

Enterprise Risk Management + Decision Science/Decision Quality

***TWO APPLICATIONS:
Clinical (Falls with Injury)
Clinical/Technological (AI CDSS)***

Deborah Lessard, JD, MA, BSN, CPHRM, FASHRM

University of Pittsburgh Medical Center

Director Corporate Risk Management Excellence

This presentation is provided solely for educational and informational purposes.

Although I am employed by UPMC, I am not representing UPMC in this presentation, and the content reflects my personal professional experience and perspectives.

Background

- **2012-2014:** DS/DA Certification/Stanford
- **2014-Current:**
 - Society of Decision Professionals
 - ASHRM ERM Faculty and Content Development
- **2016-2024:**
 - ASHRM, AHA, ABA national presentations and contributor to publications
 - Consulting w/ Systems, Commercial Carriers to develop ERM programs
- **2024-Current:** UPMC:
- **Next projected publication** “Risk Management in a Nutshell”
5/2027 (West Academic)

For Reference

UPMC : IDFS = HSD + ISD

42 academic, community, and specialty hospitals in PA, NY, MD (8,000 licensed beds)

800 outpatient sites

100,000 staff members

5,000 employed doctors

Rehab, retirement and LTC options

International Divisions: Italy, Ireland, Croatia

ISD: >4M members

ASHRM

Professional membership group of American Hospital Association

Established in 1980

> 6,000 members representing risk management, patient safety, insurance, law, and other professions

Promotes effective and innovative risk management strategies and professional leadership through education, recognition, advocacy, publications, networking, and interactions with leading health care organizations and government agencies.

ERM

*A structured enterprise approach for identifying, prioritizing, and mitigating system and patient safety risks using **COSO ERM** principles and cross-domain analysis aligned with **ASHRM risk domains**.*

COSO: Committee of Sponsoring Organizations of the Treadway Commission

ASHRM: American Society for Healthcare Risk Management

F I GB USA MEX

**ONE SIZE
DOES NOT
FIT ALL**



Von links bügeln / Iron inside out /
repasser sur l'envers / 只熨反面

Benefits of Implementing an ERM Framework

- Increases range of business opportunities considered while reducing negative surprises
 - Ex: AI Data Governance
- Identifies and manages entity-wide risks
- Reduces performance variability
- Improves resource deployment

Benefits of Implementing an ERM Process: The Risk Professional's Perspective

- Risk management becomes more comprehensive and includes risks that may have a profound impact on the organization.
- Enhances integration between risk management and other key functional areas.
- Allows for the consideration of the full complement of risks.
- Heightens awareness and appreciation of risk management principles and processes throughout the organization.

COSO Framework



Source: ©2017, Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used with permission.

Five Components of ERM

GUIDING PRINCIPLES



Source: ©2017, Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used with permission.

Performance Principles

Principles:

10. Identifies Risk

11. Assesses Severity of Risk

12. Prioritizes Risks

~~13. Implements Risk Responses~~

~~14. Develops Portfolio View~~

ASHRM ERM Domains

Domain	Examples
Operational	Internal processes (failed, inadequate), policies & procedures, business systems, Auto
Clinical/Patient Safety	Delivery of care to residents, patients & clients, PL/GL
Strategic	Organizational direction – brand, competition, failure to adapt, M&A, D&O
Financial	Financial sustainability, access to capital, external financial ratings, revenue cycle, E&O
Human Capital	Workforce, labor market, competency, engagement/culture, employee safety, Employment Practices Liability (EPL), Worker’s Compensation (WC)
Legal/Regulatory	Facilities & administrative costs, licensure, accreditation, health department, CMS/CoP, Stark, HIPAA, intellectual property
Technology	Equipment, machines, hardware/software, virtual, EMR, product liability, cyber
Reputational	Public perception of quality & safety, patient satisfaction, media scrutiny, physician & workforce reputation
Hazard	Assets/value, disaster planning, business interruption, age of plant, construction, Property & Casualty (P&C)

	Financial	Operating	Clinical/Pt Safety	Strategic
Domain Definition	Decisions that affect financial sustainability, access to capital or external financial ratings	Business of healthcare is the delivery of care that is safe, timely, effective and pt-centered within diverse populations.	Risks associated with delivery of care	Decisions relating to focus and direction of organization
Relates to	Business relationships, timing and recognition of revenue and expense	Adverse event management, credentialing, staffing, leadership, deviation from practice	All health care consumers visitors/guests, volunteers and employees	Relates to sustainability of organization
Risks within Domain	Malpractice, litigation, insurance costs, capital structure, credit/interest rate, growth in programs and facilities, corp compliance (fraud and abuse), accounts receivable	Risks resulting from inadequate or failed internal processes, people, or systems that affect business operations	Clinical risks related to failure to follow EBP, med errors, SSE, HAC, falls, etc	Risks associated with growth (M&A, Jt ventures, divestitures, purchase of capital equipt), competitive positioning, brand, reputation, weakness/failure/untimely ability to adapt to changing environment/health reform/consumer priorities, contract administration,

