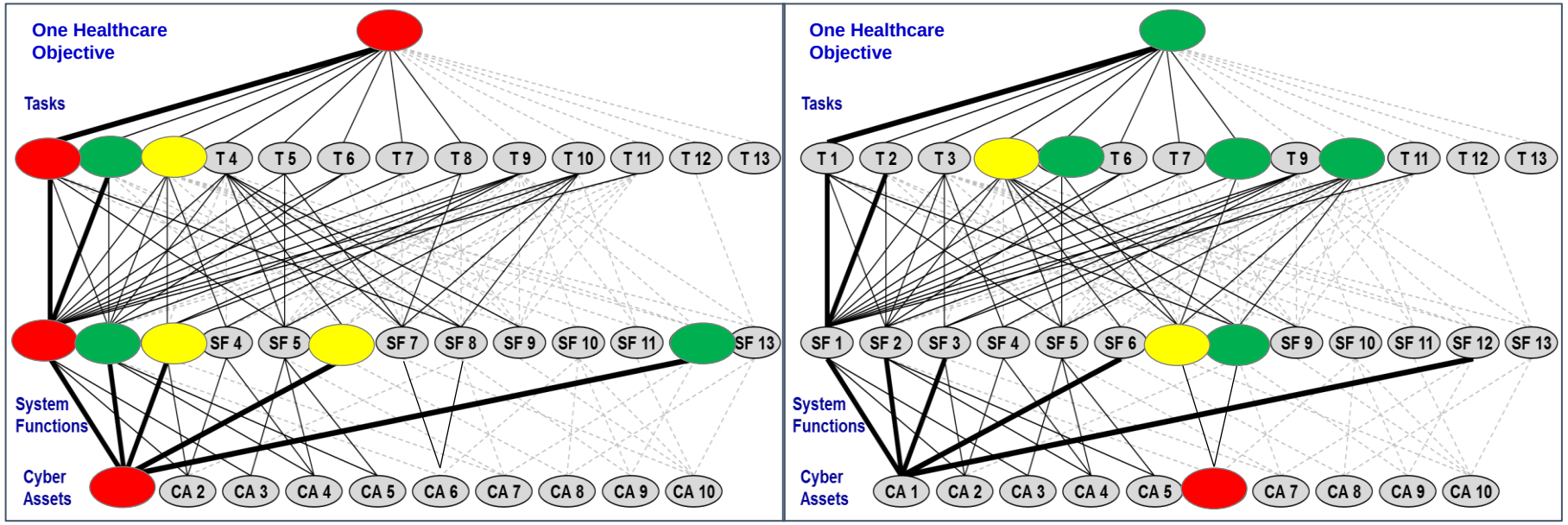
Dependency Map for one objective



After Impact Analysis, from first failed asset

When is an Asset a Crown Jewel?

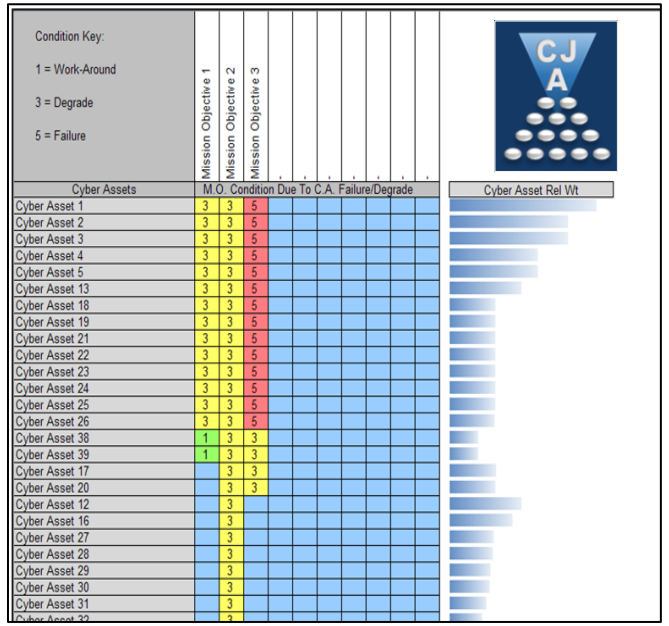
- Definition: a cyber asset whose failure, or failure to perform as intended, causes a major healthcare objective to fail
- Typically a physical, system, or information asset an organization cannot afford to lose, i.e., operate without
- Likely candidates for adversaries, especially in ransomware attacks



