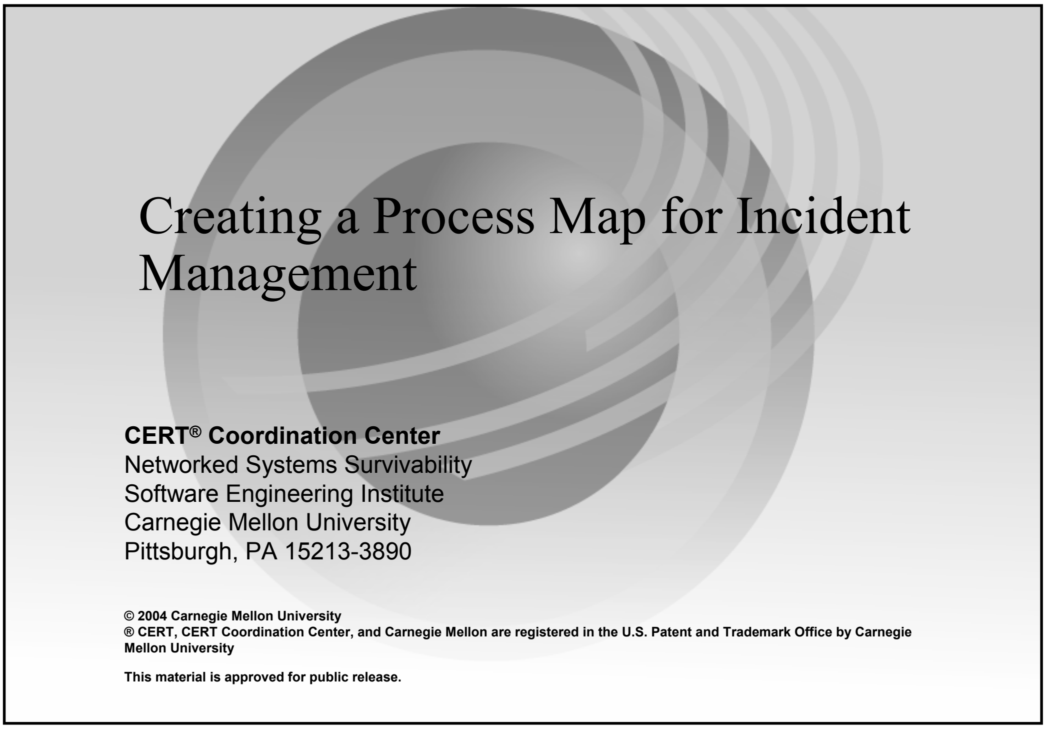
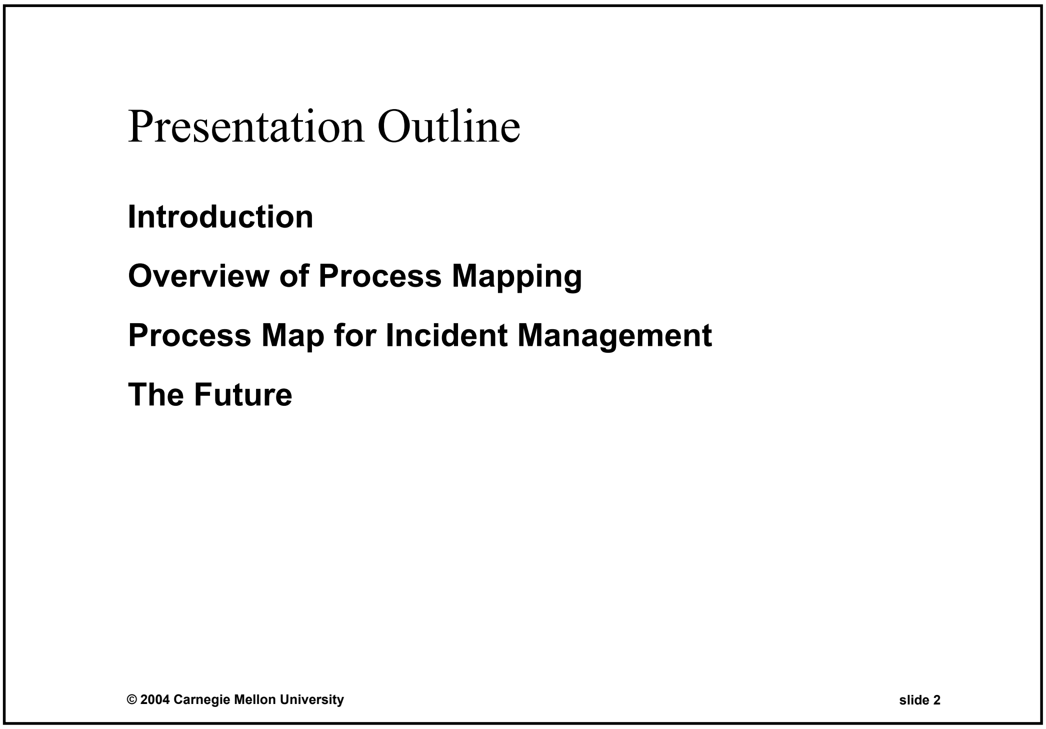


Creating a Process Map for Incident Management

CERT® Coordination Center
Networked Systems Survivability
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

This material is approved for public release.



Presentation Outline

Introduction

Overview of Process Mapping

Process Map for Incident Management

The Future

Introduction

Project Description

Project Team Members

Project Methodology

Project Requirements

Related Work

History and Rationale of CSIRT Mapping Project

The CSIRT Process Mapping "Process"

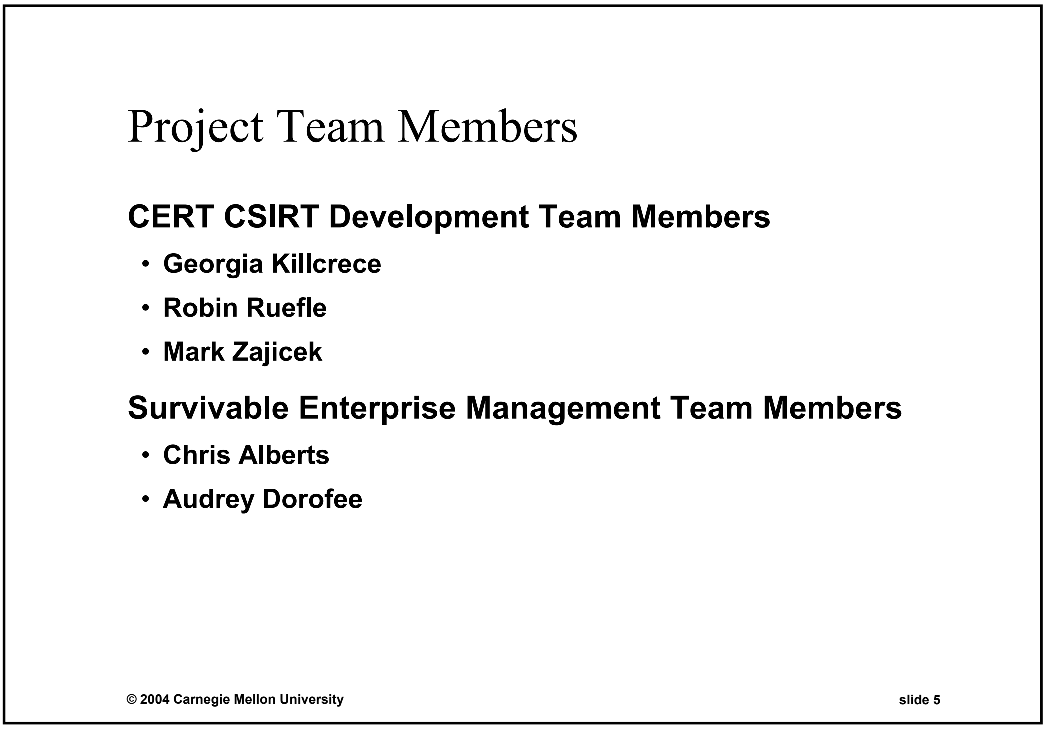
Current Status

Project Description

New work being done by the CERT CSIRT Development Team includes the development of an assessment methodology for CSIRTs.

This methodology and resulting assessment instrument will enable teams to evaluate their incident management performance for the following processes: Protect, Prepare, Detect, Triage and Respond.

The project is informally called: The CSIRT Assessment Project.



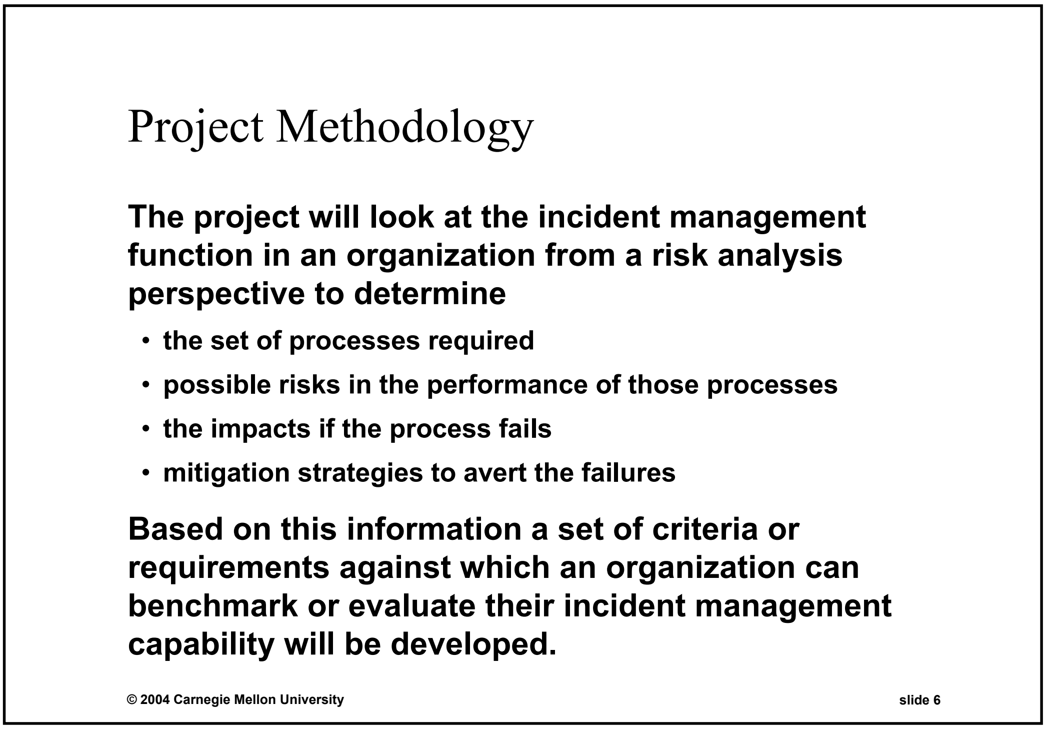
Project Team Members

CERT CSIRT Development Team Members

- Georgia Killcrece
- Robin Ruefle
- Mark Zajicek

Survivable Enterprise Management Team Members

- Chris Alberts
- Audrey Dorofee

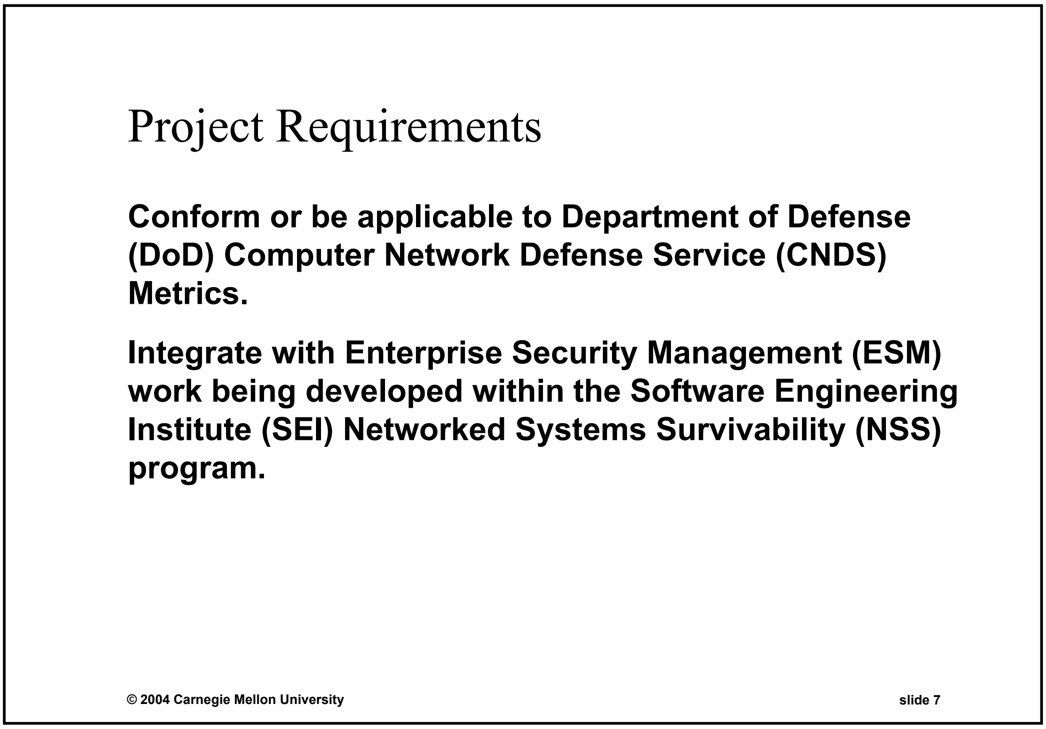


Project Methodology

The project will look at the incident management function in an organization from a risk analysis perspective to determine

- the set of processes required
- possible risks in the performance of those processes
- the impacts if the process fails
- mitigation strategies to avert the failures

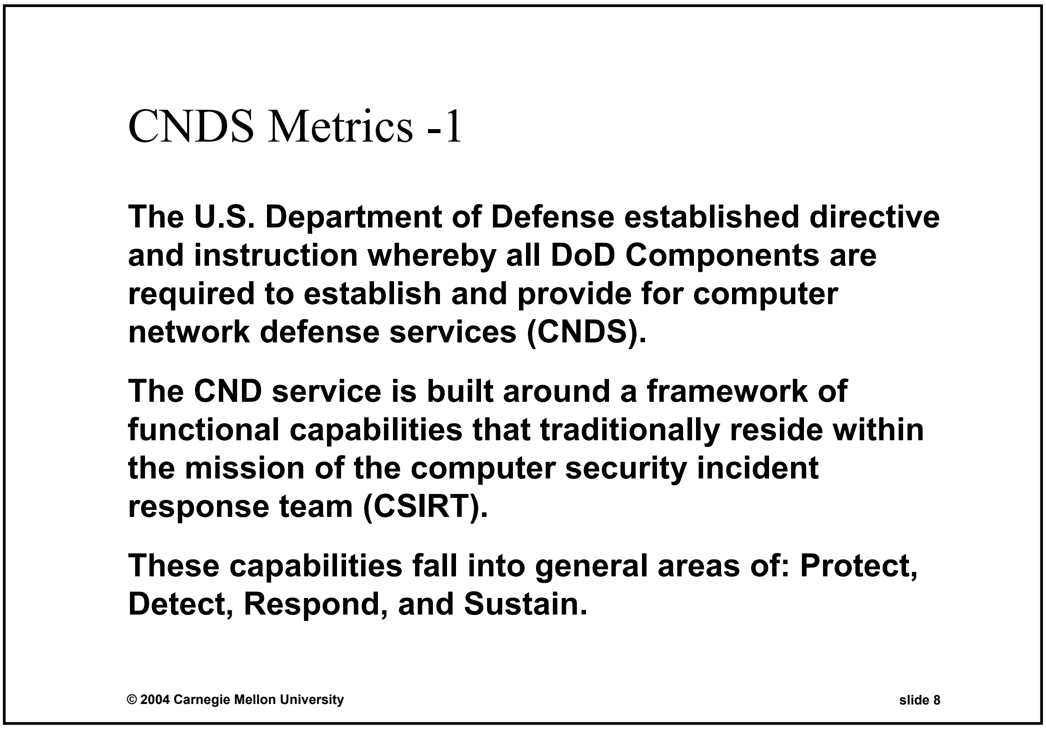
Based on this information a set of criteria or requirements against which an organization can benchmark or evaluate their incident management capability will be developed.