	Legal/Regulatory	Human Capital	Reputational	Technology	Hazard
Domain Definition	Risks associated with identifying, monitoring and managing risks on local, state and federal levels	Internal and external risks associated with work force management	Risks associated when negative publicity is triggered after business event (accurate or inaccurate interpretation)	Risks associated with tangibles: machines, hardware, equipment, devices; intangibles: techniques, algorithms, digital decision making, EMR, HER, Information Systems, systems, processes	Risks associated with assets and their value
Relates to	Relates to legal, statutory, regulatory mandates	Relates to the organization's work force and management of vendors/consultants	Actual event, perception, public reporting, "word by mouth"	Relates to the management of technology, training and competencies of individuals using technology and processes relating to maintenance and repair	Relates to insurable risk related to natural exposure and business interruption
Risks within Domain	Risks associated with CMS/CoP/CfC, MMSEA Section 111, HIPAA, licesure/accreditation, fraud and abuse, product liability mgt liability, intellectual property	Risks associated with recruitment/retention, staffing/scheduling, absenteeism, fatigue, productivity, compensation, work related injuries	Clinical events, publicized contract issues, criminal issues, competitive posits	Risks associated with EMR, Meaningful use, social networking and cyber liability, HIPAA, training/education, information storage and retrieval, asset preservation, technology for clinical dx and tx	Risks associated with facility management, building and equipment age, construction, rennovation, natural disasters

Application: Falls with Injury

What domains for falls with injury?

Reputational:

