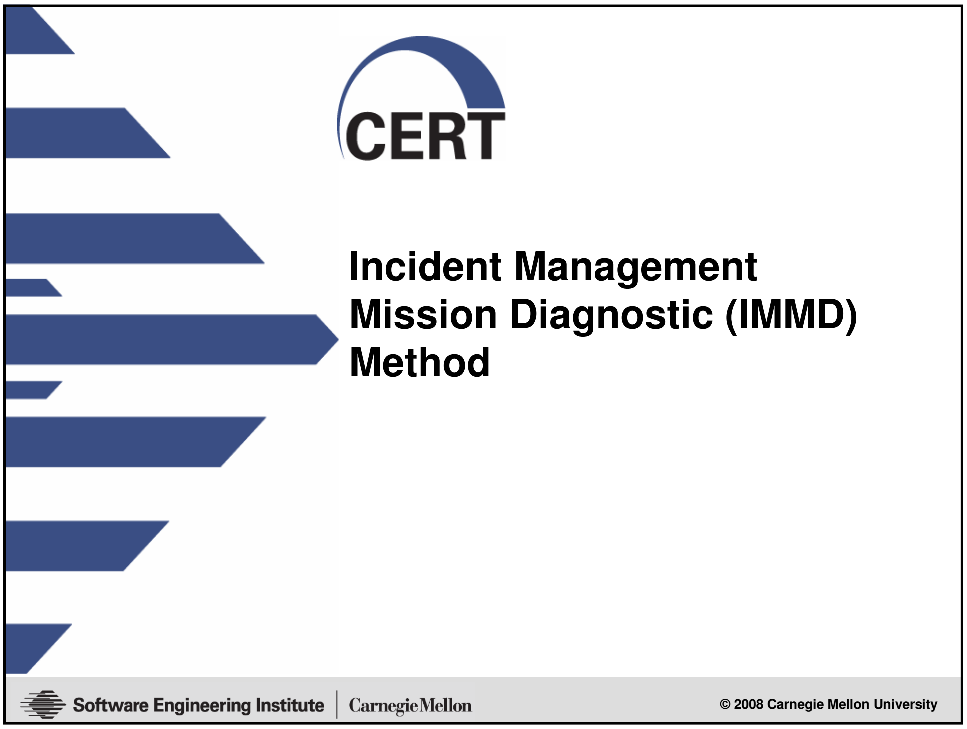
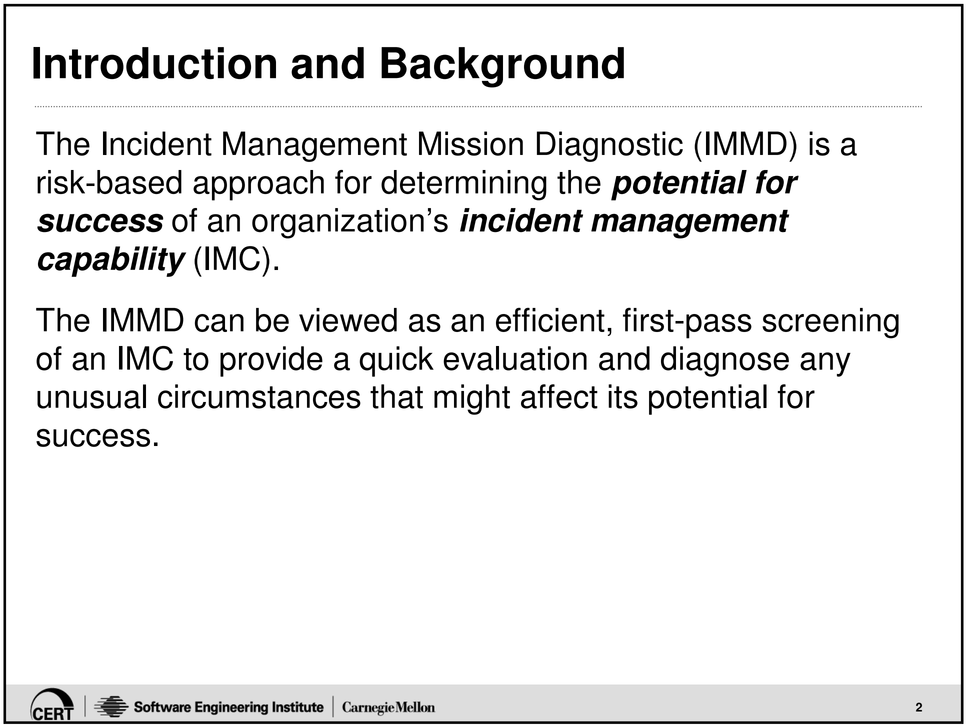


CERT

Incident Management Mission Diagnostic (IMMD) Method

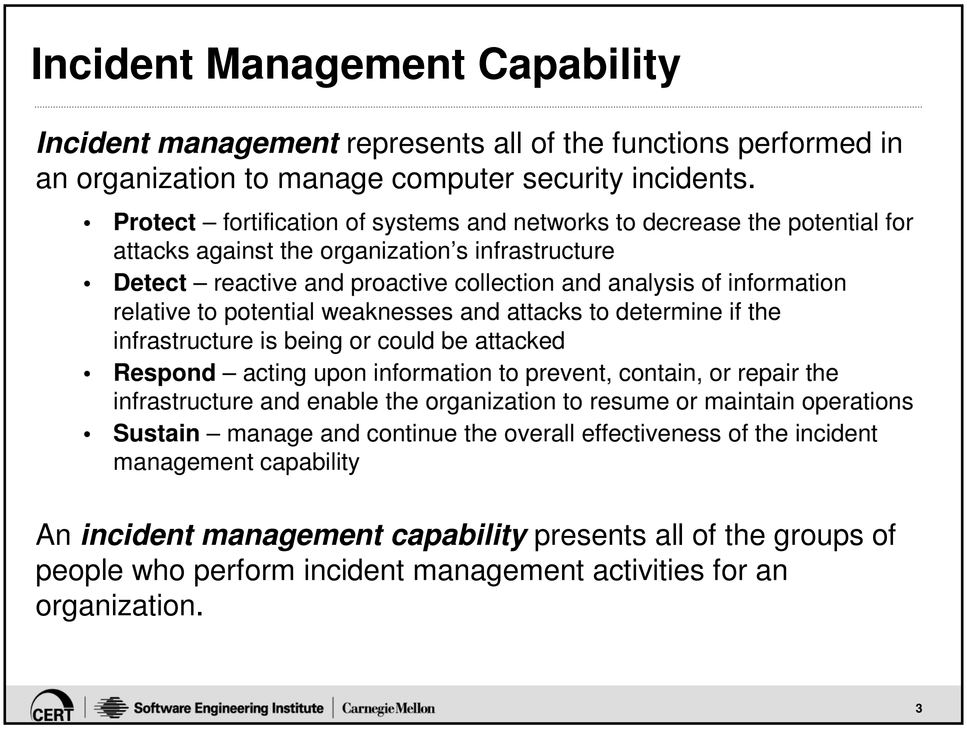
Software Engineering Institute | Carnegie Mellon



Introduction and Background

The Incident Management Mission Diagnostic (IMMD) is a risk-based approach for determining the ***potential for success*** of an organization's ***incident management capability*** (IMC).