Project Requirements

Conform or be applicable to Department of Defense (DoD) Computer Network Defense Service (CNDS) Metrics.

Integrate with Enterprise Security Management (ESM) work being developed within the Software Engineering Institute (SEI) Networked Systems Survivability (NSS) program.

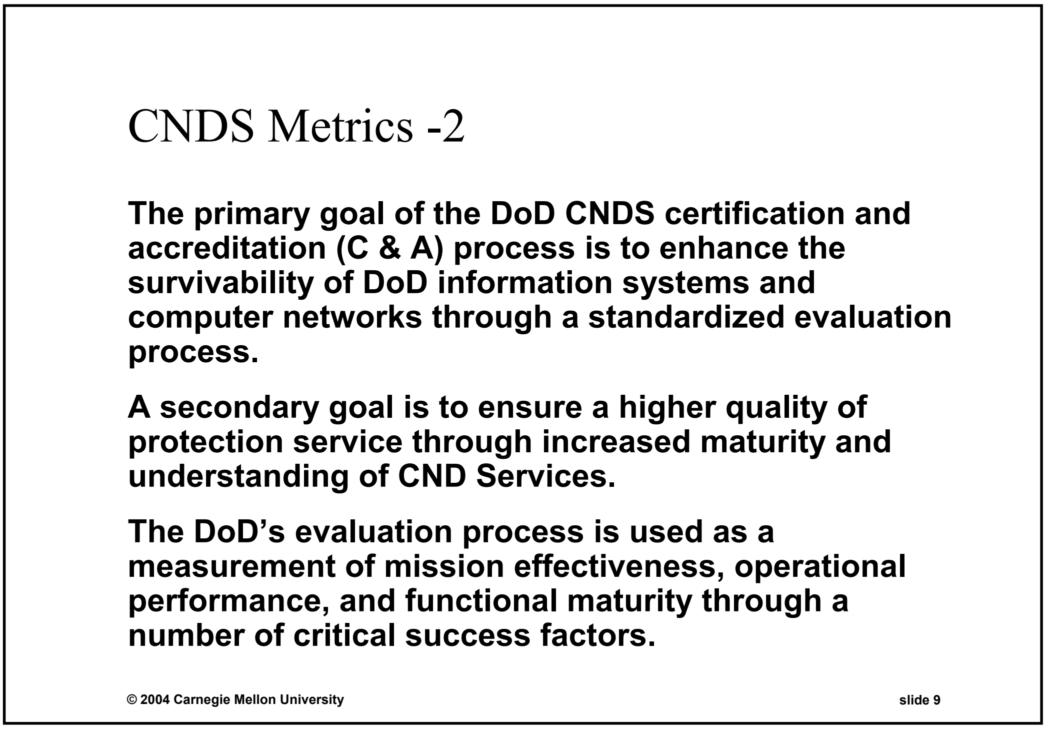


CNDS Metrics -1

The U.S. Department of Defense established directive and instruction whereby all DoD Components are required to establish and provide for computer network defense services (CNDS).

The CND service is built around a framework of functional capabilities that traditionally reside within the mission of the computer security incident response team (CSIRT).

These capabilities fall into general areas of: Protect, Detect, Respond, and Sustain.

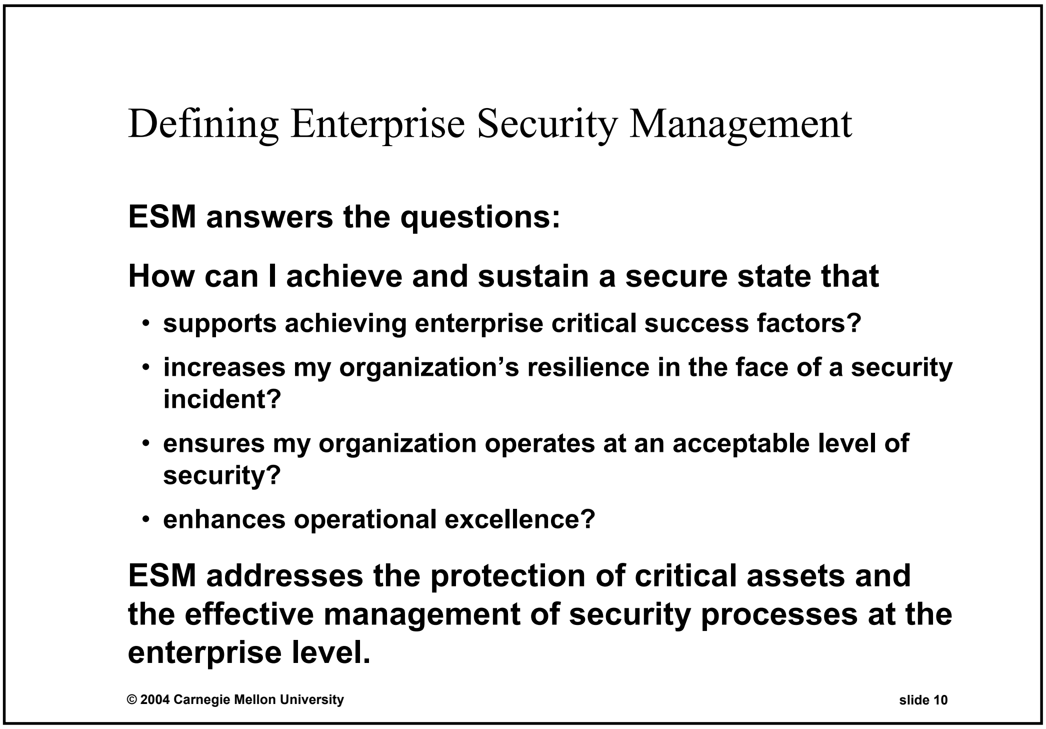


CNDS Metrics -2

The primary goal of the DoD CNDS certification and accreditation (C & A) process is to enhance the survivability of DoD information systems and computer networks through a standardized evaluation process.

A secondary goal is to ensure a higher quality of protection service through increased maturity and understanding of CND Services.

The DoD’s evaluation process is used as a measurement of mission effectiveness, operational performance, and functional maturity through a number of critical success factors.



Defining Enterprise Security Management

ESM answers the questions:

How can I achieve and sustain a secure state that

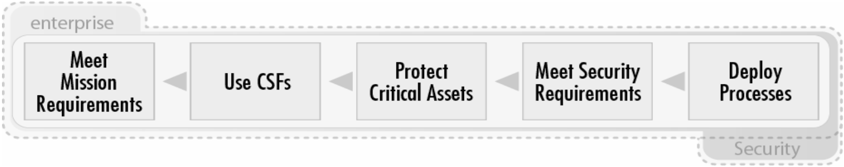
- supports achieving enterprise critical success factors?
- increases my organization’s resilience in the face of a security incident?
- ensures my organization operates at an acceptable level of security?
- enhances operational excellence?

ESM addresses the protection of critical assets and the effective management of security processes at the enterprise level.

ESM: Foundation Principles

Mobilize enterprise-wide capabilities in a coordinated and collaborative way to achieve and sustain a secure state.

- **Focus on key mission requirements by using Critical Success Factors (CSFs)**
- **Achieving CSFs requires the protection of critical assets**
- **Protecting critical assets = meeting their security requirements (using defined processes)**
- **Deploy processes that protect critical assets and achieve critical success factors**

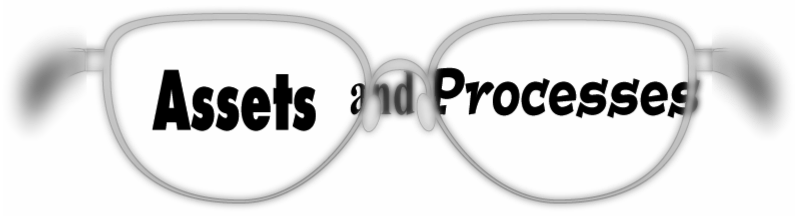


slide 11

ESM: Focus

Enterprise security management focuses on the interaction between assets **and** processes:

- *Assets* **are valued by the organization and must be protected to achieve the mission**
- **ESM** *processes* **act on these assets to ensure that their security requirements are defined, implemented, measured, and controlled**



slide 12

ESM: Components

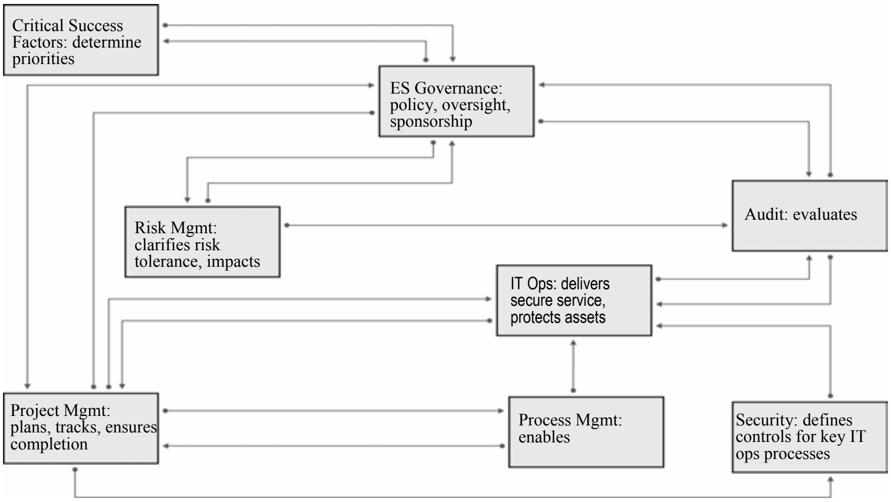
Emerging framework that defines the core capabilities necessary to achieve and sustain a secure state

A mobilizing or institutionalizing approach that defines the coordination and cooperation that must exist among the core capabilities

Tools, techniques, and methods that enable the optimization* of the core capabilities to achieve an organization's desired security state