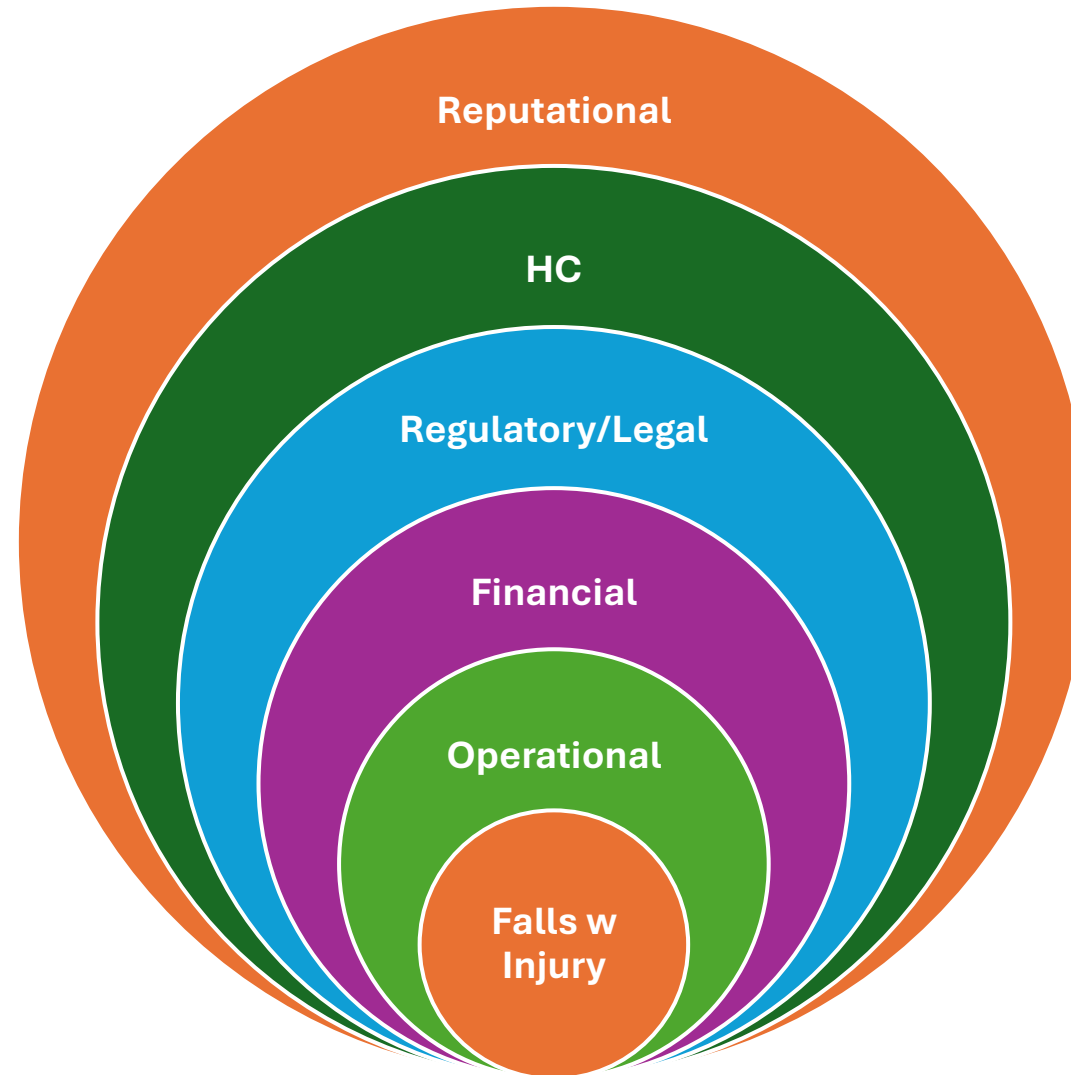
- Quality Ratings
- Patient Trust

HC:

- Staffing Assessment
- Sitter

Regulatory/Legal:

- Never Event
- Survey



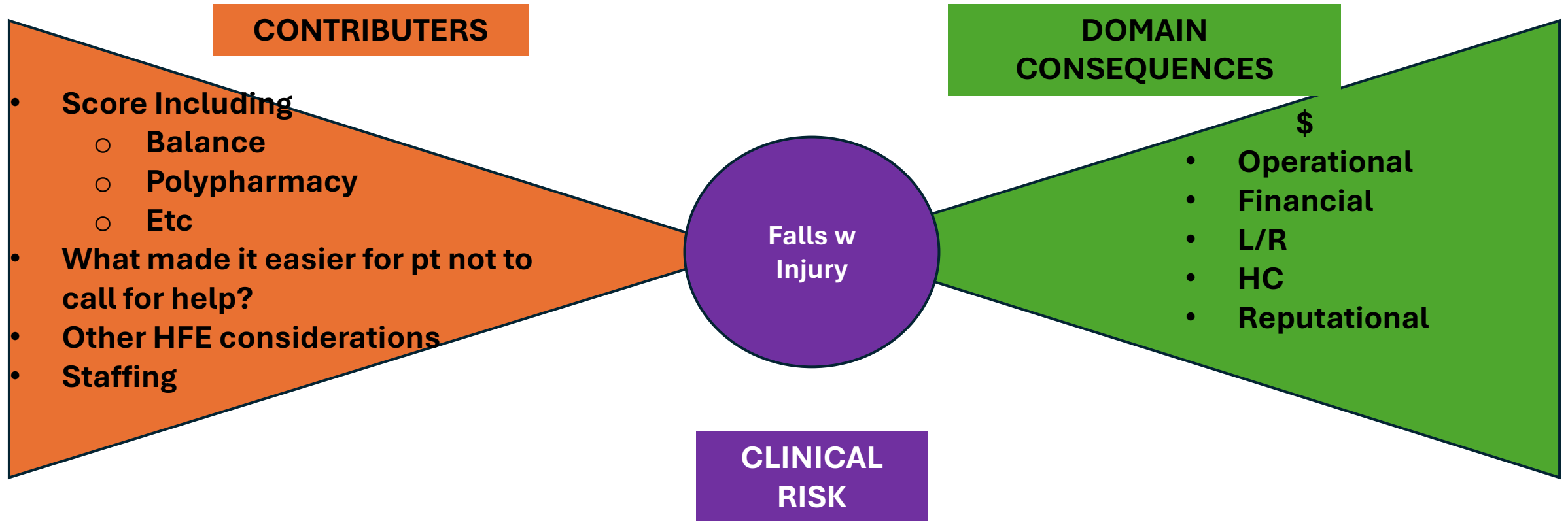
Financial:

- Increased LOS
- Unreimbursed
- Claims Cost

Operational:

- Falls scoring
- Process change
- HFE
- Documentation

What domains for falls with injury?



Falls with injury should not be framed solely a patient safety or nursing issue. Falls with injury creates consequences across multiple enterprise domains, including operational performance, regulatory compliance, financial outcomes, workforce considerations, and organizational reputation.