The IMMD can be viewed as an efficient, first-pass screening of an IMC to provide a quick evaluation and diagnose any unusual circumstances that might affect its potential for success.

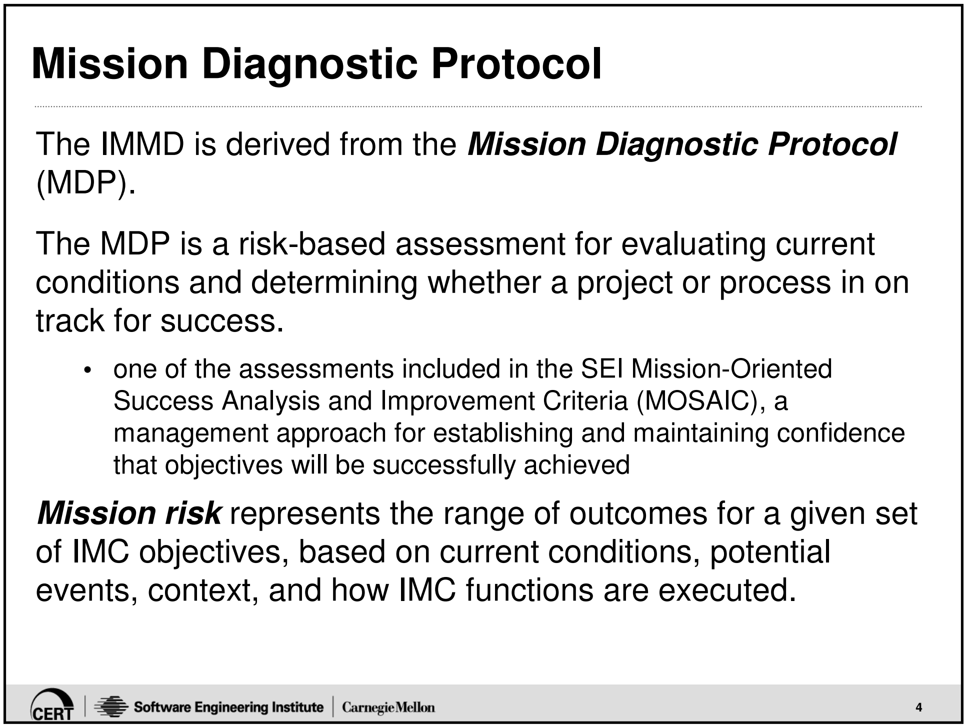


Incident Management Capability

Incident management represents all of the functions performed in an organization to manage computer security incidents.

- **Protect** – fortification of systems and networks to decrease the potential for attacks against the organization’s infrastructure
- **Detect** – reactive and proactive collection and analysis of information relative to potential weaknesses and attacks to determine if the infrastructure is being or could be attacked
- **Respond** – acting upon information to prevent, contain, or repair the infrastructure and enable the organization to resume or maintain operations
- **Sustain** – manage and continue the overall effectiveness of the incident management capability

An ***incident management capability*** presents all of the groups of people who perform incident management activities for an organization.



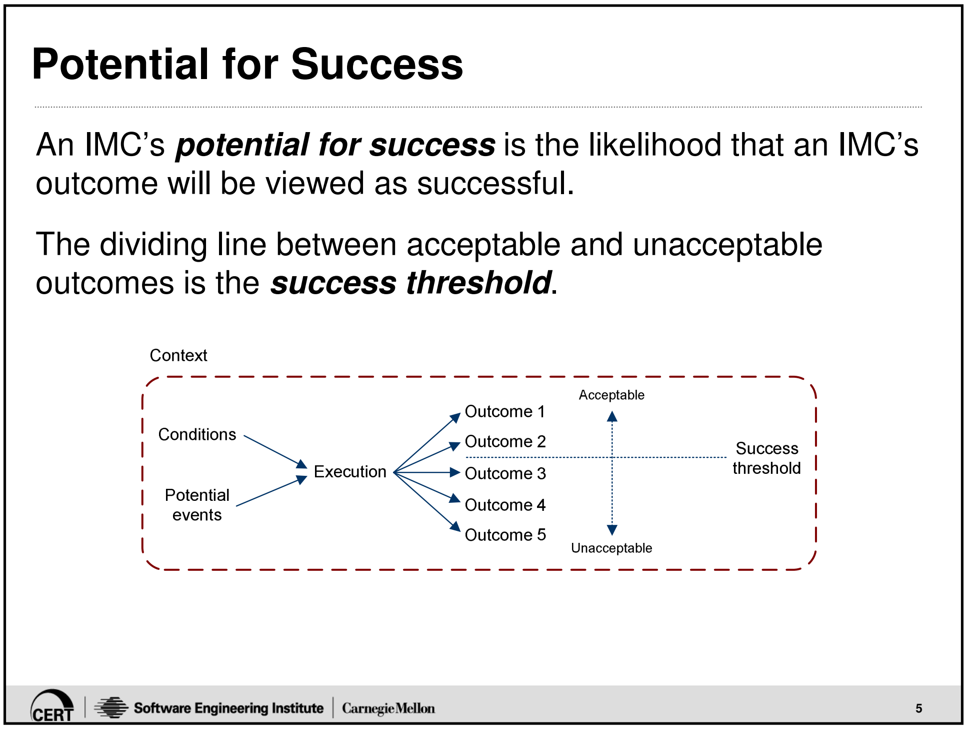
Mission Diagnostic Protocol

The IMMD is derived from the ***Mission Diagnostic Protocol*** (MDP).

The MDP is a risk-based assessment for evaluating current conditions and determining whether a project or process in on track for success.

- one of the assessments included in the SEI Mission-Oriented Success Analysis and Improvement Criteria (MOSAIC), a management approach for establishing and maintaining confidence that objectives will be successfully achieved

Mission risk represents the range of outcomes for a given set of IMC objectives, based on current conditions, potential events, context, and how IMC functions are executed.



Potential for Success

An IMC’s ***potential for success*** is the likelihood that an IMC’s outcome will be viewed as successful.

The dividing line between acceptable and unacceptable outcomes is the ***success threshold***.