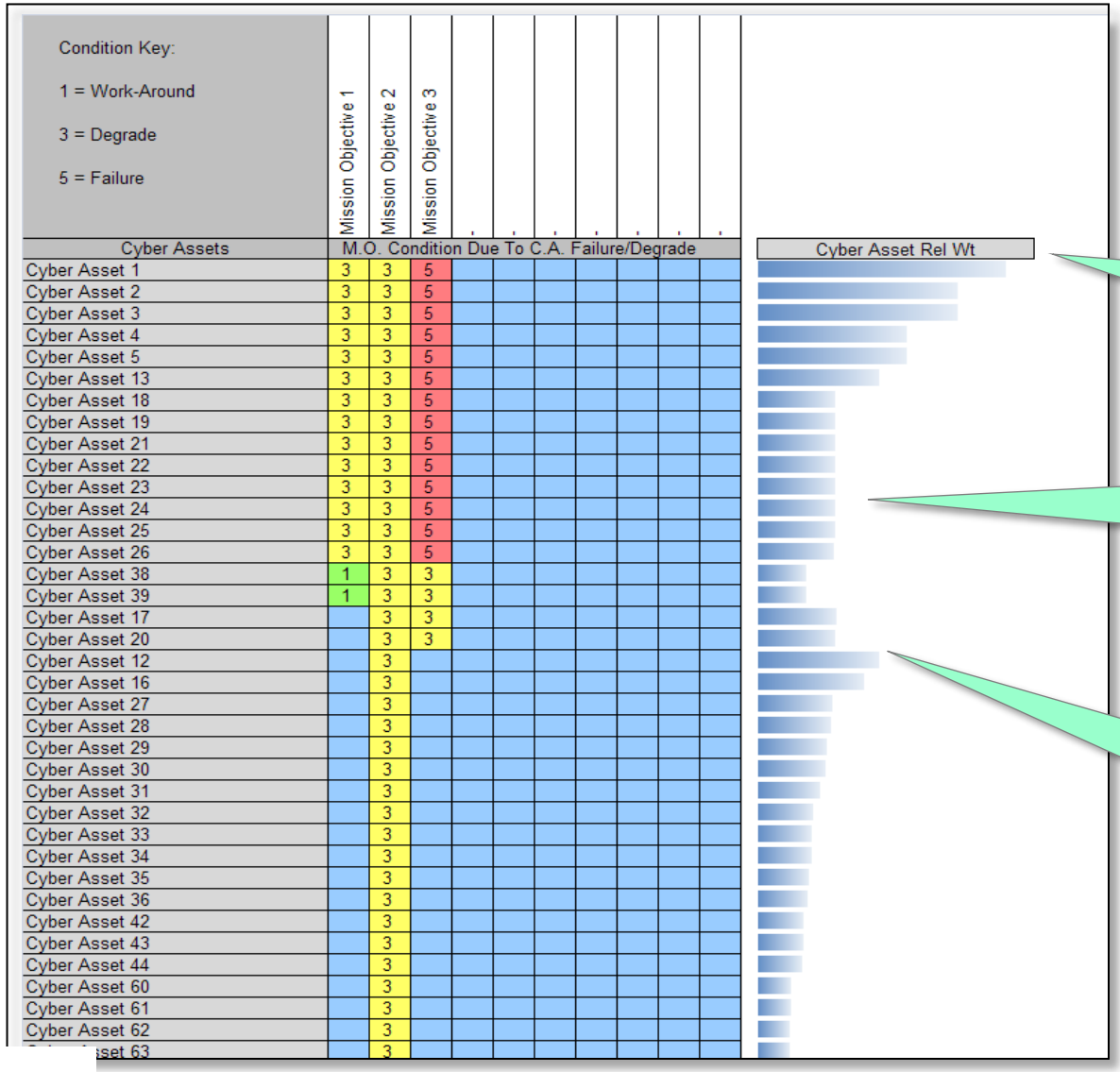
CA1 fails and is a Crown Jewel **CA6 fails but is not a Crown Jewel**