*** To make as effective or functional as possible**

Mobilizing to Achieve/Sustain Enterprise Security



Critical Success Factors: determine priorities

ES Governance: policy, oversight, sponsorship

Risk Mgmt: clarifies risk tolerance, impacts

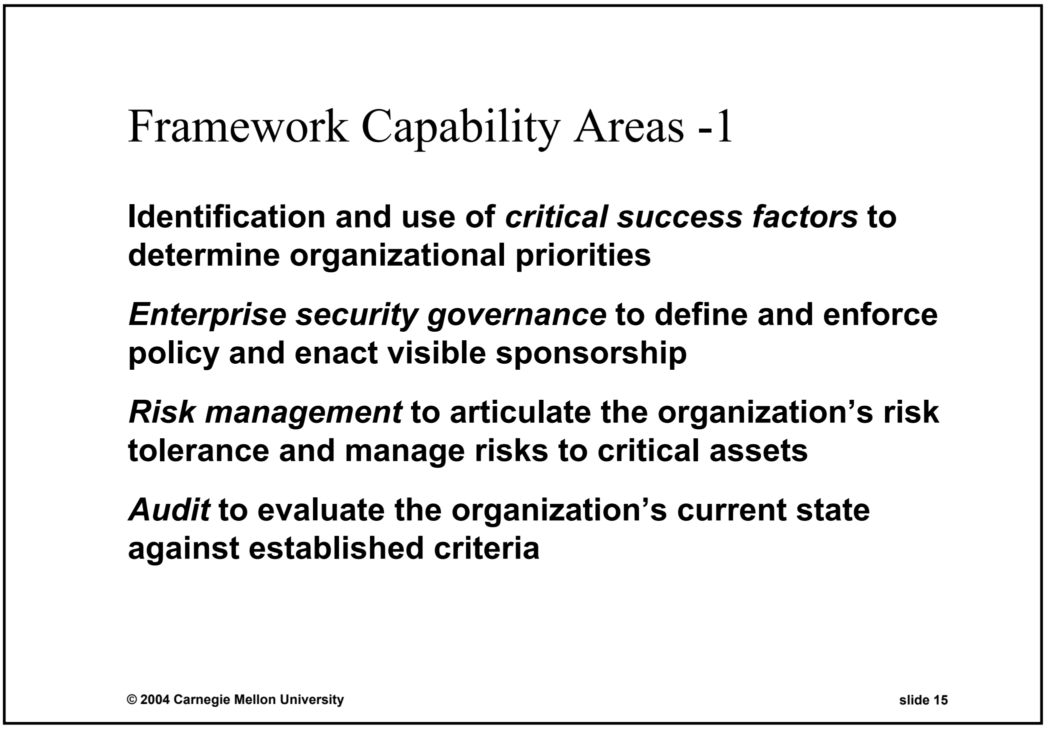
Audit: evaluates

IT Ops: delivers secure service, protects assets

Project Mgmt: plans, tracks, ensures completion

Process Mgmt: enables

Security: defines controls for key IT ops processes



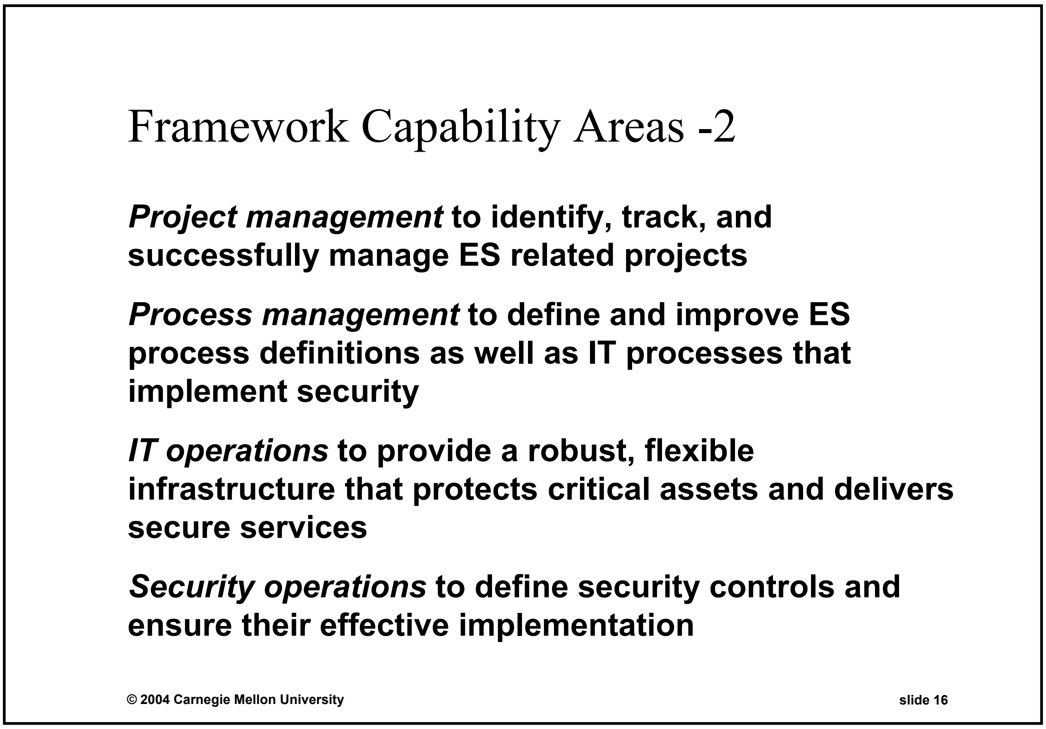
Framework Capability Areas -1

Identification and use of *critical success factors* to determine organizational priorities

Enterprise security governance to define and enforce policy and enact visible sponsorship

Risk management to articulate the organization’s risk tolerance and manage risks to critical assets

Audit to evaluate the organization’s current state against established criteria



Framework Capability Areas -2

Project management to identify, track, and successfully manage ES related projects

Process management to define and improve ES process definitions as well as IT processes that implement security

IT operations to provide a robust, flexible infrastructure that protects critical assets and delivers secure services

Security operations to define security controls and ensure their effective implementation

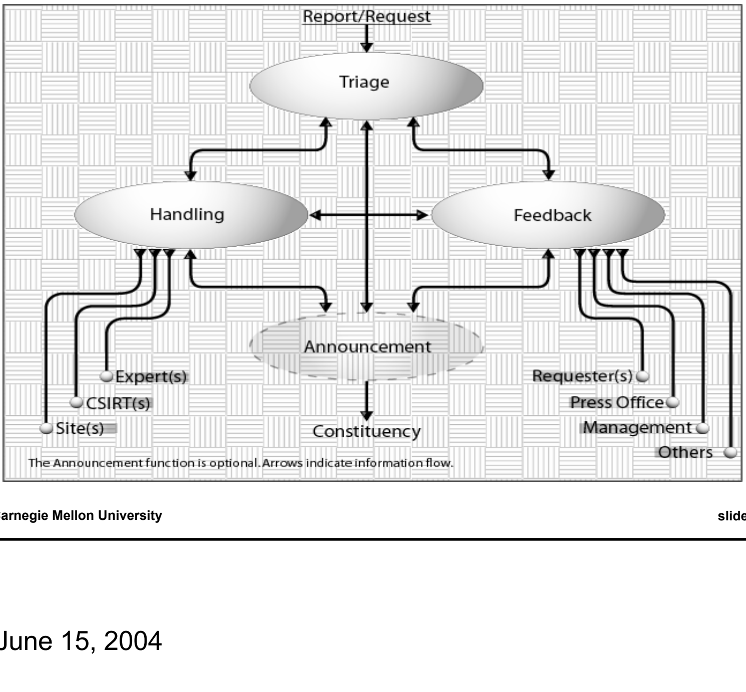
Integration of EMS and Incident Management

Incident Management is the development of a plan of action, a response plan that

- **integrates into the existing processes and organizational structures**
- **strengthens and improves the capability of the constituency to effectively manage computer security events**
- **is part of an overall strategy to protect and secure critical business functions and assets**

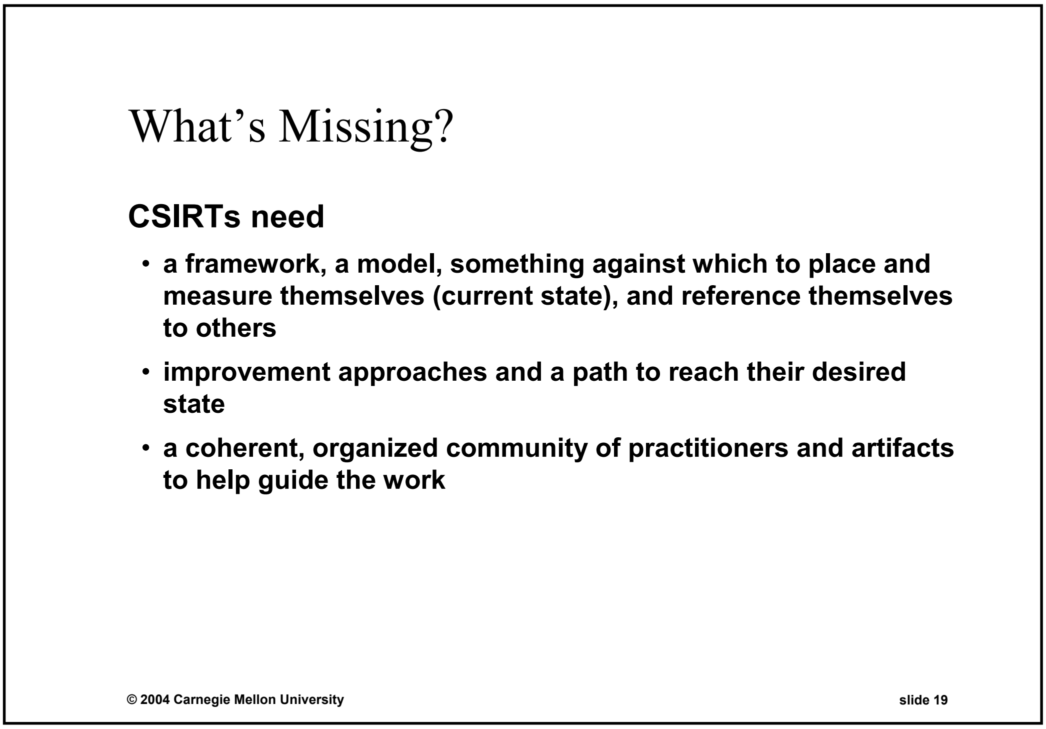
slide 17

Process Versus Technology



The Announcement function is optional. Arrows indicate information flow.

slide 18

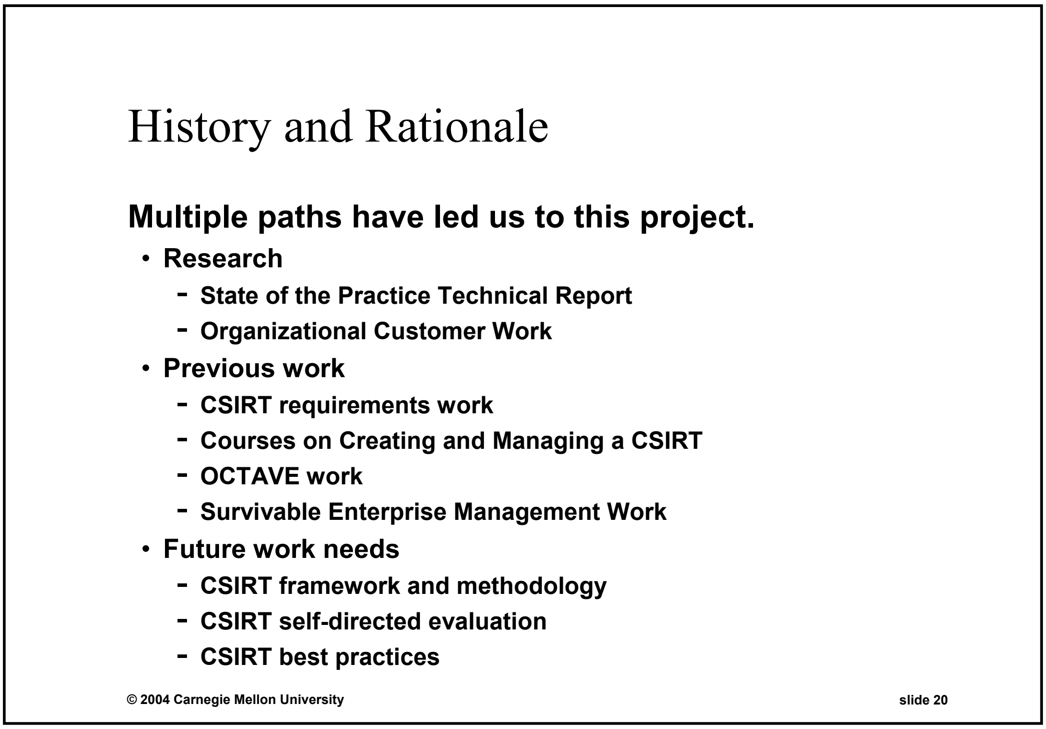


What’s Missing?

CSIRTs need

- a framework, a model, something against which to place and measure themselves (current state), and reference themselves to others
- improvement approaches and a path to reach their desired state
- a coherent, organized community of practitioners and artifacts to help guide the work

slide 19



History and Rationale

Multiple paths have led us to this project.

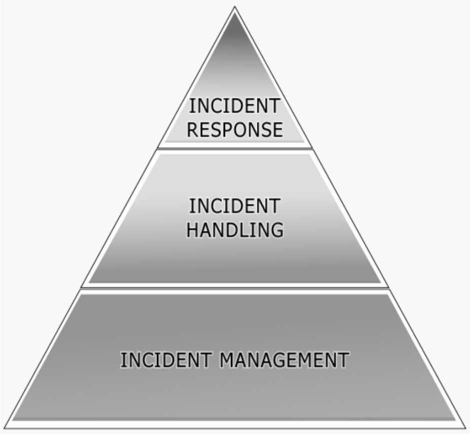
- Research
  - State of the Practice Technical Report
  - Organizational Customer Work
- Previous work
  - CSIRT requirements work
  - Courses on Creating and Managing a CSIRT
  - OCTAVE work
  - Survivable Enterprise Management Work
- Future work needs
  - CSIRT framework and methodology
  - CSIRT self-directed evaluation
  - CSIRT best practices

slide 20

Research Motivations

Questions that need answered

- **Where do I start and what steps do I take to create a CSIRT or incident handling capability?**
- **Where does incident management occur in the organizational enterprise?**



Building the Framework

Our Steps include

- **incident management process maps**
- **evaluation instrument**
- **framework for building and sustaining incident management capabilities**

Process Mapping Work Documents and Forms

Brainstorming Notes

Workflow Diagrams

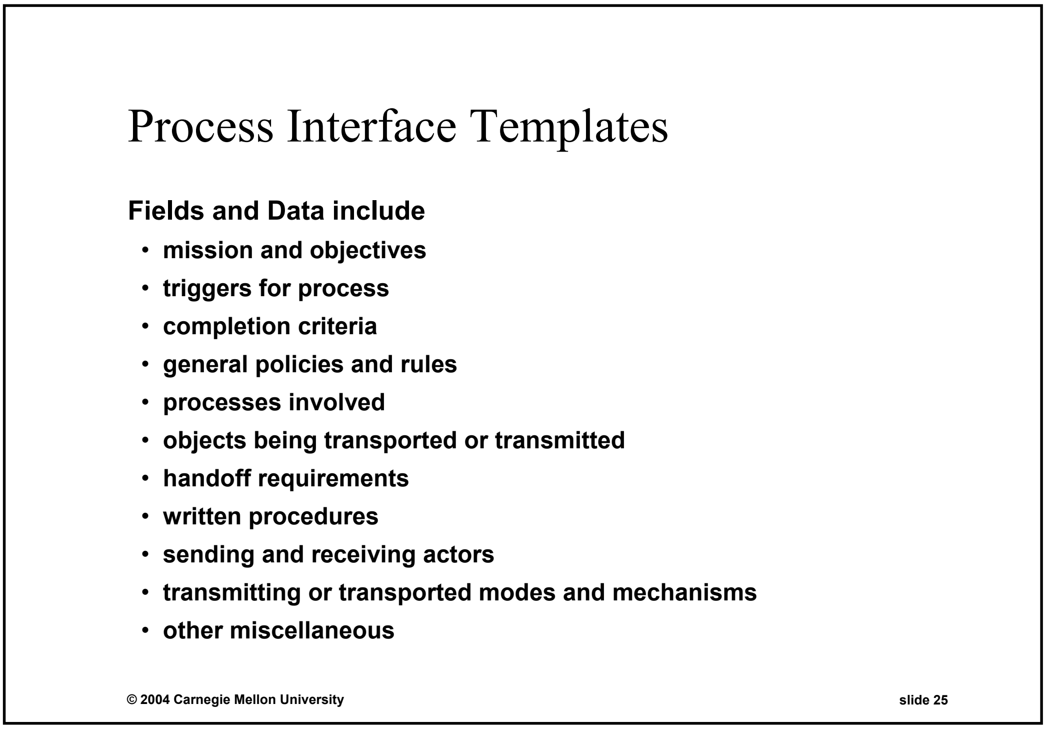
Process Data Templates

Process Interface Templates

Process Data Templates

Fields and data include

- **mission and objectives**
- **triggers for process**
- **completion criteria**
- **general policies and rules**
- **inputs and outputs**
- **process requirements**
- **written procedures**
- **people**
- **technologies**
- **other or miscellaneous information or actions**