Context

Conditions

Potential events

Execution

Outcome 1

Outcome 2

Outcome 3

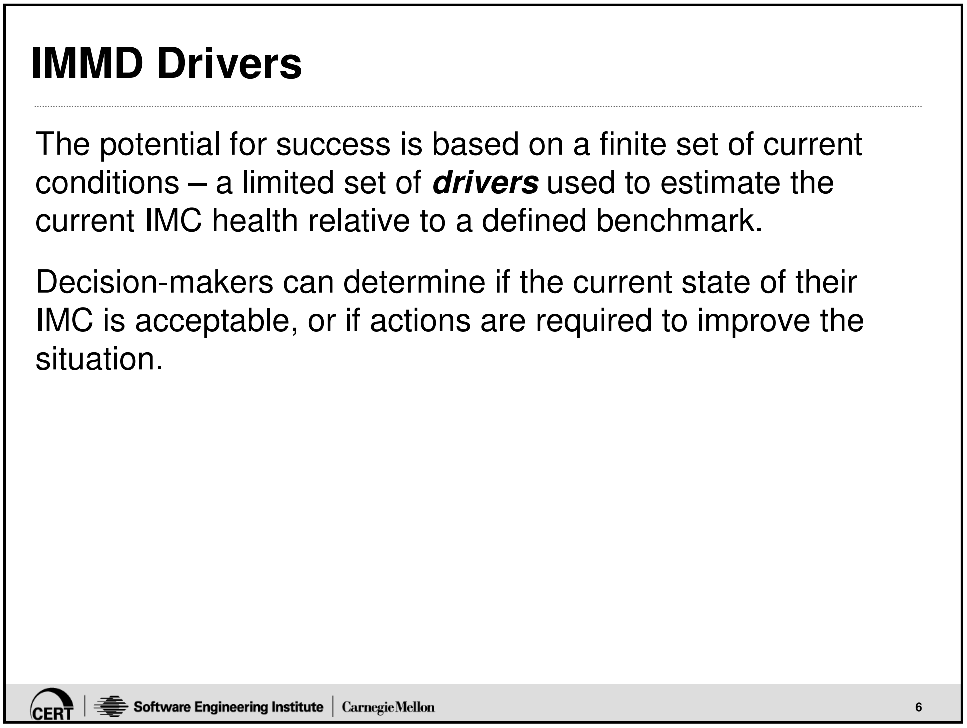
Outcome 4

Outcome 5

Acceptable

Success threshold

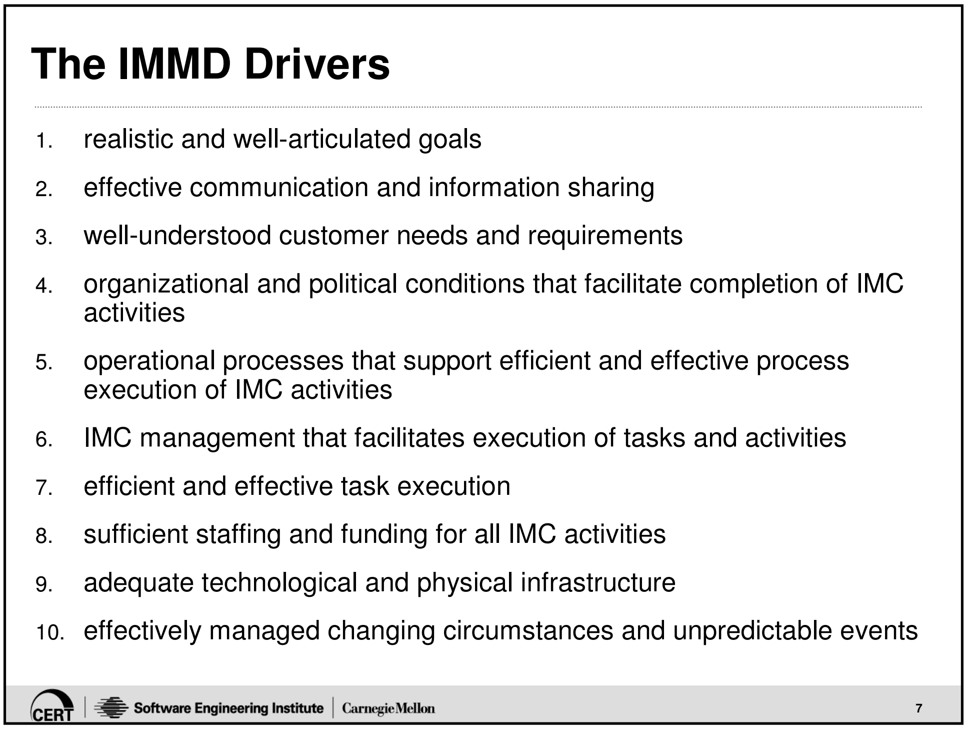
Unacceptable



IMMD Drivers

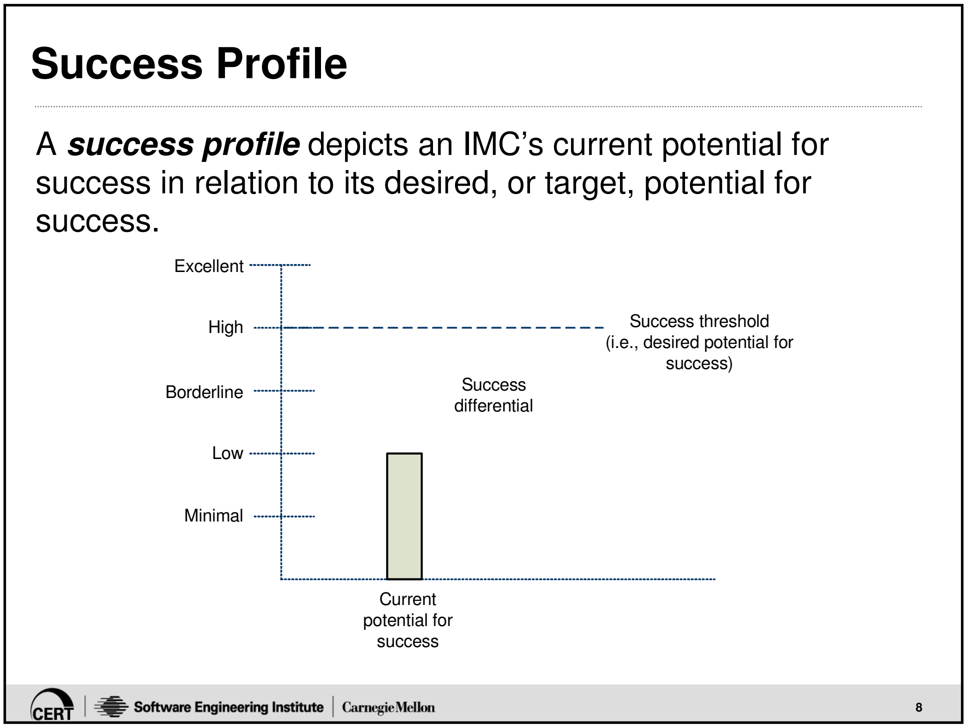
The potential for success is based on a finite set of current conditions – a limited set of ***drivers*** used to estimate the current IMC health relative to a defined benchmark.