Assessing Risk

- **Likelihood:** Use range/numbers. This may be expressed in terms of a probability or frequency of occurring.
 - Define Almost Certain, Likely, etc.
 - E.g.: Likely to happen within next two/five/ten years, etc.
- **Velocity:** How quickly a risk moves from early warning signs to significant organizational impact
 - E.g.: Hours to days, Days to weeks, Months
- **Impact:** The result or the effect of a risk. There may be a range of possible impacts associated with a risk.
 - Define Critical, Major, Moderate in dollars
 - E.g.: <\$1 million, \$1–5 million, etc.

Sample Formulas

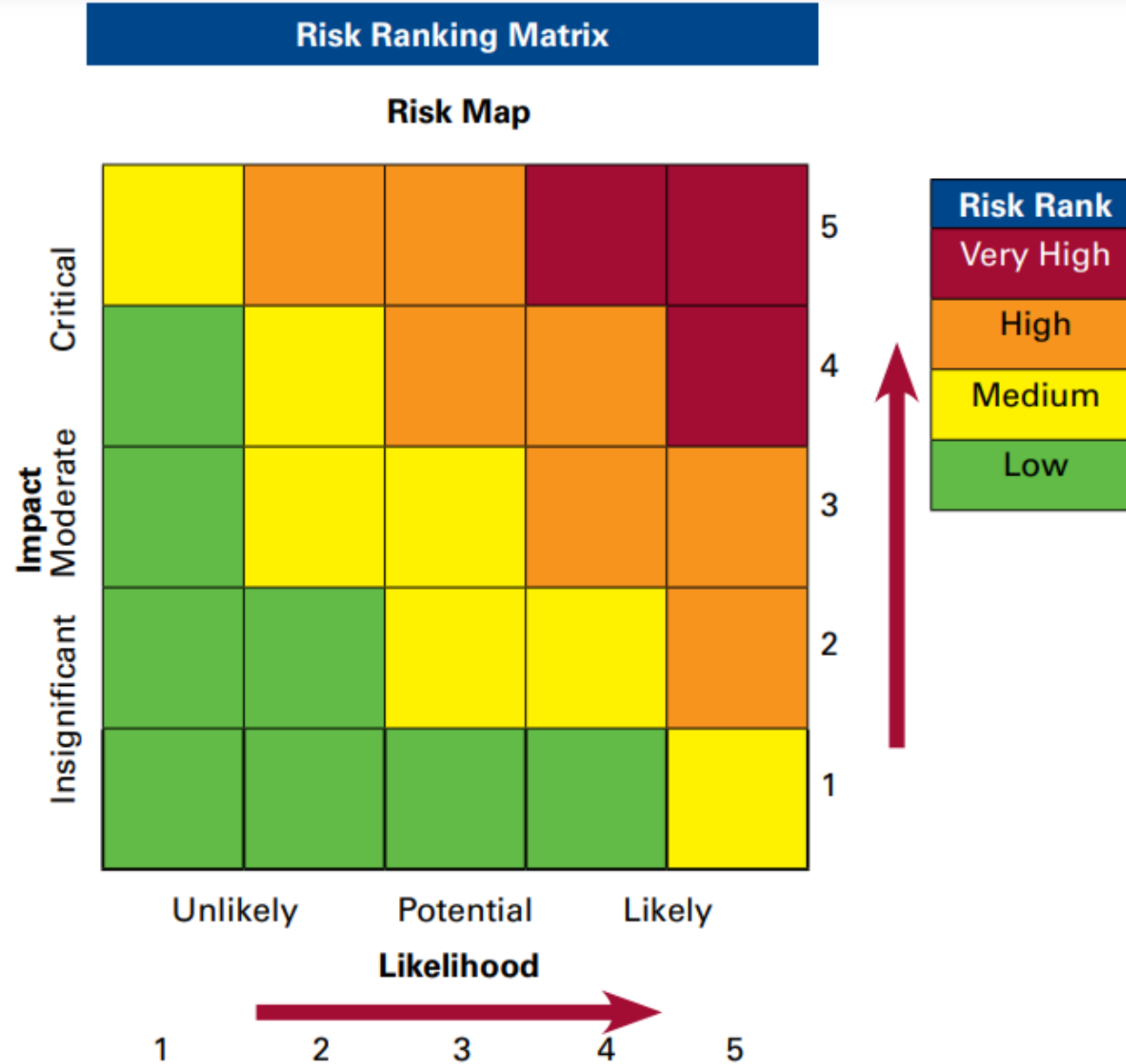
Likelihood	x	Impact	=	Risk Score
(a value 1 to 5)		(a value 1 to 5)		
1	x	1	=	1 (lowest possible score)
5	x	5	=	25 (highest possible score)

(Likelihood + Velocity)	x	Impact	=	Risk Score
(a value 1 to 5)	(a value 1 to 3)	(a value 1 to 5)		
(1 + 1)	x	1	=	2 (lowest possible score)
(5 + 3)	x	5	=	40 (highest possible score)