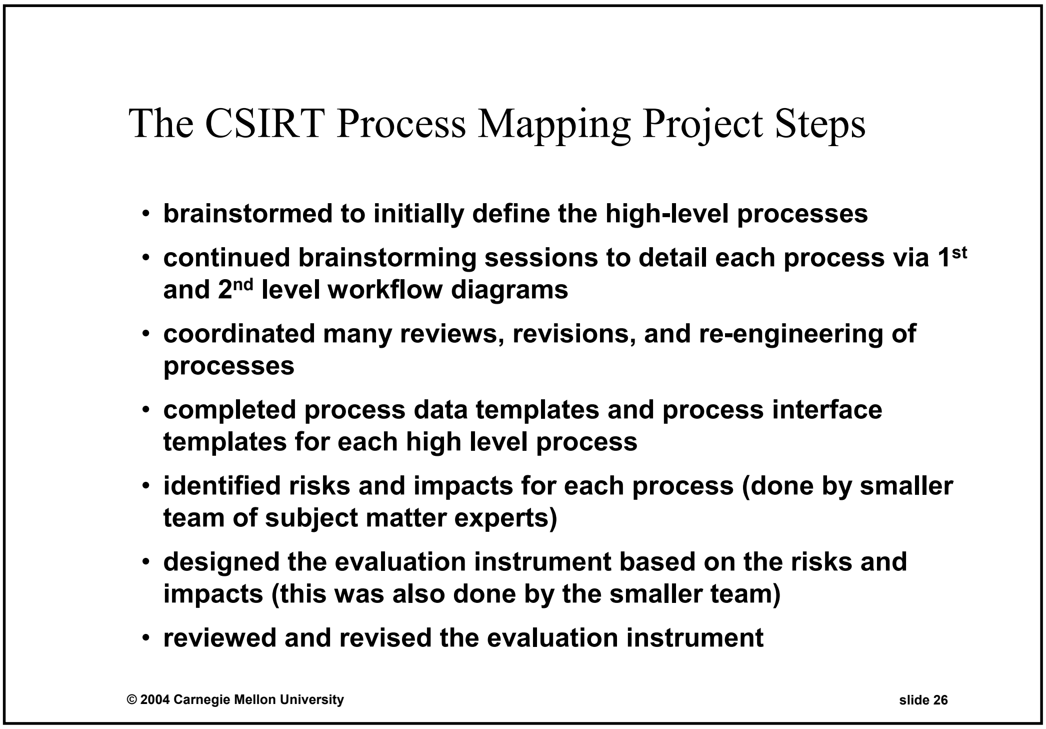


Process Interface Templates

Fields and Data include

- mission and objectives
- triggers for process
- completion criteria
- general policies and rules
- processes involved
- objects being transported or transmitted
- handoff requirements
- written procedures
- sending and receiving actors
- transmitting or transported modes and mechanisms
- other miscellaneous

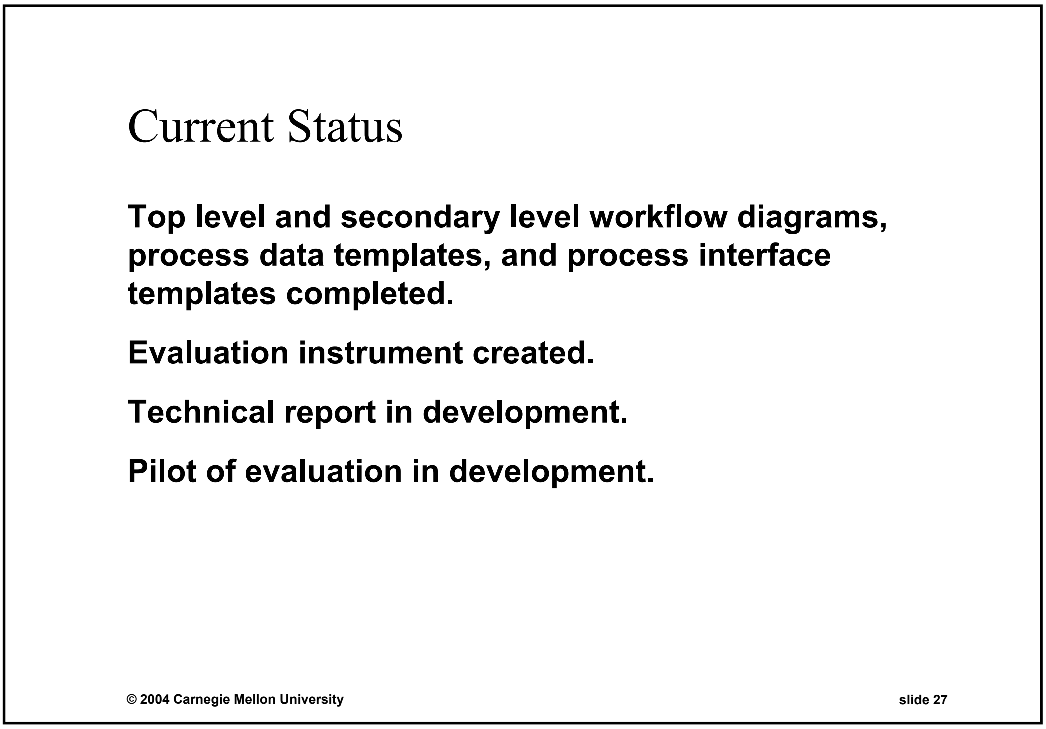
slide 25



The CSIRT Process Mapping Project Steps

- brainstormed to initially define the high-level processes
- continued brainstorming sessions to detail each process via 1st and 2nd level workflow diagrams
- coordinated many reviews, revisions, and re-engineering of processes
- completed process data templates and process interface templates for each high level process
- identified risks and impacts for each process (done by smaller team of subject matter experts)
- designed the evaluation instrument based on the risks and impacts (this was also done by the smaller team)
- reviewed and revised the evaluation instrument

slide 26



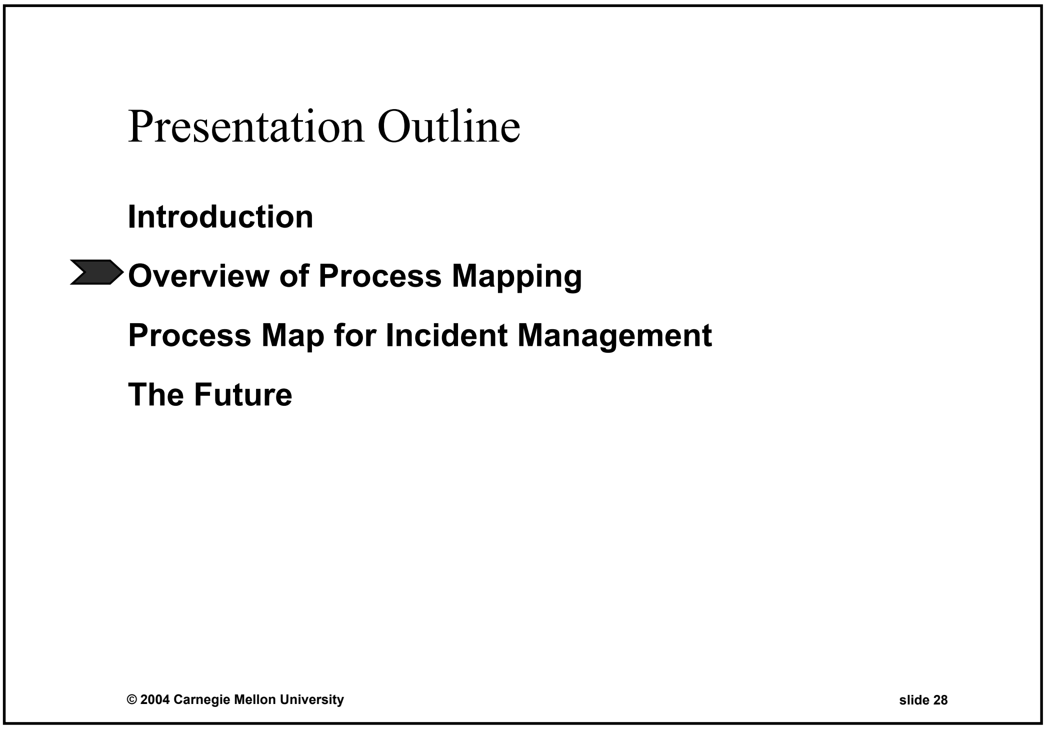
Current Status

Top level and secondary level workflow diagrams, process data templates, and process interface templates completed.

Evaluation instrument created.

Technical report in development.

Pilot of evaluation in development.



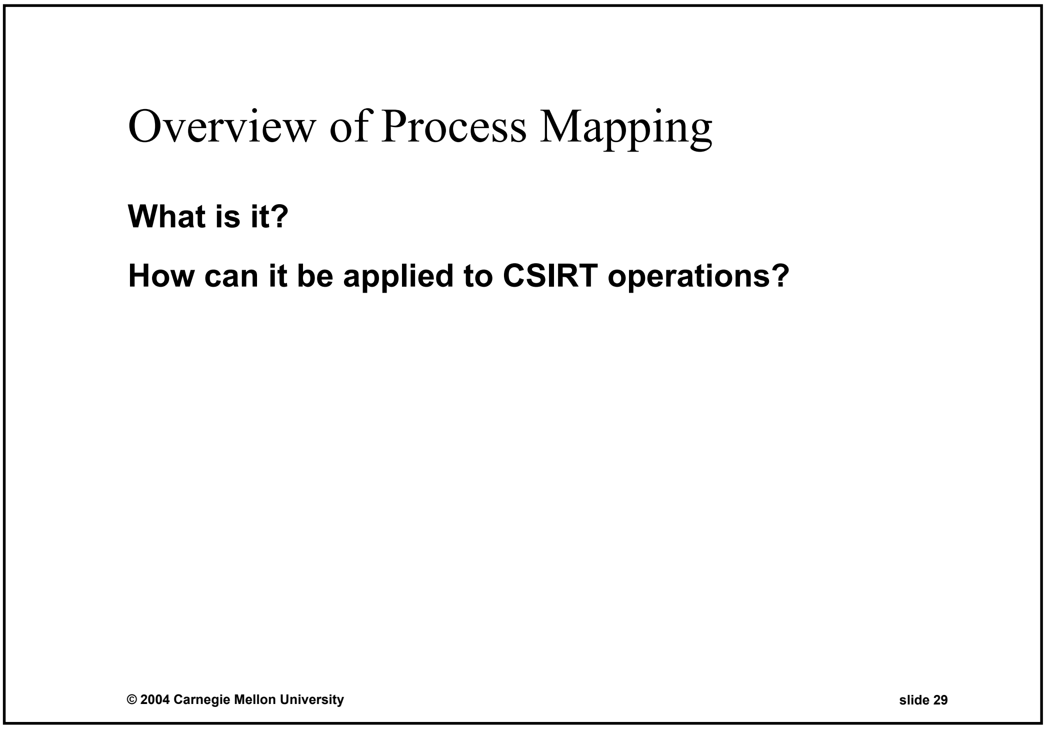
Presentation Outline

Introduction

➤ Overview of Process Mapping

Process Map for Incident Management

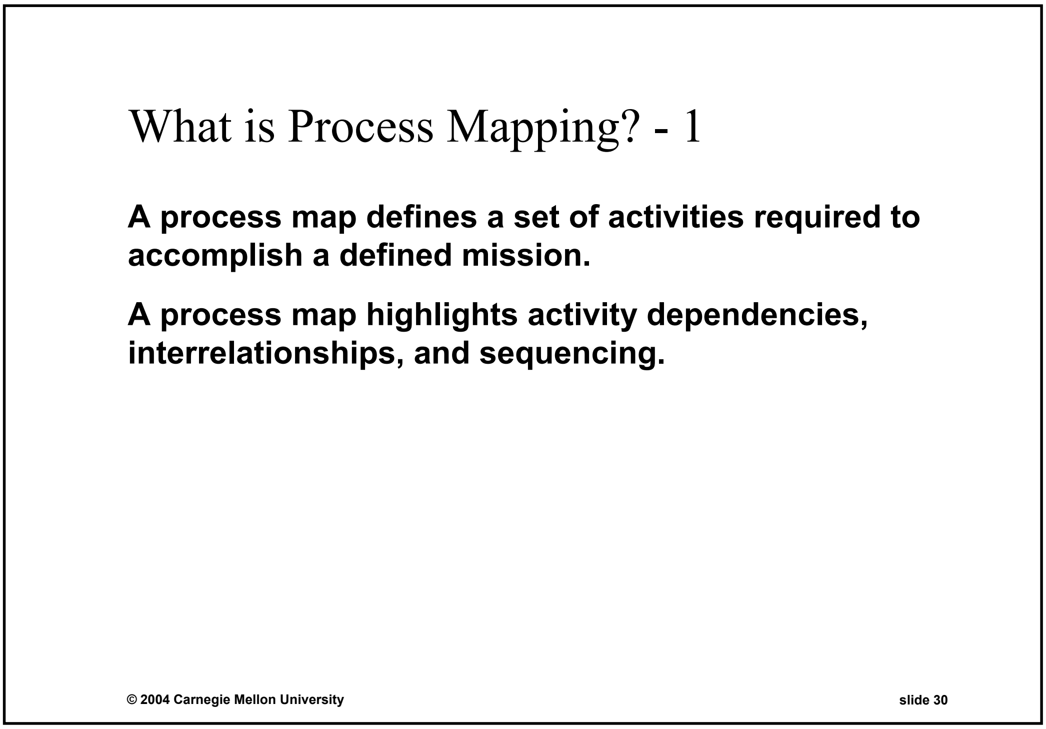
The Future



Overview of Process Mapping

What is it?

How can it be applied to CSIRT operations?



What is Process Mapping? - 1

A process map defines a set of activities required to accomplish a defined mission.

A process map highlights activity dependencies, interrelationships, and sequencing.