Decision-makers can determine if the current state of their IMC is acceptable, or if actions are required to improve the situation.



The IMMD Drivers

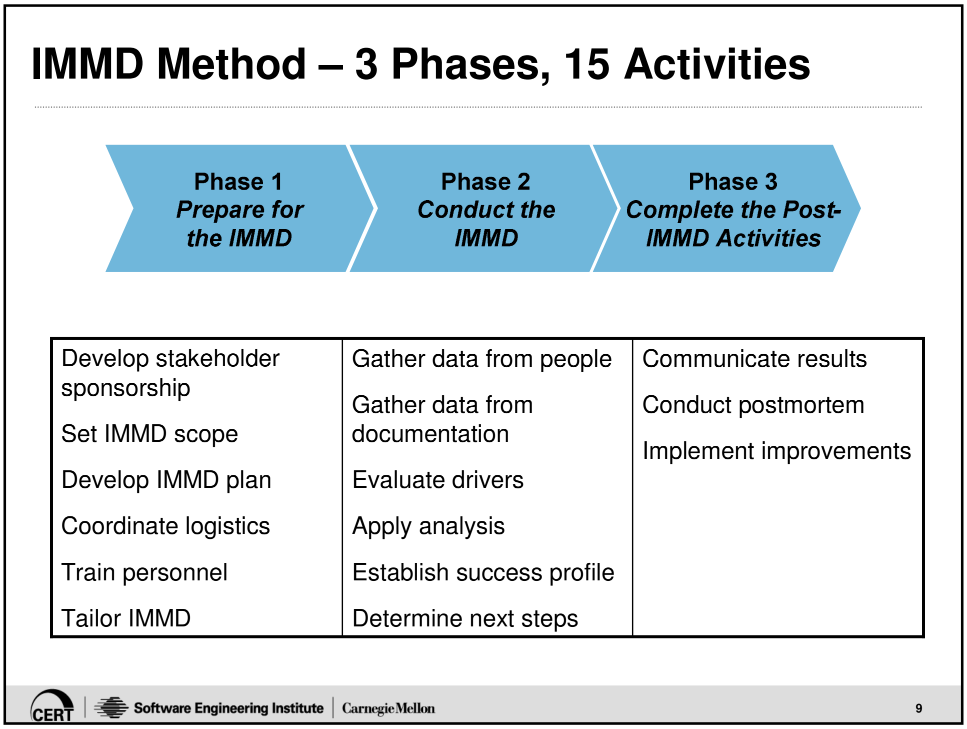
1. realistic and well-articulated goals
2. effective communication and information sharing
3. well-understood customer needs and requirements
4. organizational and political conditions that facilitate completion of IMC activities
5. operational processes that support efficient and effective process execution of IMC activities
6. IMC management that facilitates execution of tasks and activities
7. efficient and effective task execution
8. sufficient staffing and funding for all IMC activities
9. adequate technological and physical infrastructure
10. effectively managed changing circumstances and unpredictable events



Success Profile

A ***success profile*** depicts an IMC's current potential for success in relation to its desired, or target, potential for success.

Excellent
High
Borderline
Low
Minimal
Success threshold (i.e., desired potential for success)
Success differential
Current potential for success



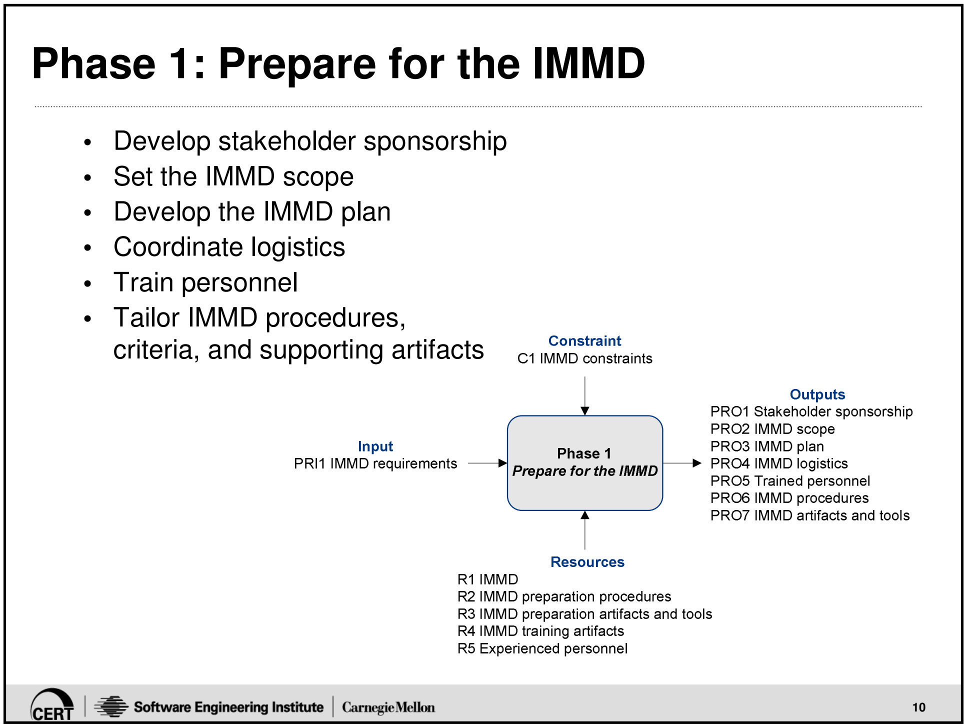
IMMD Method – 3 Phases, 15 Activities

Phase 1
Prepare for the IMMD

Phase 2
Conduct the IMMD

Phase 3
Complete the Post-IMMD Activities

Develop stakeholder sponsorship	Gather data from people	Communicate results
Set IMMD scope	Gather data from documentation	Conduct postmortem
Develop IMMD plan	Evaluate drivers	Implement improvements
Coordinate logistics	Apply analysis	
Train personnel	Establish success profile	
Tailor IMMD	Determine next steps	



Phase 1: Prepare for the IMMD

- Develop stakeholder sponsorship
- Set the IMMD scope
- Develop the IMMD plan
- Coordinate logistics
- Train personnel
- Tailor IMMD procedures, criteria, and supporting artifacts