Risk Register and Scoring Template

Identified Risk	Description & Metrics (data used to trend risk)	Likelihood	Velocity	Impact	Total	Domain(s)	Owner
Risk Title	Risk statement + metric(s)	On a scale of 1-5, how likely is this risk to occur? 1 = very unlikely 2 = unlikely 3 = possible 4 = likely 5 = very likely	On a scale of 1-3, with 3 being the fastest moving for the risk to materialize and have impact: 3 – Hours to Days 2 – Days to Weeks 1 – Weeks to Months/Years	On a scale of 1-5, how significant is the impact if the risk is not controlled? 1 = negligible 2 = minor 3 = moderate 4 = significant 5 = severe	(Likelihood + Velocity) x Impact	Operational Clinical Financial Human Capital Technology Reputational	Leader accountable for performance results

Score and prioritize in a heat map



Place in a 2x2

Risk exposure

Continuous Monitoring & Improvement	Prioritize Focus & Resources
Business as Usual	See Opportunities for Improvement

RISK RESPONSE GAP

DQ

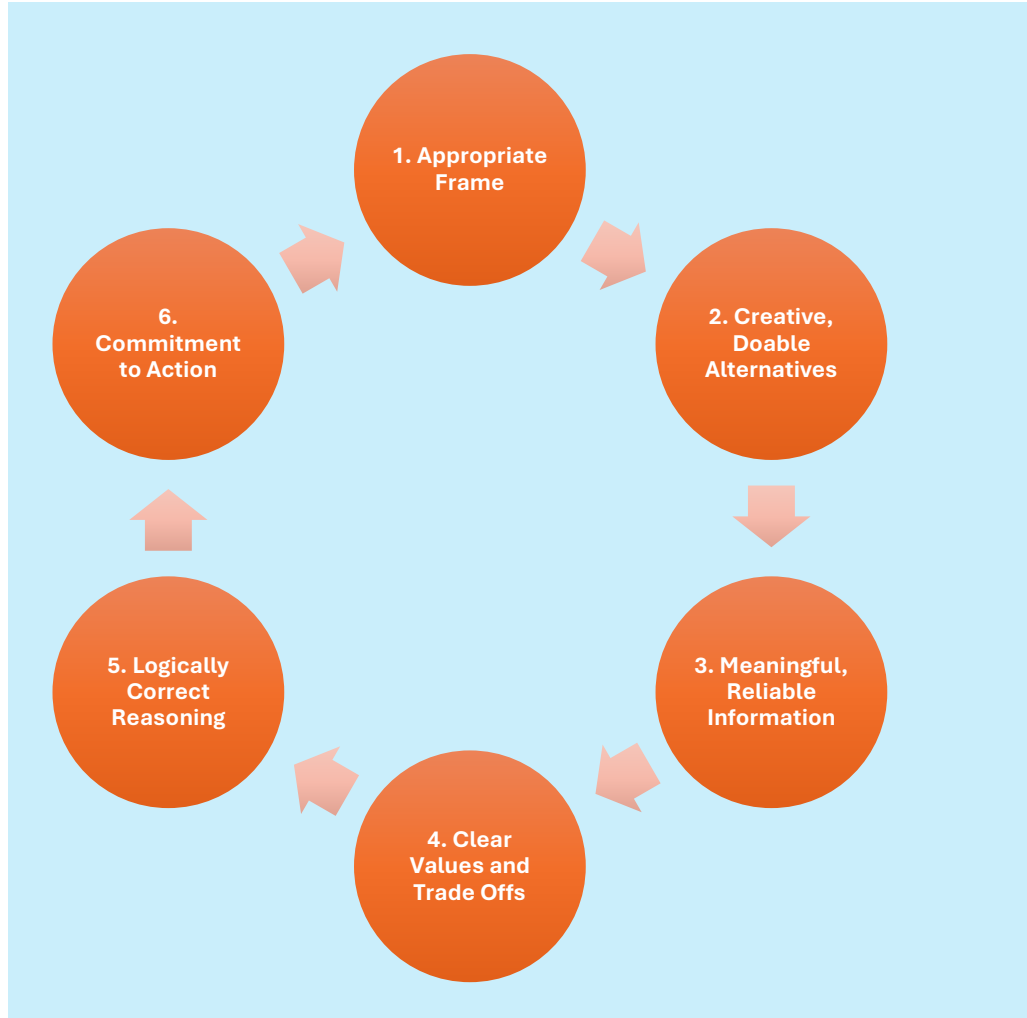
- Brings rigor, structure, and analytical clarity to complex problems
 - Analyze organizational, analytical, content complexity
- But the biggest obstacle to better decisions is rarely the framework
- It's the human on the other side of the table. Challenges:
 - When stakeholders feel unheard, misunderstood
 - Don't see the connecting thread about how DQ helps solve their actual problem