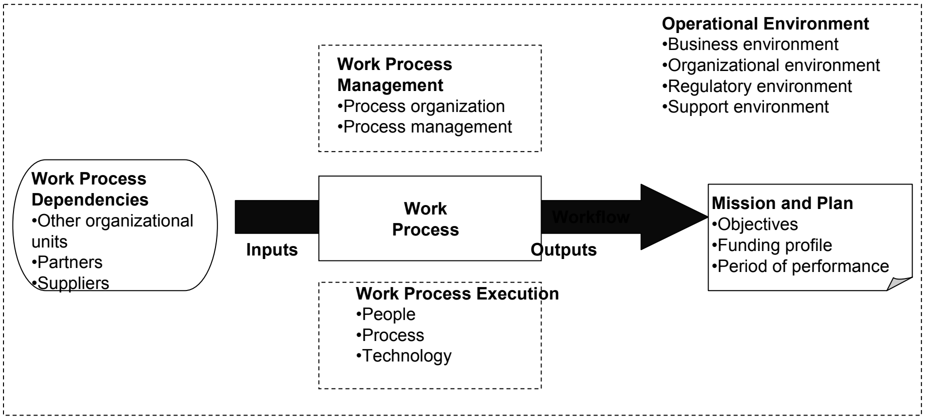
What is Process Mapping? - 2

A process map includes

- **goals and objectives**
- **processes and activities**
- **inputs and outputs**
- **roles and responsibilities**
- **constraints**
- **enablers**
- **supporting technology**
- **procedures and documentation**
- **interfaces or hand-offs**
- **interrelationships and dependencies**

slide 31

What is Process Mapping? - 3



Operational Environment
•Business environment
•Organizational environment
•Regulatory environment
•Support environment

Work Process Management
•Process organization
•Process management

Work Process Dependencies
•Other organizational units
•Partners
•Suppliers

Work Process

Inputs

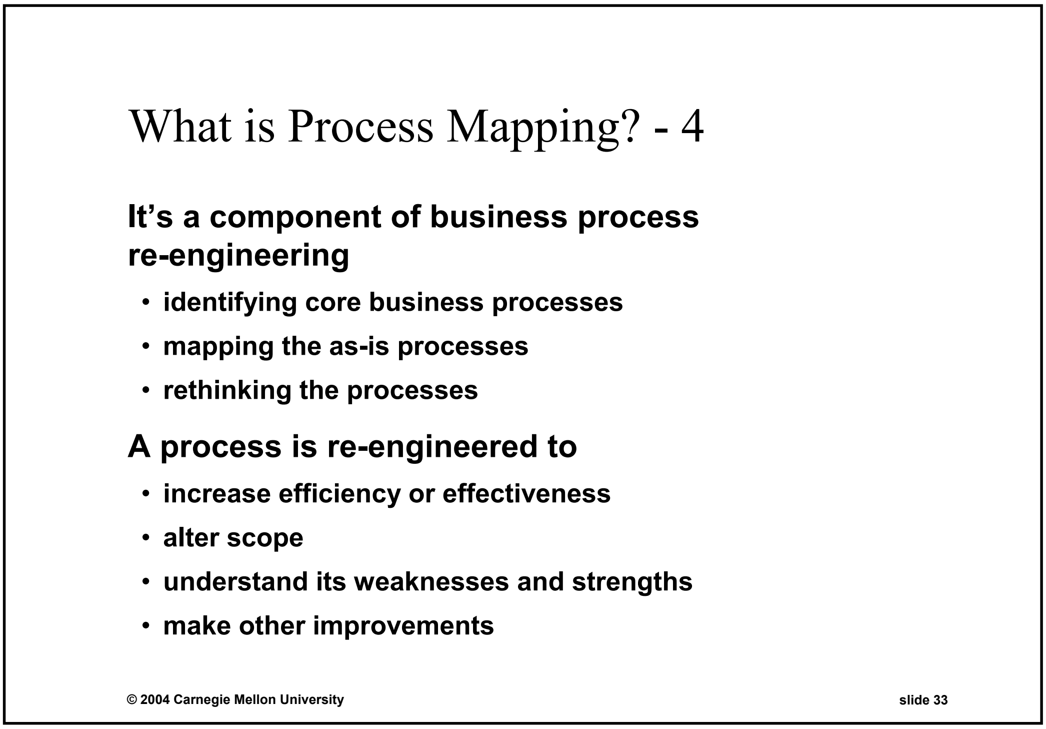
Workflow

Outputs

Mission and Plan
•Objectives
•Funding profile
•Period of performance

Work Process Execution
•People
•Process
•Technology

slide 32



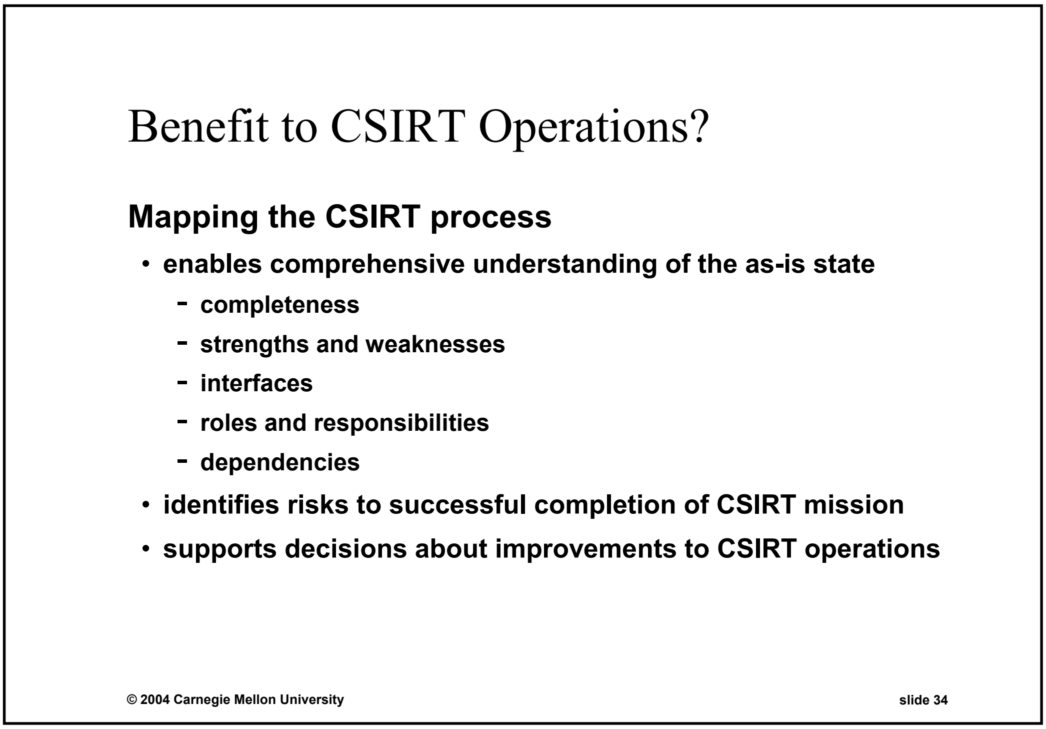
What is Process Mapping? - 4

It’s a component of business process re-engineering

- **identifying core business processes**
- **mapping the as-is processes**
- **rethinking the processes**

A process is re-engineered to

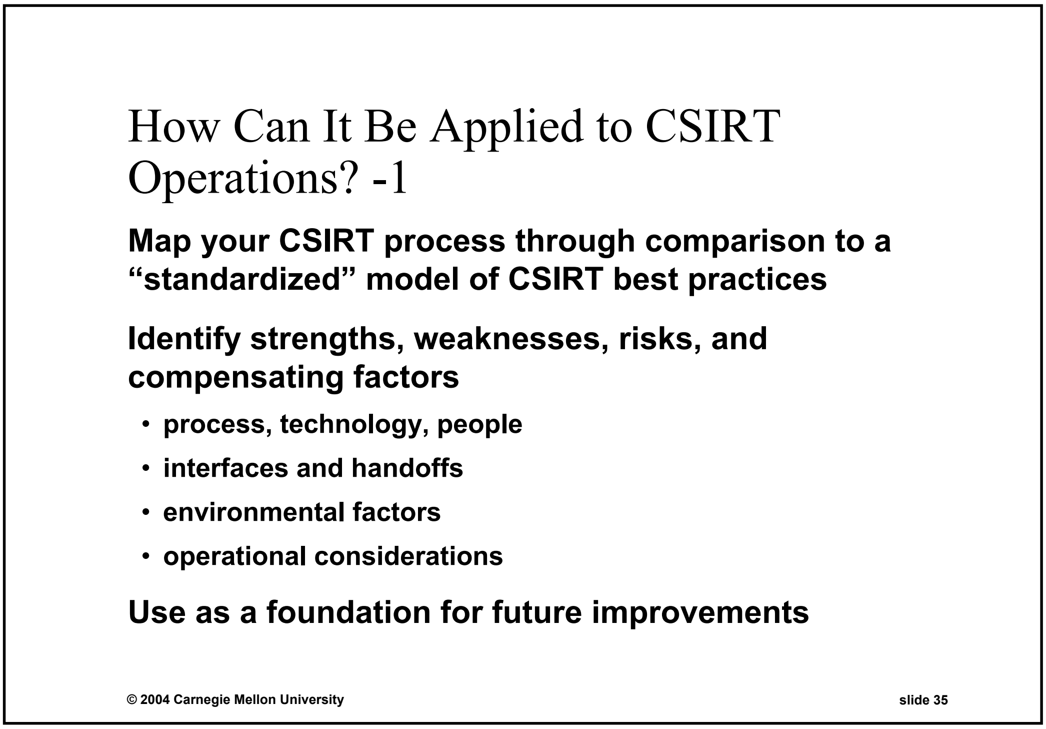
- **increase efficiency or effectiveness**
- **alter scope**
- **understand its weaknesses and strengths**
- **make other improvements**



Benefit to CSIRT Operations?

Mapping the CSIRT process

- **enables comprehensive understanding of the as-is state**
  - **completeness**
  - **strengths and weaknesses**
  - **interfaces**
  - **roles and responsibilities**
  - **dependencies**
- **identifies risks to successful completion of CSIRT mission**
- **supports decisions about improvements to CSIRT operations**



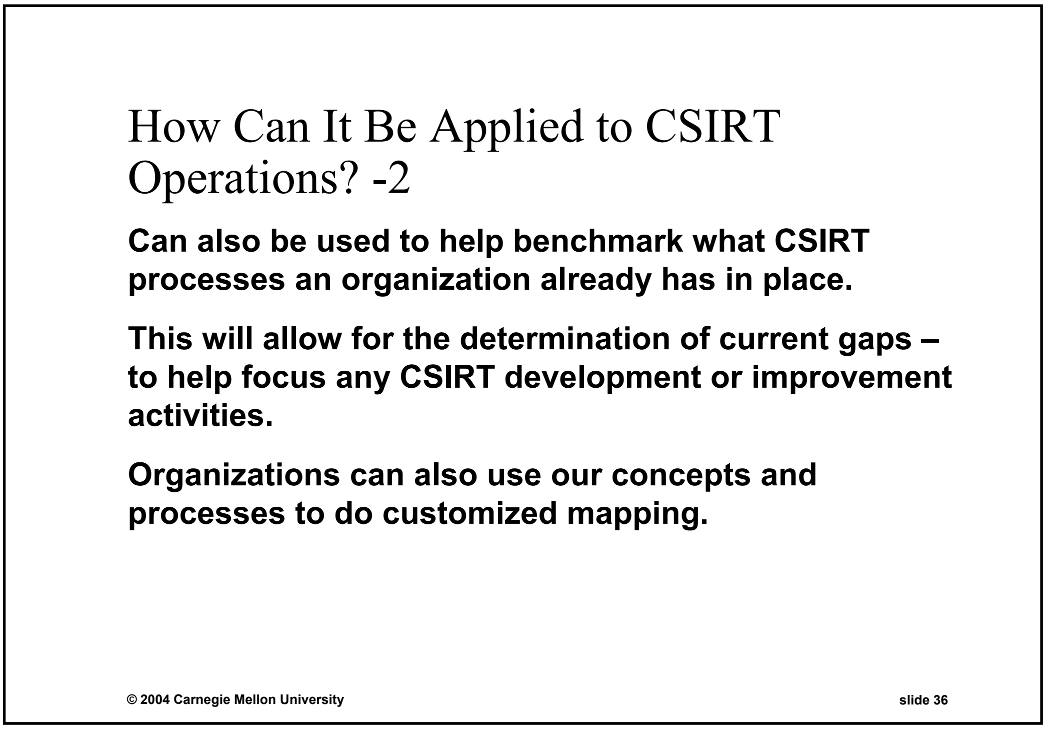
How Can It Be Applied to CSIRT Operations? -1

Map your CSIRT process through comparison to a “standardized” model of CSIRT best practices

Identify strengths, weaknesses, risks, and compensating factors

- **process, technology, people**
- **interfaces and handoffs**
- **environmental factors**
- **operational considerations**

Use as a foundation for future improvements



How Can It Be Applied to CSIRT Operations? -2

Can also be used to help benchmark what CSIRT processes an organization already has in place.

This will allow for the determination of current gaps – to help focus any CSIRT development or improvement activities.

Organizations can also use our concepts and processes to do customized mapping.

Presentation Outline

Introduction

Overview of Process Mapping

➤ Process Map for Incident Management

The Future

Process Map for Incident Management

CERT CSIRT Development Team process map for incident management

- Assumptions and rules
- Overview of process components
  - Prepare/Improve/Sustain
  - Protect
  - Detect
  - Triage
  - Respond
- Overview of first level processes
- Applying risk analysis to the process map

Assumptions and Rules

Looking at

- **Best practices**
- **Common practices**

Not exceptions

- **You can always think up an exception or special situation.**
- **We tried to exclude these types of processes.**

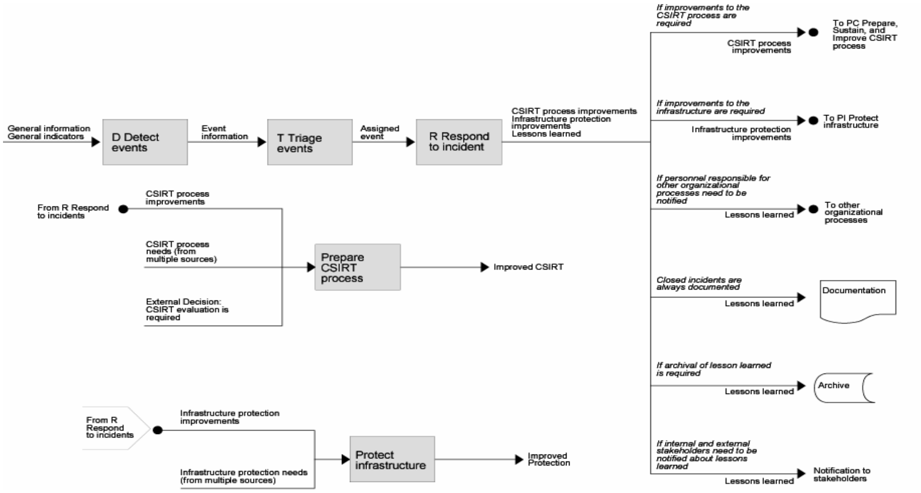
slide 39

Overview of Process Components

- **Prepare/Improve/Sustain**
- **Protect**
- **Detect**
- **Triage**
- **Respond**

slide 40

Incident Response



General information
General indicators

D Detect events

Event information

T Triage events

Assigned event

R Respond to incident

CSIRT process improvements
Infrastructure protection improvements
Lessons learned

If improvements to the CSIRT process are required
CSIRT process improvements
To PC Prepare, Sustain, and Improve CSIRT process

If improvements to the infrastructure are required
Infrastructure protection improvements
To PI Protect infrastructure