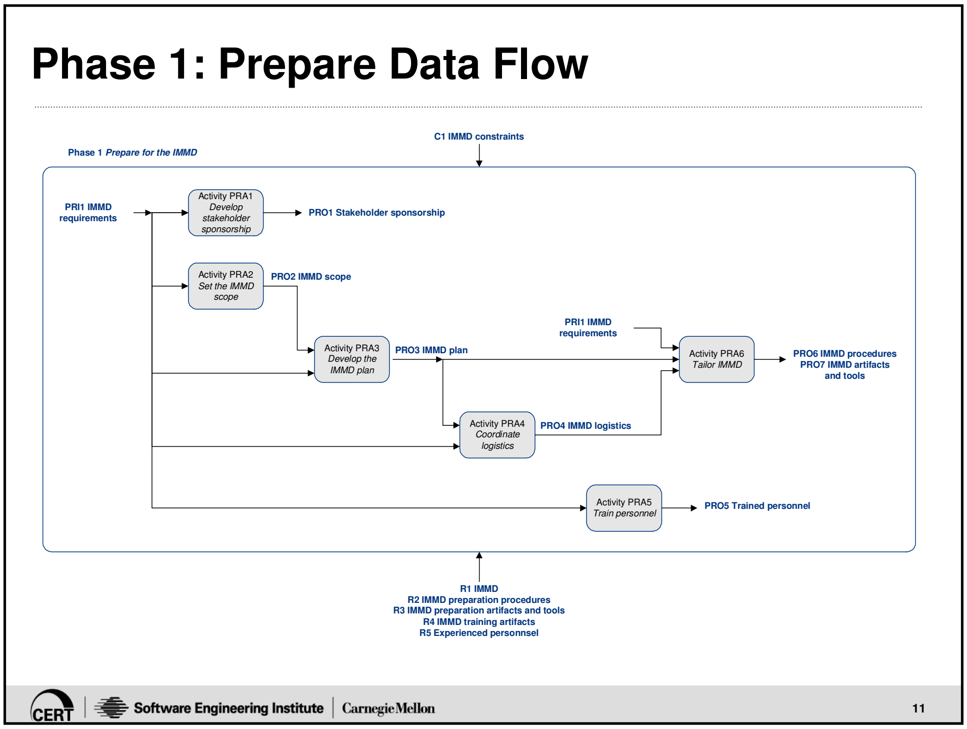
Constraint
C1 IMMD constraints

Input
PRI1 IMMD requirements

Phase 1
Prepare for the IMMD

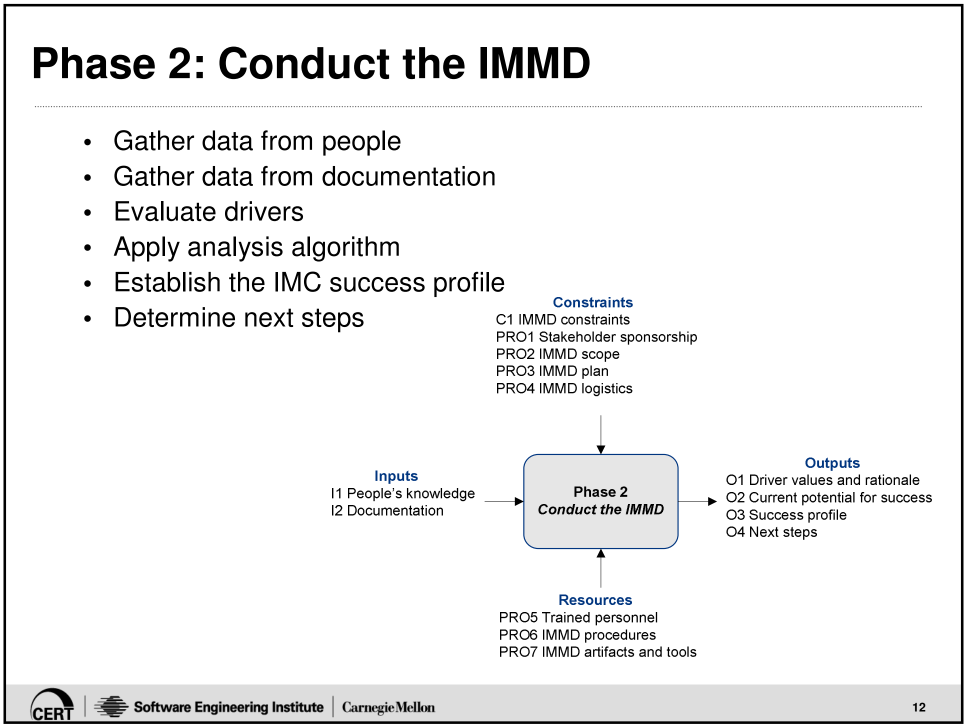
Outputs
PRO1 Stakeholder sponsorship
PRO2 IMMD scope
PRO3 IMMD plan
PRO4 IMMD logistics
PRO5 Trained personnel
PRO6 IMMD procedures
PRO7 IMMD artifacts and tools

Resources
R1 IMMD
R2 IMMD preparation procedures
R3 IMMD preparation artifacts and tools
R4 IMMD training artifacts
R5 Experienced personnel



Phase 1: Prepare Data Flow

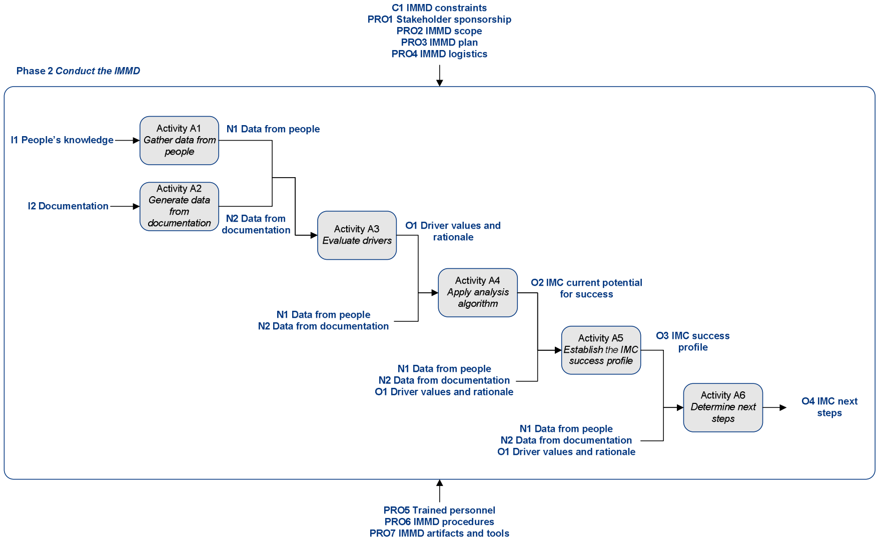
C1 IMMD constraints
Phase 1 *Prepare for the IMMD*
PRI1 IMMD requirements
Activity PRA1 *Develop stakeholder sponsorship*
PRO1 Stakeholder sponsorship
Activity PRA2 *Set the IMMD scope*
PRO2 IMMD scope
PRI1 IMMD requirements
Activity PRA3 *Develop the IMMD plan*
PRO3 IMMD plan
Activity PRA6 *Tailor IMMD*
PRO6 IMMD procedures
PRO7 IMMD artifacts and tools
Activity PRA4 *Coordinate logistics*
PRO4 IMMD logistics
Activity PRA5 *Train personnel*
PRO5 Trained personnel
R1 IMMD
R2 IMMD preparation procedures
R3 IMMD preparation artifacts and tools
R4 IMMD training artifacts
R5 Experienced personnsel