Decision Quality

- Brings rigor, structure, and analytical clarity to complex problems
 - Analyze organizational, analytical, content complexity
- But the biggest obstacle to better decisions is rarely the framework
- It's the human on the other side of the table. Challenges:
 - When stakeholders feel unheard, misunderstood
 - Don't see the connecting thread about how DQ helps solve their actual problem

Steps

Six steps in the decision quality (DQ) process



1. Appropriate frame (*What am I deciding?*)
2. Creative doable *alternatives* (*What are my choices?*)
3. Meaningful, reliable information (*What do I know?*)
4. Clear values and trade offs (*What consequences do I care about?*)
5. Logically correct reasoning (*Am I thinking straight about this?*)
6. Commitment to action (*Action = follow through*)

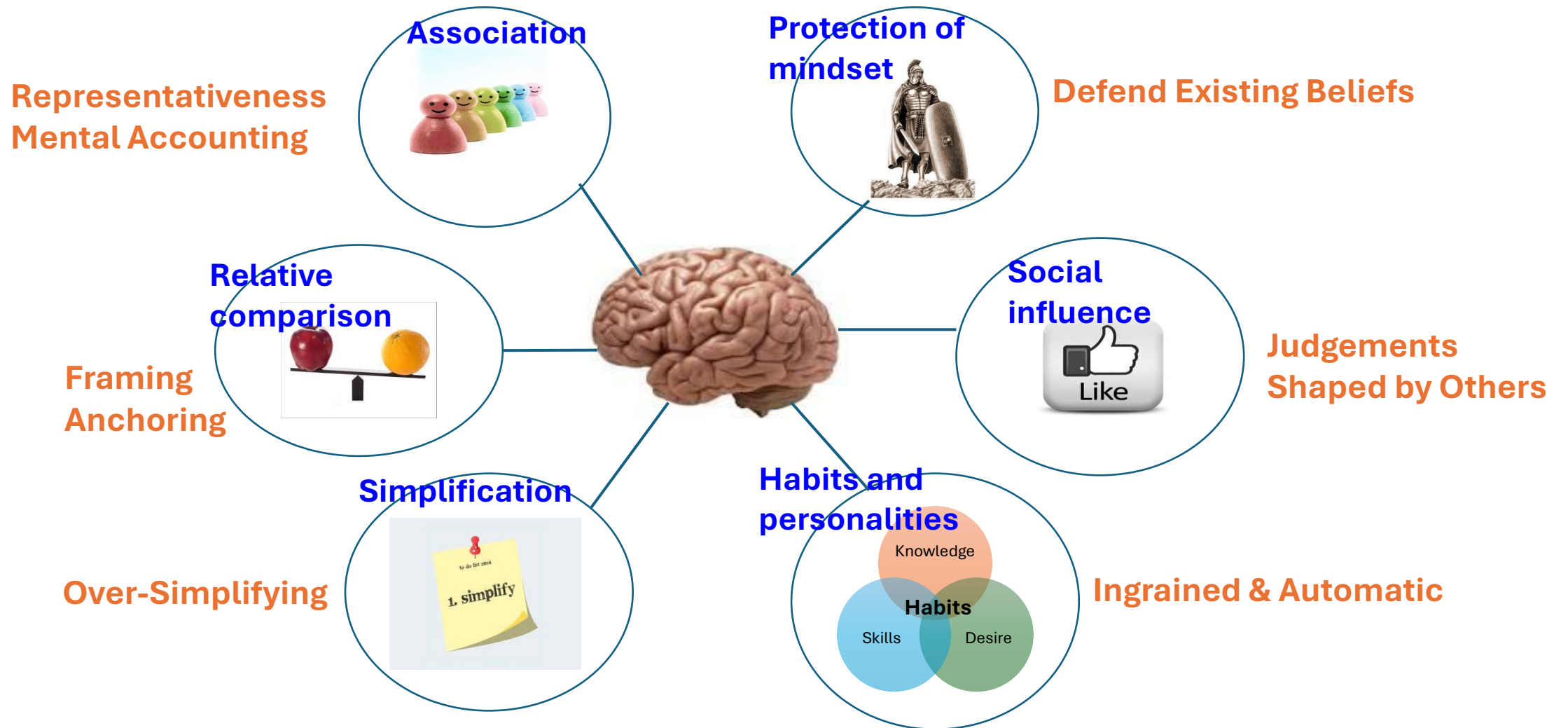
The objective is to achieve quality in each step to produce quality in the decision. You can think of these steps as 6 links in a chain. Stanford University and the SDG developed this analogy: If the chain has a weak link (meaning that it does not have quality in the step), the weakness will be transferred to the integrity of the chain and the decision will suffer that weakness.