If personnel responsible for other organizational processes need to be notified
Lessons learned
To other organizational processes

Closed incidents are always documented
Lessons learned
Documentation

If archival of lesson learned is required
Lessons learned
Archive

If internal and external stakeholders need to be notified about lessons learned
Lessons learned
Notification to stakeholders

From R Respond to incidents
CSIRT process improvements
CSIRT process needs (from multiple sources)
External Decision: CSIRT evaluation is required
Prepare CSIRT process
Improved CSIRT

From R Respond to incidents
Infrastructure protection improvements
Infrastructure protection needs (from multiple sources)
Protect infrastructure
Improved Protection

slide 41

Prepare/Improve/Sustain CSIRT

Inputs include

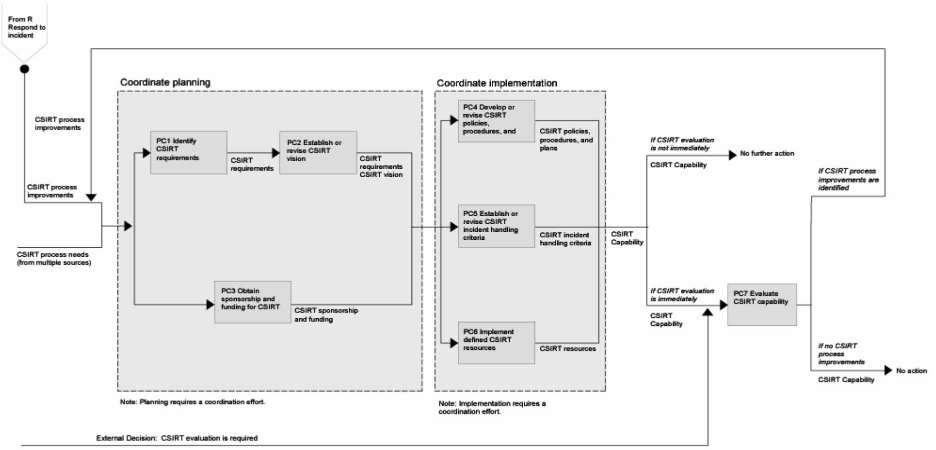
- **CSIRT process requirements**
- **CSIRT process needs**

Processes include

- **coordinate planning**
  - **identify CSIRT requirements**
  - **establish CSIRT vision**
  - **obtain CSIRT funding and sponsorship**
- **coordinate implementation**
  - **develop CSIRT policies, processes, or plans**
  - **establish CSIRT incident handling criteria**
  - **implement defined CSIRT resources (staff, equipment and infrastructure)**
- **evaluate CSIRT capability**
- **determine CSIRT process modifications**
- **implement CSIRT process modifications**

slide 42

PC Prepare, Sustain, and Improve CSIRT Process


From R Respond to incident
CSIRT process improvements
CSIRT process improvements
CSIRT process needs (from multiple sources)
Coordinate planning
PC1 Identify CSIRT requirements
CSIRT requirements
PC2 Establish or revise CSIRT vision
CSIRT requirements CSIRT vision
PC3 Obtain sponsorship and funding for CSIRT
CSIRT sponsorship and funding
Note: Planning requires a coordination effort.
Coordinate implementation
PC4 Develop or revise CSIRT policies, procedures, and
CSIRT policies, procedures, and plans
PC5 Establish or revise CSIRT incident handling criteria
CSIRT incident handling criteria
PC6 Implement defined CSIRT resources
CSIRT resources
Note: Implementation requires a coordination effort.
CSIRT Capability
If CSIRT evaluation is not immediately
CSIRT Capability
No further action
If CSIRT evaluation is immediately
CSIRT Capability
PC7 Evaluate CSIRT capability
If CSIRT process improvements are identified
If no CSIRT process improvements
CSIRT Capability
No action
External Decision: CSIRT evaluation is required

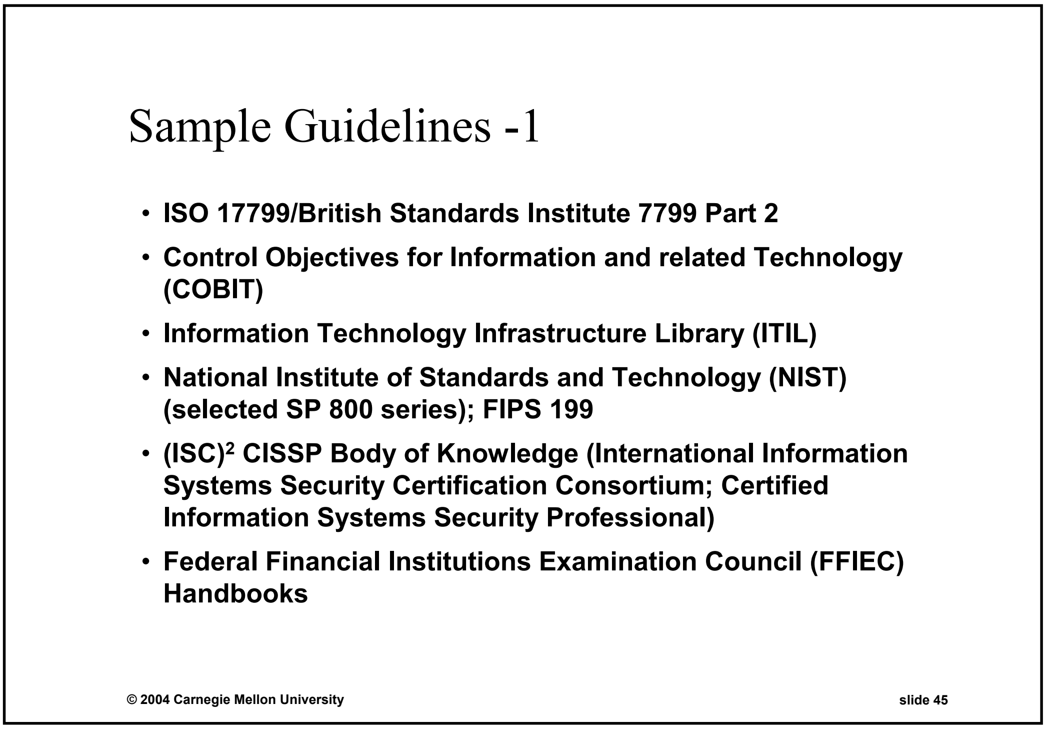
Protect Infrastructure

Inputs include

- **organizational policies**
- **relevant laws and statutes**
- **standards, metrics, and best practices**

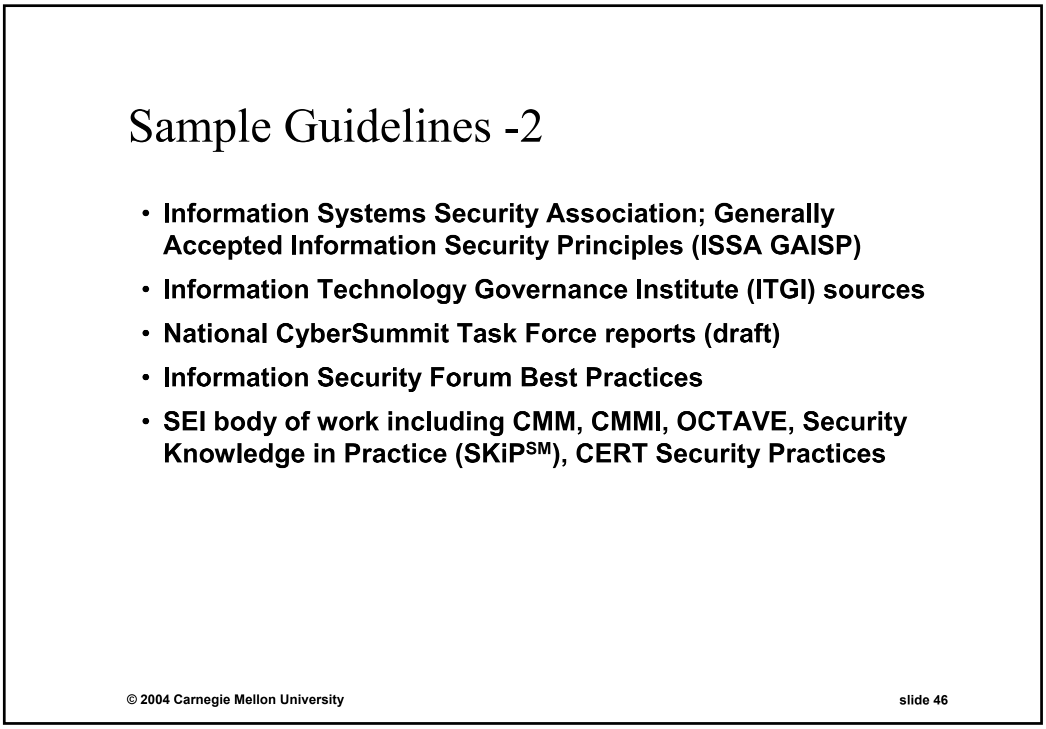
Processes include

- **determine infrastructure protection and survivability requirements**
- **harden and secure infrastructures according to the requirements and continue to carry out changes and improvements as needed**
- **monitor, assess, and analyze infrastructure for survivability (e.g., monitor network activity and physical access, conduct periodic risks assessments)**
- **repair and recover from problems, events, or incidents**



Sample Guidelines -1

- ISO 17799/British Standards Institute 7799 Part 2
- Control Objectives for Information and related Technology (COBIT)
- Information Technology Infrastructure Library (ITIL)
- National Institute of Standards and Technology (NIST) (selected SP 800 series); FIPS 199
- (ISC)^2 CISSP Body of Knowledge (International Information Systems Security Certification Consortium; Certified Information Systems Security Professional)
- Federal Financial Institutions Examination Council (FFIEC) Handbooks



Sample Guidelines -2

- Information Systems Security Association; Generally Accepted Information Security Principles (ISSA GAISP)
- Information Technology Governance Institute (ITGI) sources
- National CyberSummit Task Force reports (draft)
- Information Security Forum Best Practices
- SEI body of work including CMM, CMMI, OCTAVE, Security Knowledge in Practice (SKiP^{SM}), CERT Security Practices

Detect

Reactive processes

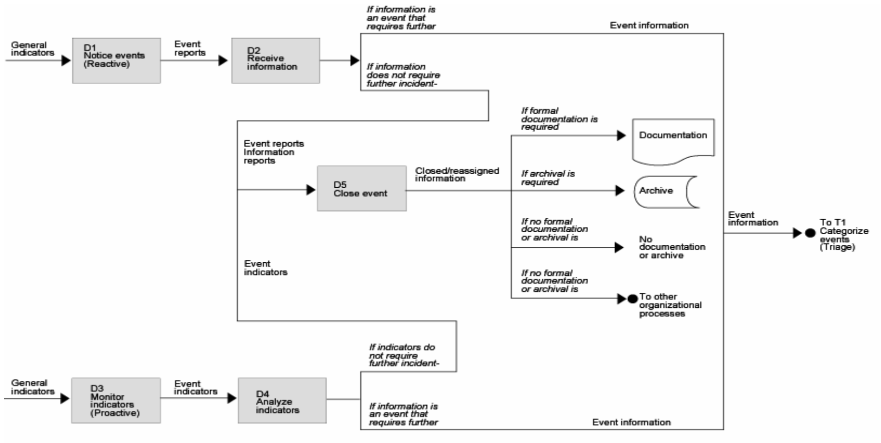
- **notice events**
  - **constituency member notices unusual activity**
  - **external sources report activity or events or share advisories and alerts**
- **receive information**

Proactive processes

- **monitor indicators**
  - **monitor networks and hosts**
  - **proactive vulnerability evaluation**
  - **public monitoring/technology watch**
- **analyze indicators**

Send notable information to triage.

D Detect Events


General indicators
D1 Notice events (Reactive)
Event reports
D2 Receive information
If information is an event that requires further
If information does not require further incident-
Event information
Event reports Information reports
D5 Close event
Closed/reassigned information
If formal documentation is required
Documentation
If archival is required
Archive
If no formal documentation or archival is
No documentation or archive
If no formal documentation or archival is
To other organizational processes
Event information
To T1 Categorize events (Triage)
Event indicators
If indicators do not require further incident-
General indicators
D3 Monitor indicators (Proactive)
Event indicators
D4 Analyze indicators
If information is an event that requires further
Event information

Triage

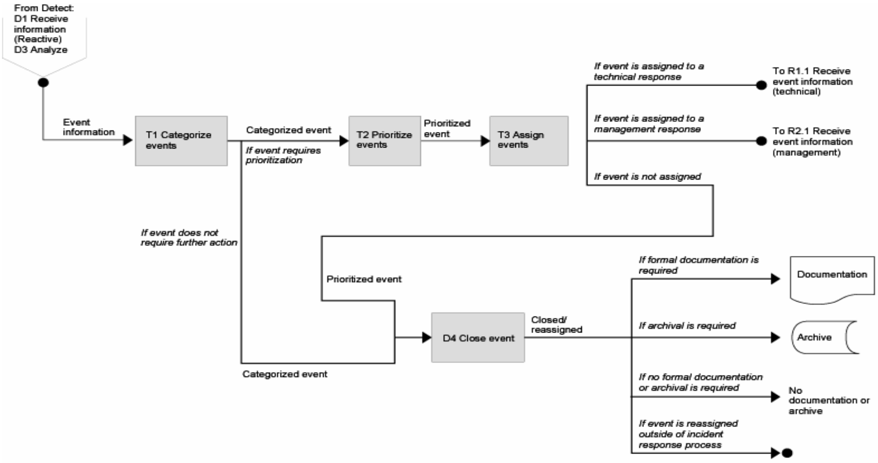
Inputs

- event information from detect process
- analysis of indicators from detect process

Processes include

- categorize events
- prioritize events
- assign events
- close events

T Triage Events


From Detect:
D1 Receive information (Reactive)
D3 Analyze
Event information
T1 Categorize events
Categorized event
If event requires prioritization
T2 Prioritize events
Prioritized event
T3 Assign events
If event is assigned to a technical response
To R1.1 Receive event information (technical)
If event is assigned to a management response
To R2.1 Receive event information (management)
If event is not assigned
If event does not require further action
Prioritized event
Categorized event
D4 Close event
Closed/ reassigned
If formal documentation is required
Documentation
If archival is required
Archive
If no formal documentation or archival is required
No documentation or archive
If event is reassigned outside of incident response process