Phase 2: Conduct the IMMD

- Gather data from people
- Gather data from documentation
- Evaluate drivers
- Apply analysis algorithm
- Establish the IMC success profile
- Determine next steps

Phase 2: Conduct IMMD Data Flow



C1 IMMD constraints
PRO1 Stakeholder sponsorship
PRO2 IMMD scope
PRO3 IMMD plan
PRO4 IMMD logistics

Phase 2 *Conduct the IMMD*

I1 People's knowledge

Activity A1
Gather data from people

N1 Data from people

I2 Documentation

Activity A2
Generate data from documentation

N2 Data from documentation

Activity A3
Evaluate drivers

O1 Driver values and rationale

N1 Data from people
N2 Data from documentation

Activity A4
Apply analysis algorithm

O2 IMC current potential for success

N1 Data from people
N2 Data from documentation
O1 Driver values and rationale

Activity A5
Establish the IMC success profile

O3 IMC success profile

N1 Data from people
N2 Data from documentation
O1 Driver values and rationale

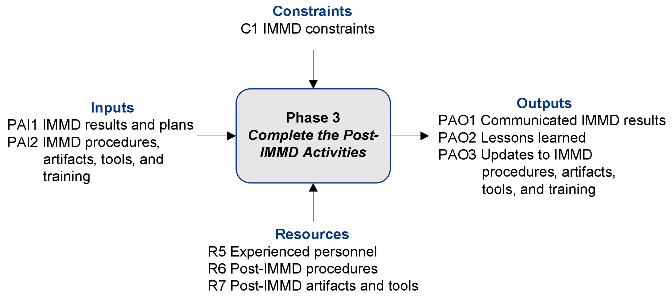
Activity A6
Determine next steps

O4 IMC next steps

PRO5 Trained personnel
PRO6 IMMD procedures
PRO7 IMMD artifacts and tools

Phase 3: Complete the Post-IMMD Activities

- Communicate results
- Conduct postmortem of the IMMD
- Implement improvements to the IMMD process



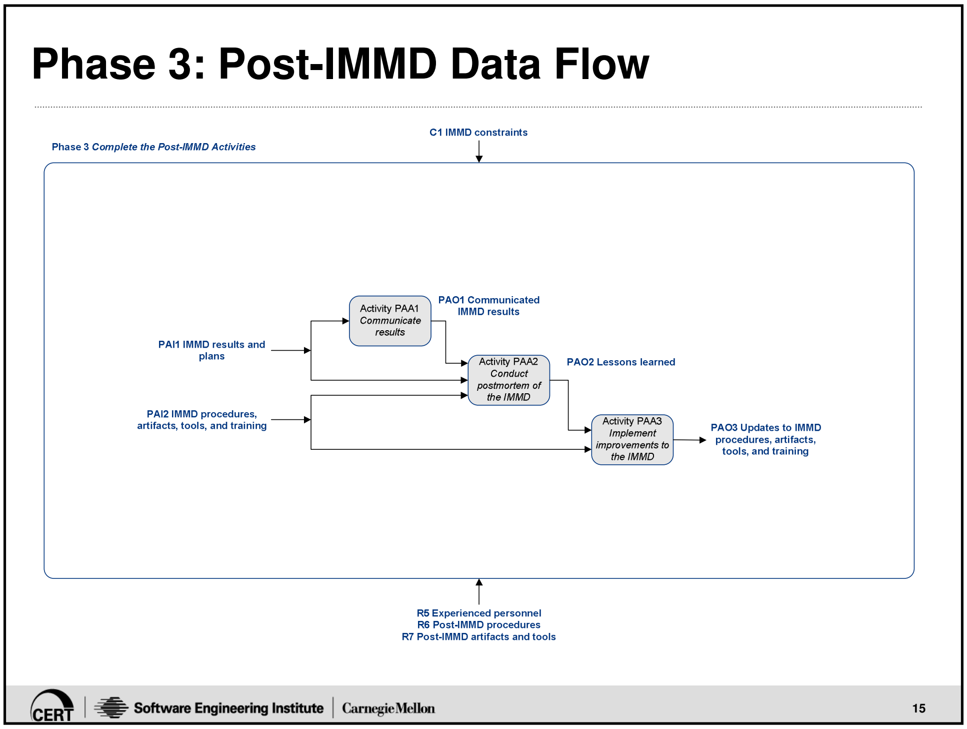
Constraints
C1 IMMD constraints

Inputs
PAI1 IMMD results and plans
PAI2 IMMD procedures, artifacts, tools, and training

Phase 3
Complete the Post-IMMD Activities

Outputs
PAO1 Communicated IMMD results
PAO2 Lessons learned
PAO3 Updates to IMMD procedures, artifacts, tools, and training

Resources
R5 Experienced personnel
R6 Post-IMMD procedures
R7 Post-IMMD artifacts and tools



Phase 3: Post-IMMD Data Flow

C1 IMMD constraints

Phase 3 *Complete the Post-IMMD Activities*

PAI1 IMMD results and plans

PAI2 IMMD procedures, artifacts, tools, and training

Activity PAA1 *Communicate results*

PAO1 Communicated IMMD results

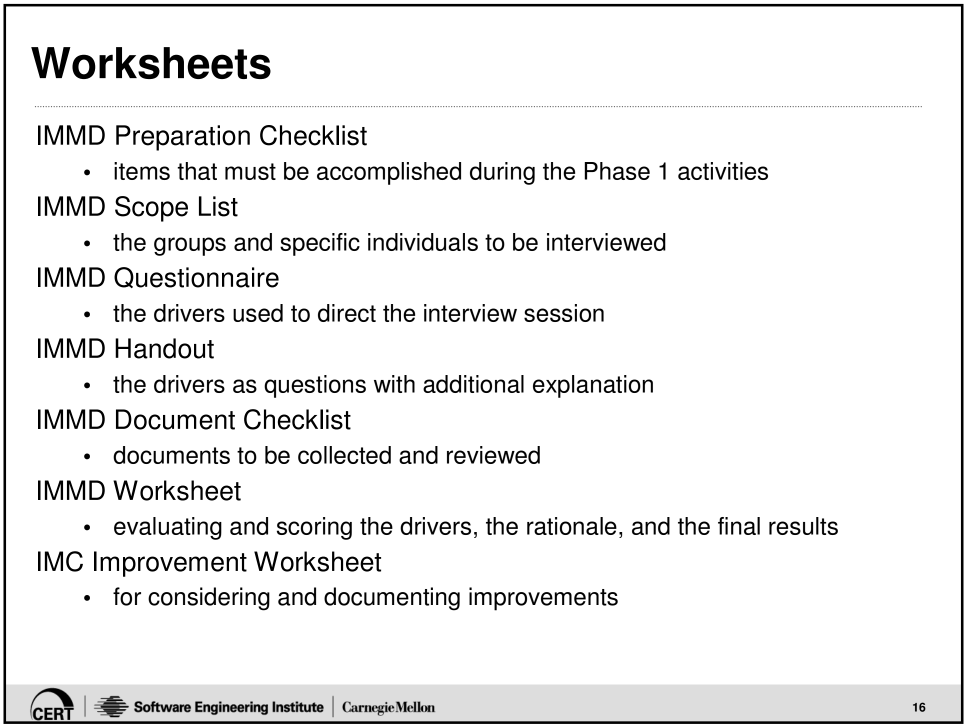
Activity PAA2 *Conduct postmortem of the IMMD*