CJA Results: Portrayal Table

- **Available as part of Impact Analysis**
  - Shows relative weights of each cyber asset as a whole. Allows for healthcare SME reality checks
- **Impact view option**
  - Sorts by impact to bring Crown Jewels to the top.
  - Assists in prioritizing resources for follow-on assessments and/or resiliency mitigations
- **Intermediate option**
  - Allows an intermediate Portrayal Table to view after Matrices 1 & 2, before populating Matrices 3 & 4
  - Good way to solidify model before going forward, especially if model is large, complex
- **Propagation option**
  - Allows a force of all degraded scores in tables to impact as failures
  - Commonly used in scenarios where human life and safety are paramount, e.g., manned spaceflight



Portrayal Table Expanded



Condition Key:

1 = Work-Around

3 = Degrade

5 = Failure

Cyber Assets	M.O. Condition Due To C.A. Failure/Degrade										Cyber Asset Rel Wt
	Mission Objective 1	Mission Objective 2	Mission Objective 3								
Cyber Asset 1	3	3	5								
Cyber Asset 2	3	3	5								
Cyber Asset 3	3	3	5								
Cyber Asset 4	3	3	5								
Cyber Asset 5	3	3	5								
Cyber Asset 13	3	3	5								
Cyber Asset 18	3	3	5								
Cyber Asset 19	3	3	5								
Cyber Asset 21	3	3	5								
Cyber Asset 22	3	3	5								
Cyber Asset 23	3	3	5								
Cyber Asset 24	3	3	5								
Cyber Asset 25	3	3	5								
Cyber Asset 26	3	3	5								
Cyber Asset 38	1	3	3								
Cyber Asset 39	1	3	3								
Cyber Asset 17		3	3								
Cyber Asset 20		3	3								
Cyber Asset 12		3									
Cyber Asset 16		3									
Cyber Asset 27		3									
Cyber Asset 28		3									
Cyber Asset 29		3									
Cyber Asset 30		3									
Cyber Asset 31		3									
Cyber Asset 32		3									
Cyber Asset 33		3									
Cyber Asset 34		3									
Cyber Asset 35		3									
Cyber Asset 36		3									
Cyber Asset 42		3									
Cyber Asset 43		3									
Cyber Asset 44		3									
Cyber Asset 60		3									
Cyber Asset 61		3									
Cyber Asset 62		3									
Cyber Asset 63		3									

Sorted by Impact

High relative weights confirm already-suspected cyber assets

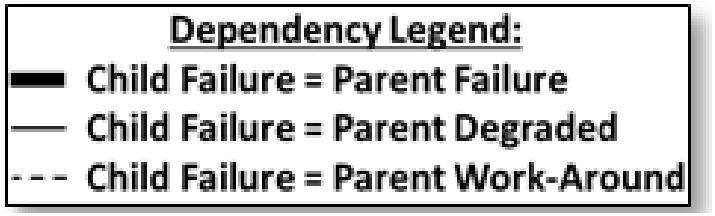
Relative weights provide a means of prioritizing among crown jewels

Impact analysis reveals little-used cyber assets that are nonetheless healthcare critical

MITRE

Dependency Maps & Impact Maps

- Available after model build and data entry, like Portrayal Table.
- Part of Impact Analysis (IA)
  - Reading **down** a map shows dependencies. Look at weight of lines