Respond

Inputs include

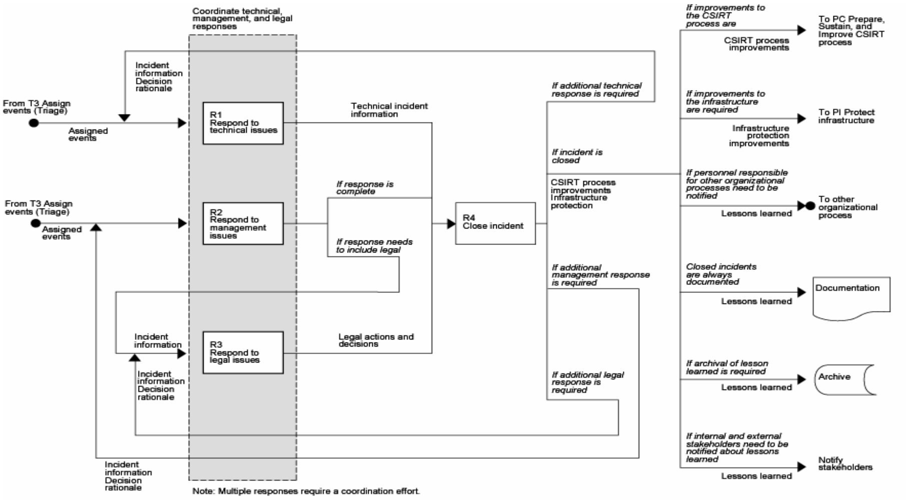
- event information
- incident information

Processes include

- receive information
- analyze information
- plan response strategy
- coordinate and respond to incident (coordinate technical, management, and legal response as needed or appropriate)
- close incident (could include as appropriate: document, archive, post-mortem, notify)

slide 51

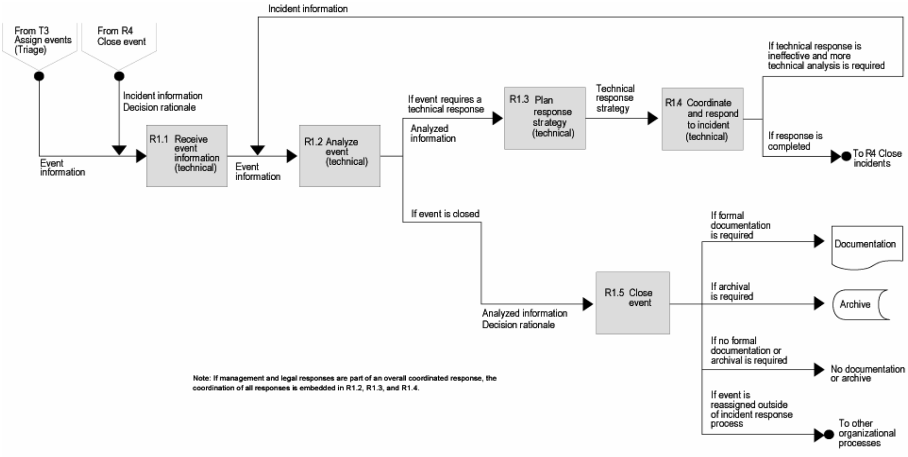
R Respond to Incidents


Coordinate technical, management, and legal responses
Incident information Decision rationale
From T3 Assign events (Triage)
Assigned events
R1 Respond to technical issues
Technical incident information
From T3 Assign events (Triage)
Assigned events
R2 Respond to management issues
If response is complete
If response needs to include legal
R4 Close incident
Incident information
R3 Respond to legal issues
Legal actions and decisions
Incident information Decision rationale
Incident information Decision rationale
If additional technical response is required
If incident is closed
CSIRT process improvements Infrastructure protection
If additional management response is required
If additional legal response is required
If improvements to the CSIRT process are
CSIRT process improvements
To PC Prepare, Sustain, and Improve CSIRT process
If improvements to the infrastructure are required
Infrastructure protection improvements
To PI Protect infrastructure
If personnel responsible for other organizational processes need to be notified
Lessons learned
To other organizational process
Closed incidents are always documented
Lessons learned
Documentation
If archival of lesson learned is required
Lessons learned
Archive
If internal and external stakeholders need to be notified about lessons learned
Lessons learned
Notify stakeholders

Note: Multiple responses require a coordination effort.

slide 52

R1 Respond to Technical Issues


Incident information
From T3 Assign events (Triage)
From R4 Close event
Incident information Decision rationale
Event information
R1.1 Receive event information (technical)
Event information
R1.2 Analyze event (technical)
If event requires a technical response
Analyzed information
R1.3 Plan response strategy (technical)
Technical response strategy
R1.4 Coordinate and respond to incident (technical)
If technical response is ineffective and more technical analysis is required
If response is completed
To R4 Close incidents
If event is closed
Analyzed information Decision rationale
R1.5 Close event
If formal documentation is required
Documentation
If archival is required
Archive
If no formal documentation or archival is required
No documentation or archive
If event is reassigned outside of incident response process
To other organizational processes

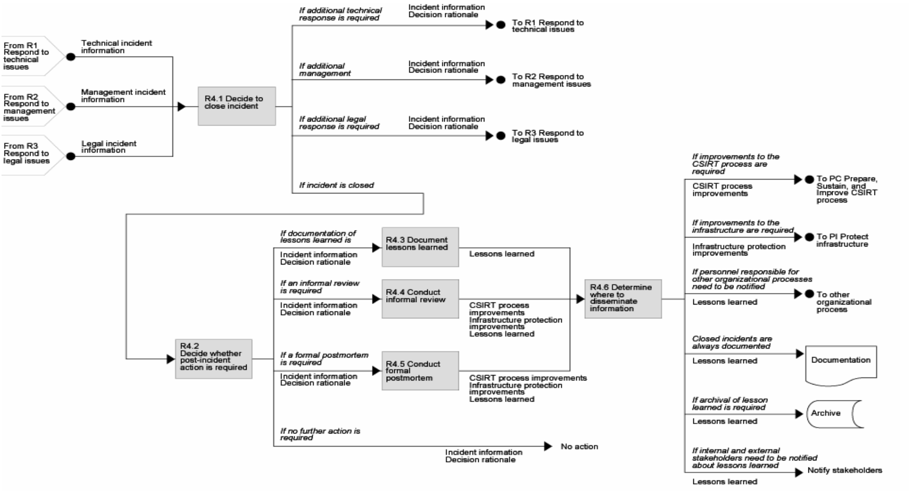
Note: If management and legal responses are part of an overall coordinated response, the coordination of all responses is embedded in R1.2, R1.3, and R1.4.

Close Incident

Decision points include

- decide to perform a post-mortem
- decide if and how to disseminate information
- decide if and how to archive and document information

R4 Close Incident



From R1 Respond to technical issues
Technical incident information

From R2 Respond to management issues
Management incident information

From R3 Respond to legal issues
Legal incident information

R4.1 Decide to close incident

If additional technical response is required
Incident information
Decision rationale
To R1 Respond to technical issues

If additional management
Incident information
Decision rationale
To R2 Respond to management issues

If additional legal response is required
Incident information
Decision rationale
To R3 Respond to legal issues

If incident is closed

R4.2 Decide whether post-incident action is required

If documentation of lessons learned is
Incident information
Decision rationale
R4.3 Document lessons learned
Lessons learned

If an informal review is required
Incident information
Decision rationale
R4.4 Conduct informal review
CSIRT process improvements
Infrastructure protection improvements
Lessons learned

If a formal postmortem is required
Incident information
Decision rationale
R4.5 Conduct formal postmortem
CSIRT process improvements
Infrastructure protection improvements
Lessons learned

If no further action is required
Incident information
Decision rationale
No action

R4.6 Determine where to disseminate information

If improvements to the CSIRT process are required
CSIRT process improvements
To PC Prepare, Sustain, and Improve CSIRT process

If improvements to the infrastructure are required
Infrastructure protection improvements
To PI Protect infrastructure

If personnel responsible for other organizational processes need to be notified
Lessons learned
To other organizational process

Closed incidents are always documented
Lessons learned
Documentation

If archival of lesson learned is required
Lessons learned
Archive

If internal and external stakeholders need to be notified about lessons learned
Lessons learned
Notify stakeholders

Next Steps

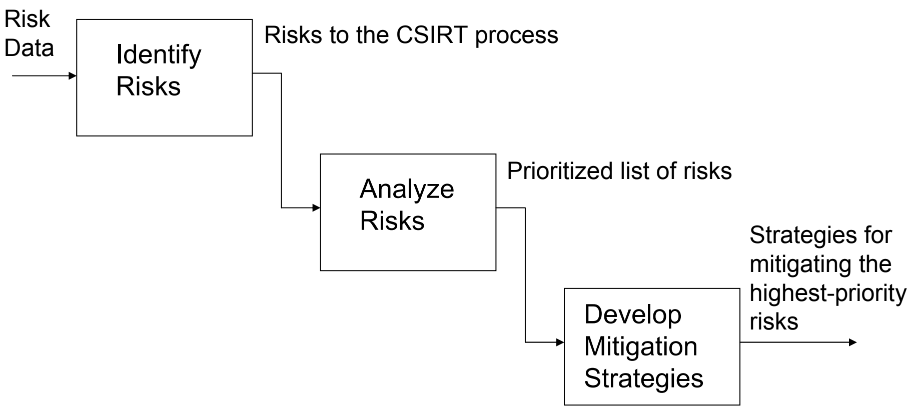
Develop a gap analysis instrument to help document the "as-is" state of an organization in regards to incident management processes.

Apply risk analysis to incident management processes.

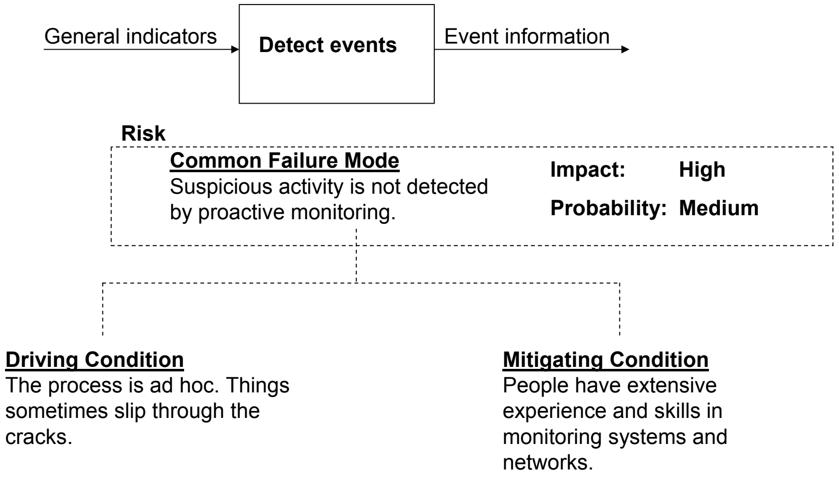
Determine common failure modes for processes.

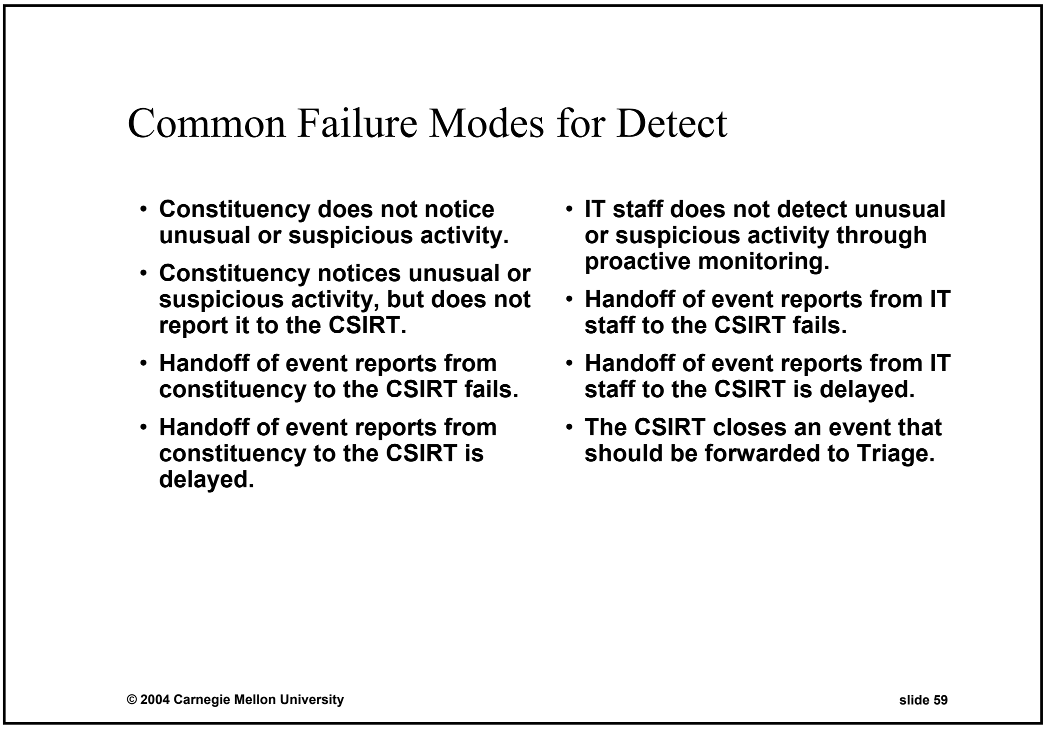
Determine common mitigation strategies to prevent failure.