PAO2 Lessons learned

Activity PAA3 *Implement improvements to the IMMD*

PAO3 Updates to IMMD procedures, artifacts, tools, and training

R5 Experienced personnel
R6 Post-IMMD procedures
R7 Post-IMMD artifacts and tools



Worksheets

IMMD Preparation Checklist

- items that must be accomplished during the Phase 1 activities

IMMD Scope List

- the groups and specific individuals to be interviewed

IMMD Questionnaire

- the drivers used to direct the interview session

IMMD Handout

- the drivers as questions with additional explanation

IMMD Document Checklist

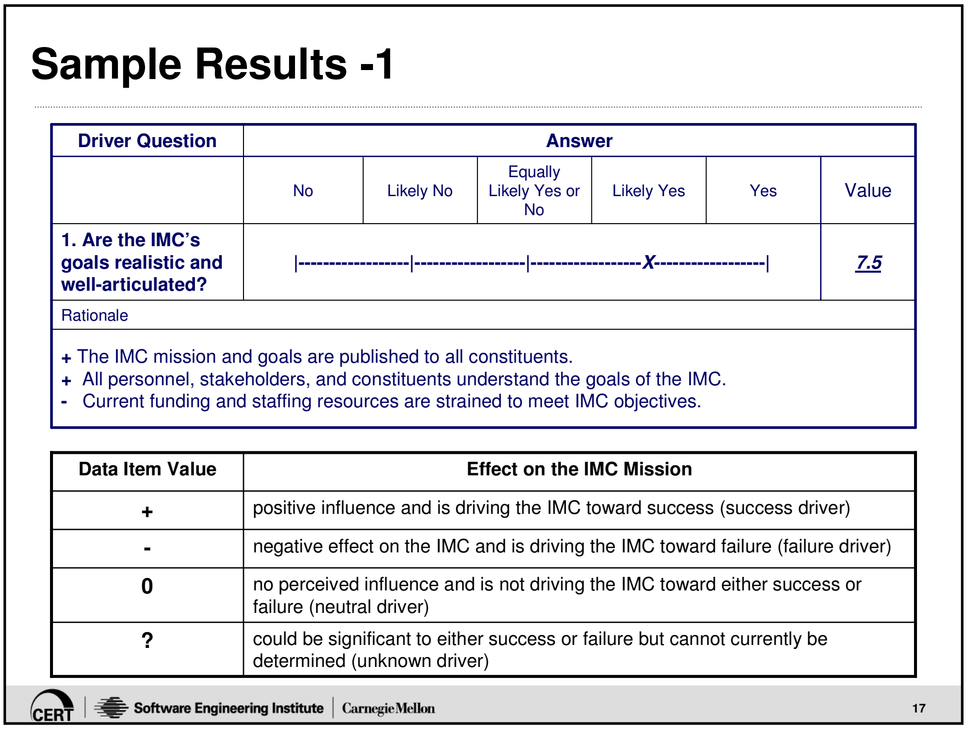
- documents to be collected and reviewed

IMMD Worksheet

- evaluating and scoring the drivers, the rationale, and the final results

IMC Improvement Worksheet

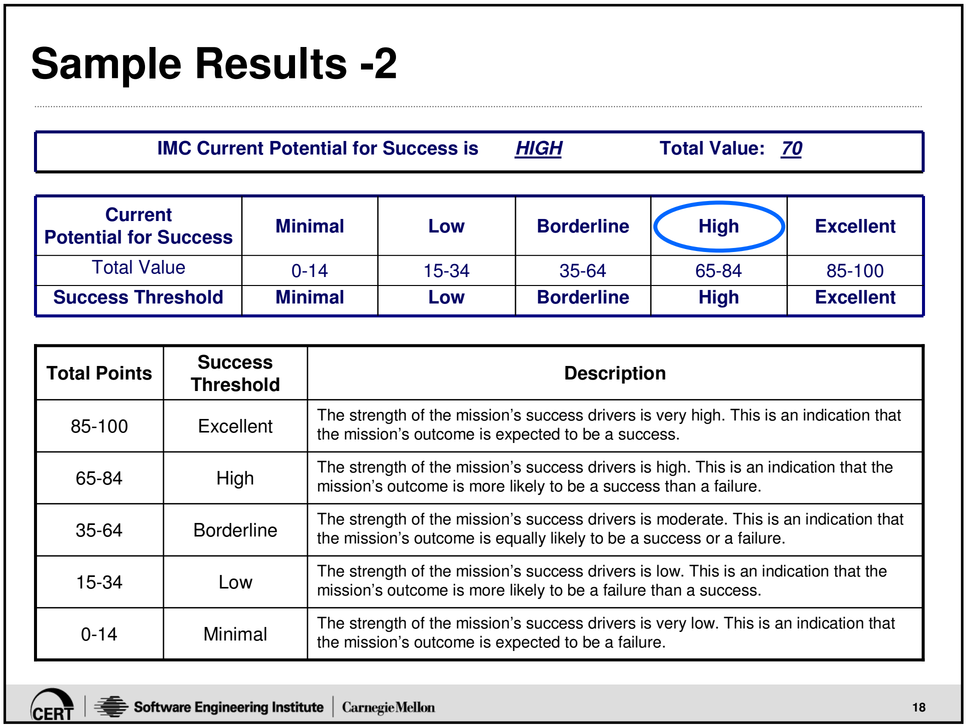
- for considering and documenting improvements



Sample Results -1

<table>
<tr><th>Driver Question</th><th colspan="6">Answer</th></tr>
<tr><td></td><td>No</td><td>Likely No</td><td>Equally Likely Yes or No</td><td>Likely Yes</td><td>Yes</td><td>Value</td></tr>
<tr><td><b>1. Are the IMC’s goals realistic and well-articulated?</b></td><td colspan="5">|------------------|------------------|------------------X------------------|</td><td><i>7.5</i></td></tr>
<tr><td colspan="7">Rationale</td></tr>
<tr><td colspan="7">+ The IMC mission and goals are published to all constituents.
+ All personnel, stakeholders, and constituents understand the goals of the IMC.
- Current funding and staffing resources are strained to meet IMC objectives.</td></tr>
</table>