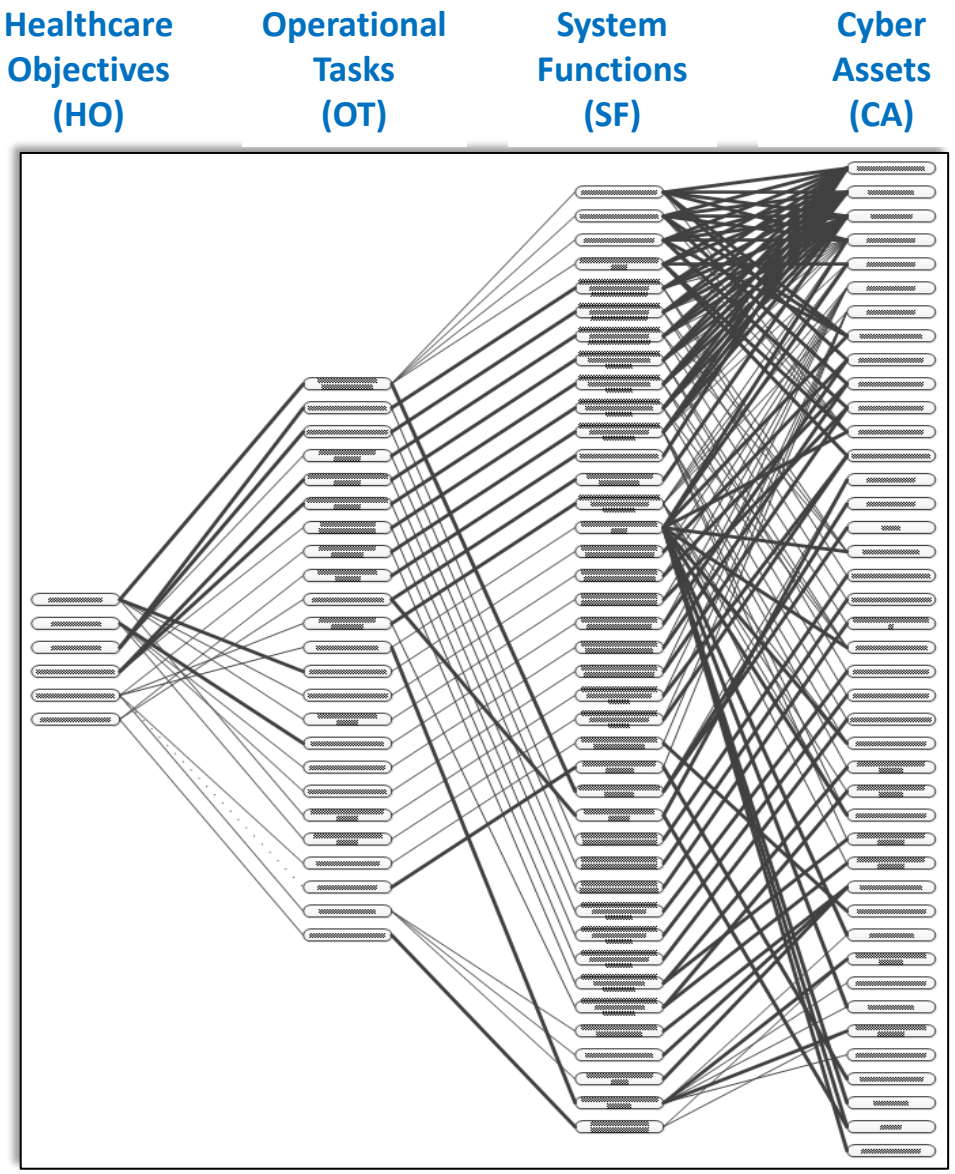


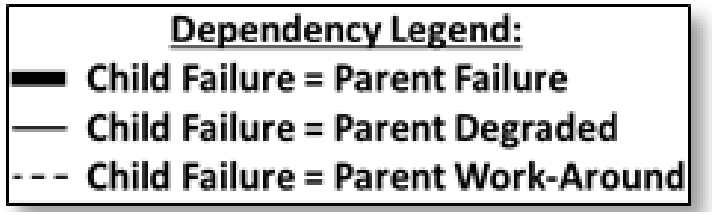
  - Reading **up** a map shows impact (criticality)

- Map for an entire system can be large. Usually does not fit on one slide in readable way. Can display/print one HO at a time for further analysis by healthcare organization

Dependency Map Example

- Full dependency map for 4 objective example. Can zoom and isolate for clear displays of branches and nodes.
- All OT, SF and CA are represented, not just those thought to be critical at the outset
- Overall map provides context and insights to organization
- Provides a visual opportunity to validate the data in an overall sense





MITRE

How Can CJA Help?
Conclusions for your Healthcare Organization

- CJA identifies an organization's **crown jewels,** using prioritized healthcare objectives, as determined from an organization's senior team, as its foundation
- CJA creates a model that is **organization and architecture agnostic,** working for any size organization employing any types of hardware, software, and data
- Upon completion, an organization gains **architecture and functional decompositions** of their HIS, with CJA Dependency Maps and Impact Analysis. The model is reused by an organization as situations necessitate
- CJA offers a **strong component to Cyber Resiliency and Risk Management Planning,** especially when faced with top-tier adversaries capable of executing advanced persistent threats (APTs), such as ransomware
- CJA has been employed in serving our nation's top, critical, federal sponsors **for over 12 years.** CJA SMEs have deep reachback

MITRE