Risk Evaluation Process


Risk Data
Identify Risks
Risks to the CSIRT process
Analyze Risks
Prioritized list of risks
Develop Mitigation Strategies
Strategies for mitigating the highest-priority risks

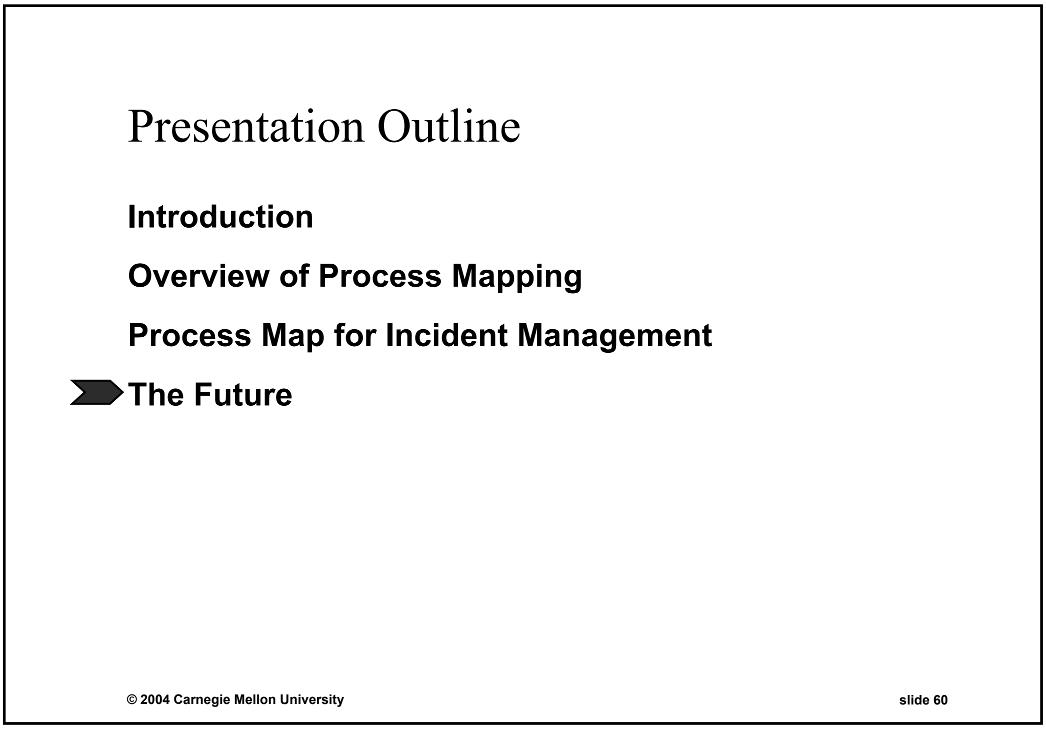
Example of Evaluation Results


General indicators
Detect events
Event information
Risk
Common Failure Mode
Suspicious activity is not detected by proactive monitoring.
Impact: High
Probability: Medium
Driving Condition
The process is ad hoc. Things sometimes slip through the cracks.
Mitigating Condition
People have extensive experience and skills in monitoring systems and networks.



Common Failure Modes for Detect

- Constituency does not notice unusual or suspicious activity.
- Constituency notices unusual or suspicious activity, but does not report it to the CSIRT.
- Handoff of event reports from constituency to the CSIRT fails.
- Handoff of event reports from constituency to the CSIRT is delayed.
- IT staff does not detect unusual or suspicious activity through proactive monitoring.
- Handoff of event reports from IT staff to the CSIRT fails.
- Handoff of event reports from IT staff to the CSIRT is delayed.
- The CSIRT closes an event that should be forwarded to Triage.



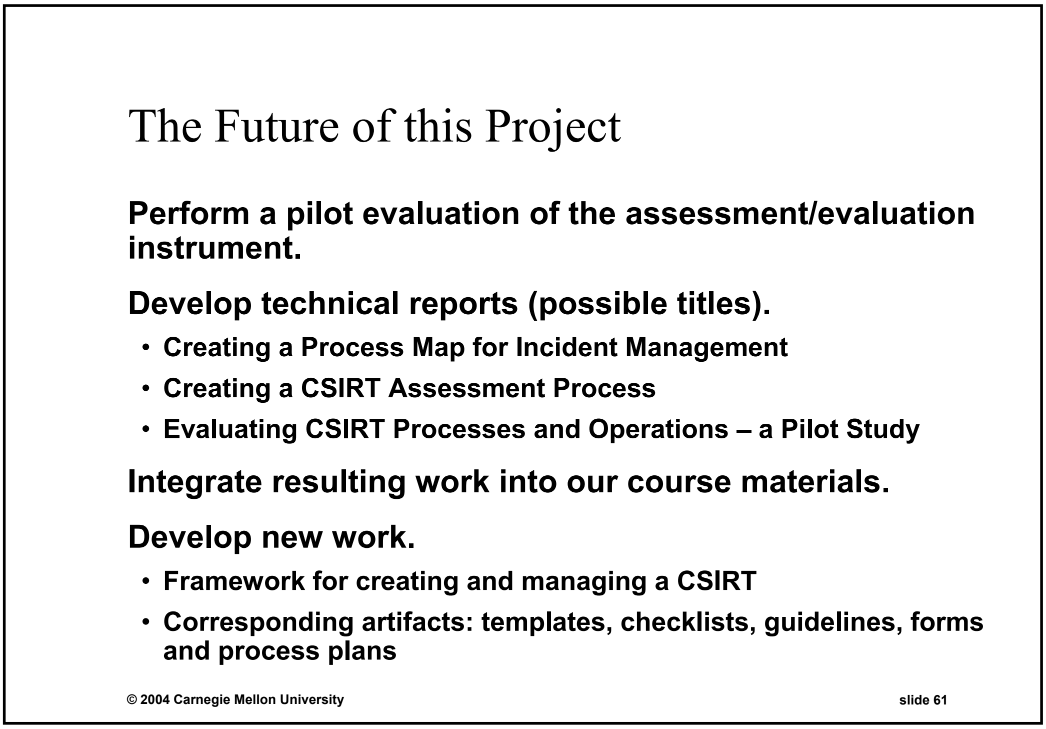
Presentation Outline

Introduction

Overview of Process Mapping

Process Map for Incident Management

➤ **The Future**



The Future of this Project

Perform a pilot evaluation of the assessment/evaluation instrument.

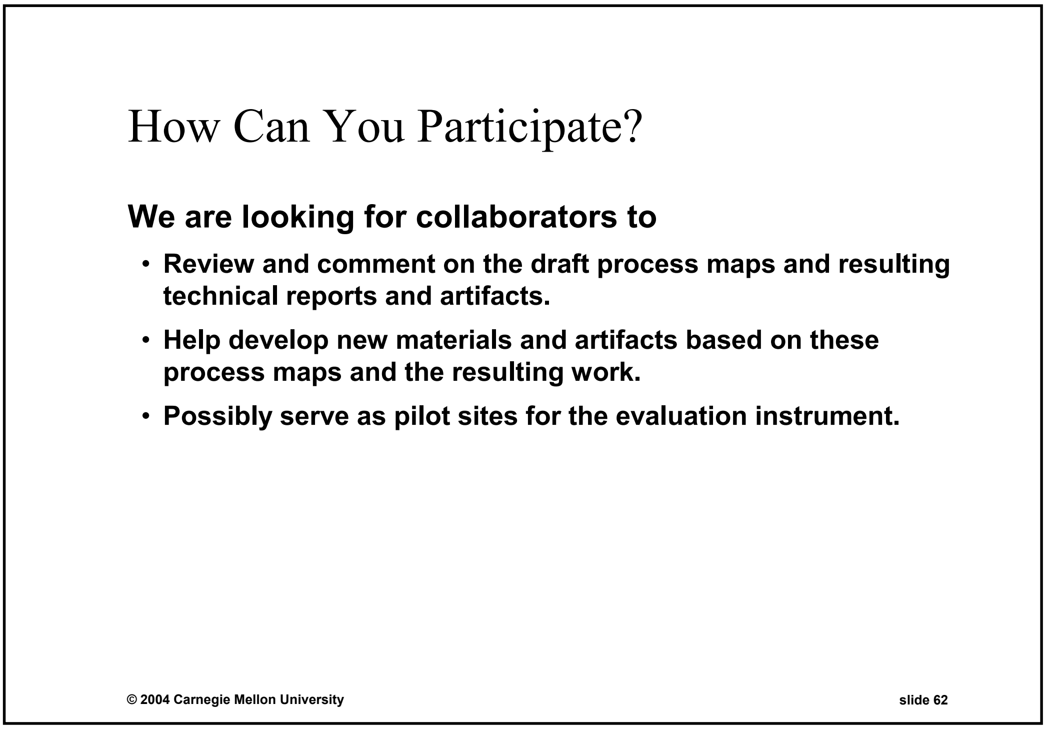
Develop technical reports (possible titles).

- **Creating a Process Map for Incident Management**
- **Creating a CSIRT Assessment Process**
- **Evaluating CSIRT Processes and Operations – a Pilot Study**

Integrate resulting work into our course materials.

Develop new work.

- **Framework for creating and managing a CSIRT**
- **Corresponding artifacts: templates, checklists, guidelines, forms and process plans**



How Can You Participate?

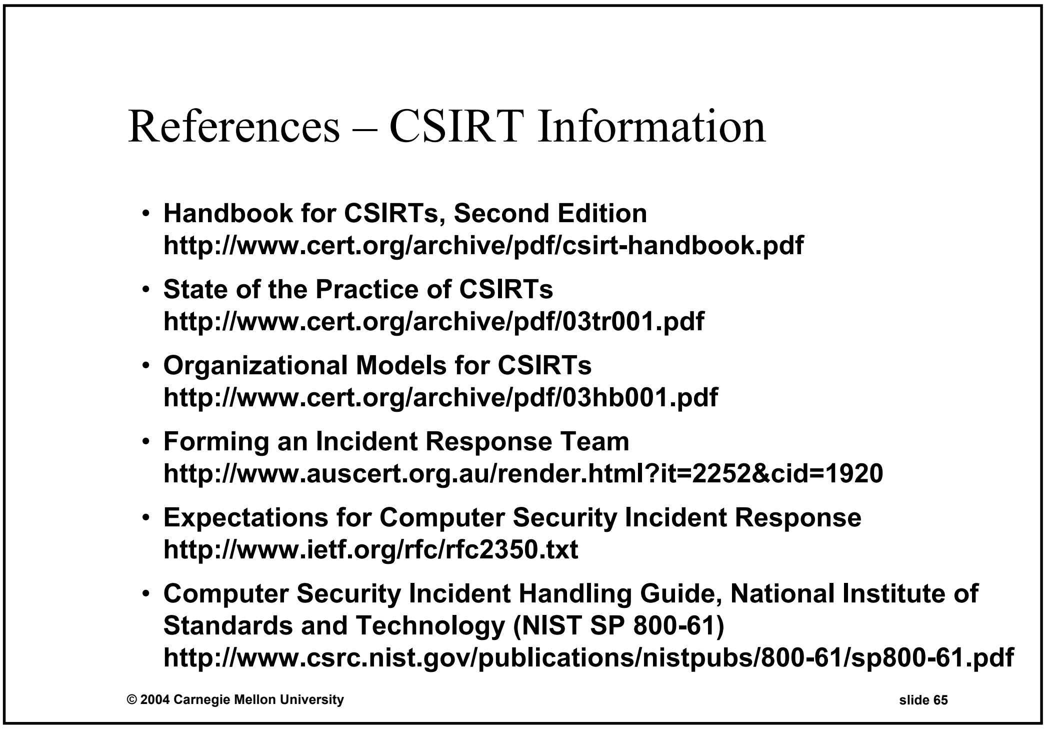
We are looking for collaborators to

- **Review and comment on the draft process maps and resulting technical reports and artifacts.**
- **Help develop new materials and artifacts based on these process maps and the resulting work.**
- **Possibly serve as pilot sites for the evaluation instrument.**

Questions and Comments?

References – Process Mapping

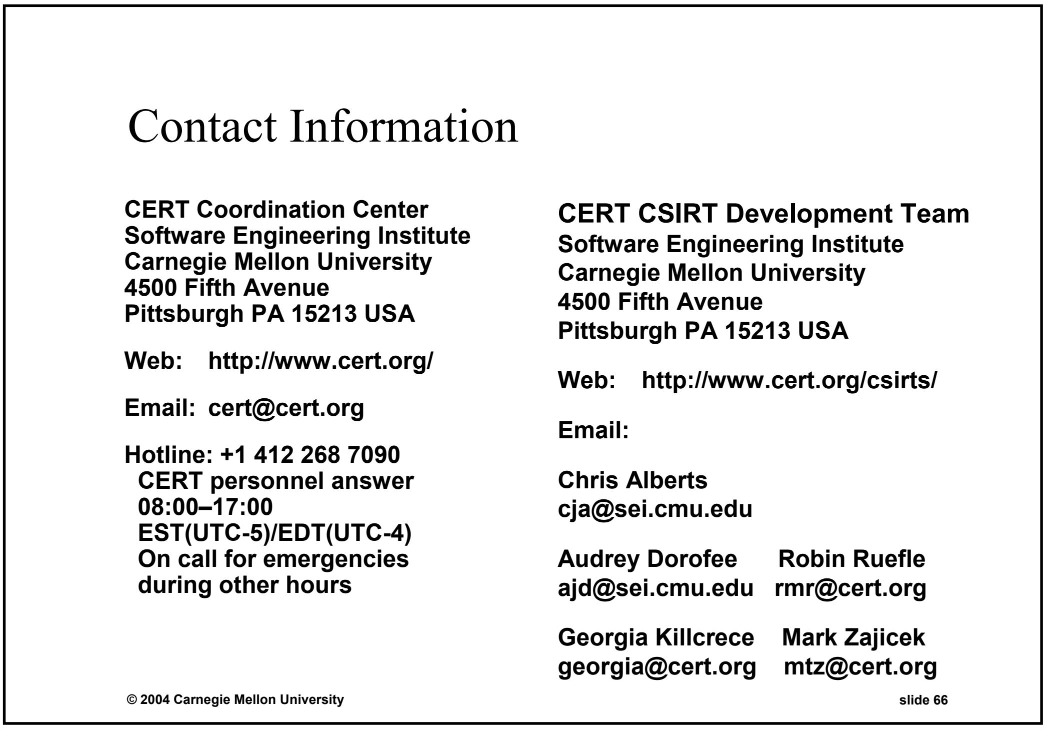
- **Sharp, Alex and McDermott, Patrick. Workflow Modeling. Artech House; Boston, MA. 2001.**
- **Jackson, Michael and Twaddle, Graham. Business Process Implementation: Building Workflow Systems. Association for Computing Machinery Press; New York, NY. and Addison-Wesley; Harlow, England. 1997.**
- **Kobielus, James G. Workflow Strategies. IDG Books Worldwide, Inc.; Foster City, CA. 1997**



References – CSIRT Information

- Handbook for CSIRTs, Second Edition
  http://www.cert.org/archive/pdf/csirt-handbook.pdf
- State of the Practice of CSIRTs
  http://www.cert.org/archive/pdf/03tr001.pdf
- Organizational Models for CSIRTs
  http://www.cert.org/archive/pdf/03hb001.pdf
- Forming an Incident Response Team
  http://www.auscert.org.au/render.html?it=2252&cid=1920
- Expectations for Computer Security Incident Response
  http://www.ietf.org/rfc/rfc2350.txt
- Computer Security Incident Handling Guide, National Institute of Standards and Technology (NIST SP 800-61)
  http://www.csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf

slide 65



Contact Information

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA 15213 USA

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

Email: cert@cert.org

Hotline: +1 412 268 7090
CERT personnel answer
08:00–17:00
EST(UTC-5)/EDT(UTC-4)
On call for emergencies
during other hours

CERT CSIRT Development Team
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA 15213 USA

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

Email:

Chris Alberts
cja@sei.cmu.edu

Audrey Dorofee   Robin Ruefle
ajd@sei.cmu.edu   rmr@cert.org

Georgia Killcrece   Mark Zajicek
georgia@cert.org   mtz@cert.org

slide 66