DART

Decision Analysis Reserve Targeting Decision Analysis Reserve and Trial Strategy

- Purpose: replace intuition-driven malpractice reserving and litigation strategy with a formal, quantitative decision-analysis process that explicitly modeled uncertainty and downside risk in complex healthcare claims
- [Stanford Approach Helps Avoid Huge Verdict |... | Clinician.com](#)

Biases, uncertainty and probability



Application: AI CDSS

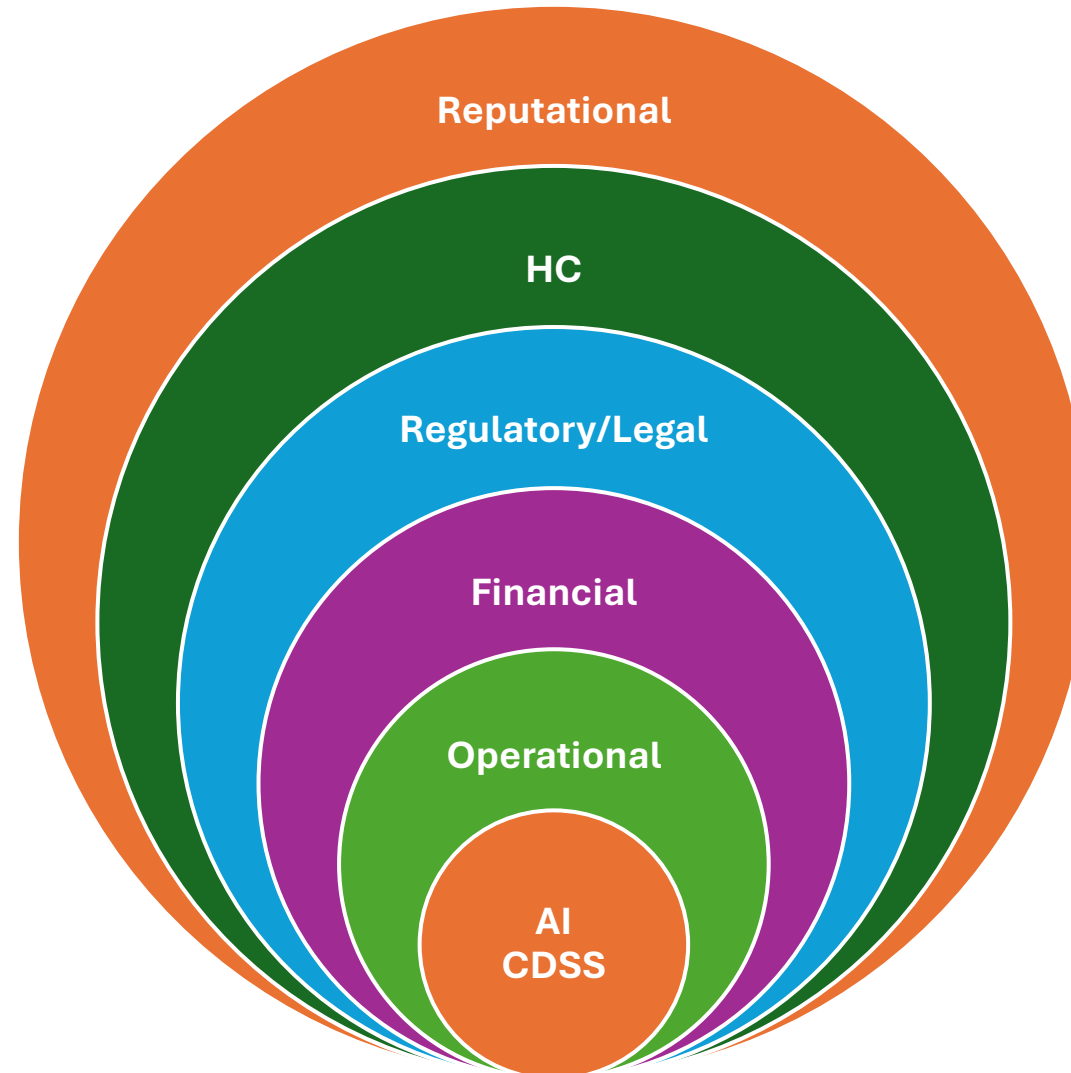
What domains for AI CDSS?