Data Item Value	Effect on the IMC Mission
+	positive influence and is driving the IMC toward success (success driver)
-	negative effect on the IMC and is driving the IMC toward failure (failure driver)
0	no perceived influence and is not driving the IMC toward either success or failure (neutral driver)
?	could be significant to either success or failure but cannot currently be determined (unknown driver)

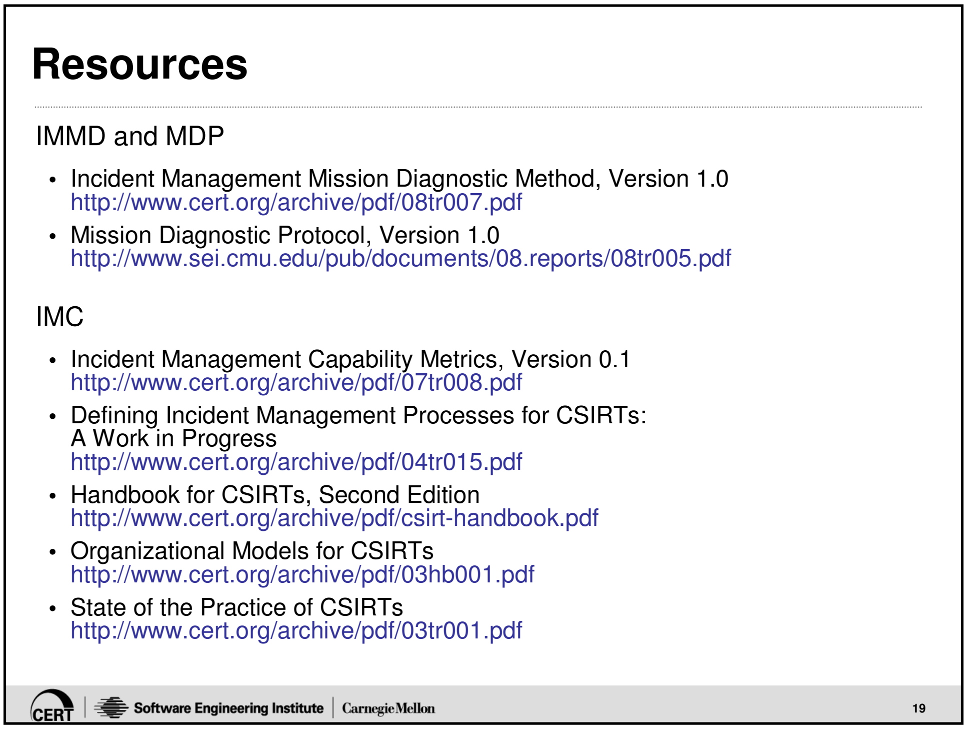


Sample Results -2

IMC Current Potential for Success is *HIGH*   Total Value: *70*

Current Potential for Success	Minimal	Low	Borderline	[✓ High]	Excellent
Total Value	0-14	15-34	35-64	65-84	85-100
Success Threshold	**Minimal**	**Low**	**Borderline**	**High**	**Excellent**

Total Points	Success Threshold	Description
85-100	Excellent	The strength of the mission’s success drivers is very high. This is an indication that the mission’s outcome is expected to be a success.
65-84	High	The strength of the mission’s success drivers is high. This is an indication that the mission’s outcome is more likely to be a success than a failure.
35-64	Borderline	The strength of the mission’s success drivers is moderate. This is an indication that the mission’s outcome is equally likely to be a success or a failure.
15-34	Low	The strength of the mission’s success drivers is low. This is an indication that the mission’s outcome is more likely to be a failure than a success.
0-14	Minimal	The strength of the mission’s success drivers is very low. This is an indication that the mission’s outcome is expected to be a failure.



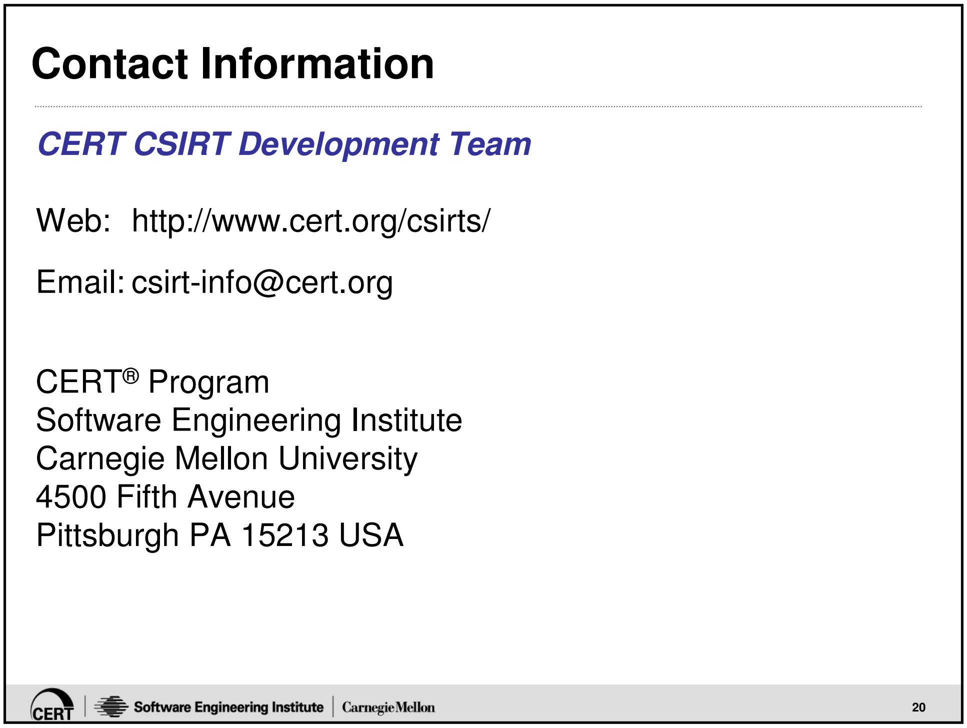
Resources

IMMD and MDP

- Incident Management Mission Diagnostic Method, Version 1.0
  http://www.cert.org/archive/pdf/08tr007.pdf
- Mission Diagnostic Protocol, Version 1.0
  http://www.sei.cmu.edu/pub/documents/08.reports/08tr005.pdf

IMC

- Incident Management Capability Metrics, Version 0.1
  http://www.cert.org/archive/pdf/07tr008.pdf
- Defining Incident Management Processes for CSIRTs:
  A Work in Progress
  http://www.cert.org/archive/pdf/04tr015.pdf
- Handbook for CSIRTs, Second Edition
  http://www.cert.org/archive/pdf/csirt-handbook.pdf
- Organizational Models for CSIRTs
  http://www.cert.org/archive/pdf/03hb001.pdf
- State of the Practice of CSIRTs
  http://www.cert.org/archive/pdf/03tr001.pdf



Contact Information

CERT CSIRT Development Team

Web: http://www.cert.org/csirts/

Email: csirt-info@cert.org

CERT® Program
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA 15213 USA