Reputational:

- Quality Ratings
- Patient Trust
- Clinical Confidence
- Public Perception of AI Use

HC:

- Human Oversight Expectations
- Training & Competency
- Cognitive Load/Alert Fatigue



Regulatory/Legal:

- FDA Considerations
- Privacy Security Data Use
- Survey & Accreditation Scrutiny

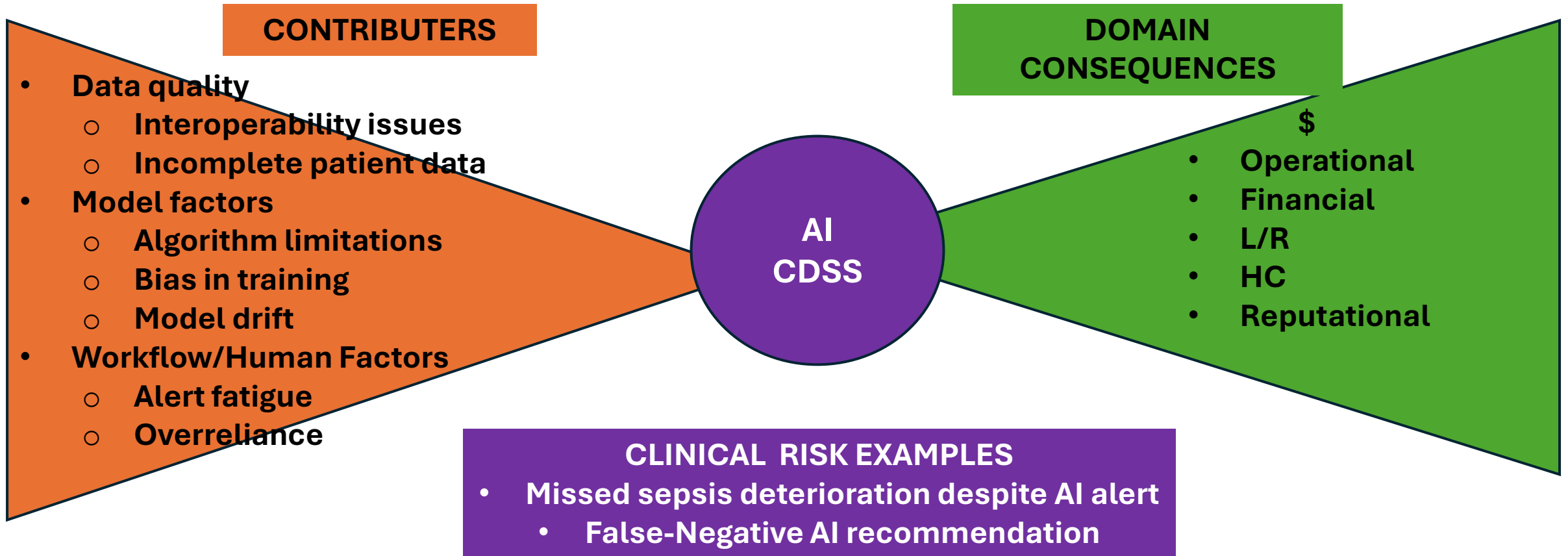
Financial:

- Implementation & Maintenance Cost
- Claims & Litigation Cost

Operational:

- Model Monitoring & Drift
- Escalation Pathways
- Downtime or Override Process

What domains for AI CDSS?



AI CDSS should not be framed as only a technology or clinical workflow issue. Like “***falls with injury***”, AI CDSS creates risk and value across multiple enterprise domains. A single inaccurate, poorly timed, poorly understood, or poorly governed AI recommendation may affect patient safety, clinician workflow, regulatory posture, liability exposure, cost a, and trust.

Using domains helps ensure the organization evaluates not only the tool itself, but the broader system in which the tool is deployed.

AI-specific event categories that support learning and improvement

- AI Prediction Error (false positive, false negative, calibration issues)
- Human-AI Decision-Making Error (automation bias, anchoring bias, inappropriate reliance)
- Alert Management Issues (alert fatigue, excessive alerts, ignored alerts)
- Bias and Equity Concerns (differential performance among patient populations)
- Governance and Oversight Failures (required review not completed, monitoring gaps)
- Technical and Integration Failures (data quality issues, interface failures, model deployment errors)

Capture both adverse events and successful human intervention

- AI-related adverse events
- AI-related near misses
- Unsafe conditions involving AI
- Good catches where human oversight prevented harm
- Workflow inefficiencies associated with AI use