Risk Adaptable Access Control (RAdAC)

September 2009

Robert W. McGraw

Information Assurance Architecture and Systems Security Engineering Group

National Security Agency

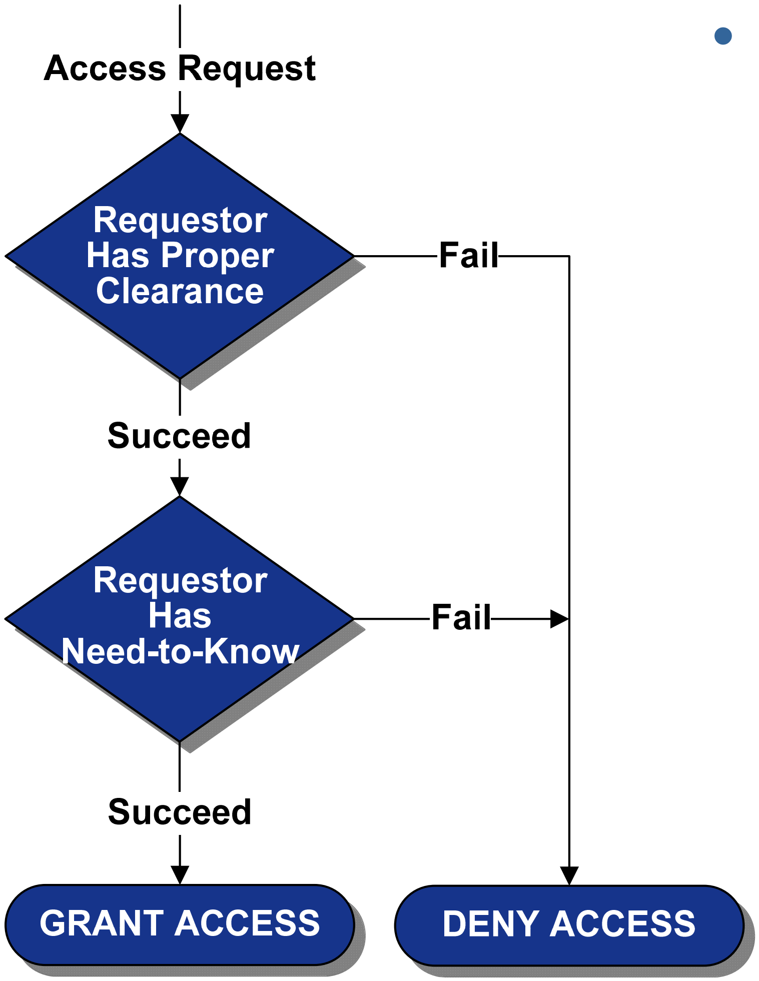
Outline

- Thinking About Access Control
  - Access Control Philosophy
  - Traditional Access Control
  - Simple Model for Access Control Considerations
- Risk Adaptable Access Control (RAdAC)
  - What is RAdAC?
  - Notional Processing
  - Functional View
  - Supporting Infrastructures
- Challenges
- Summary/Discussion/Questions

Some Access Control Philosophy Questions

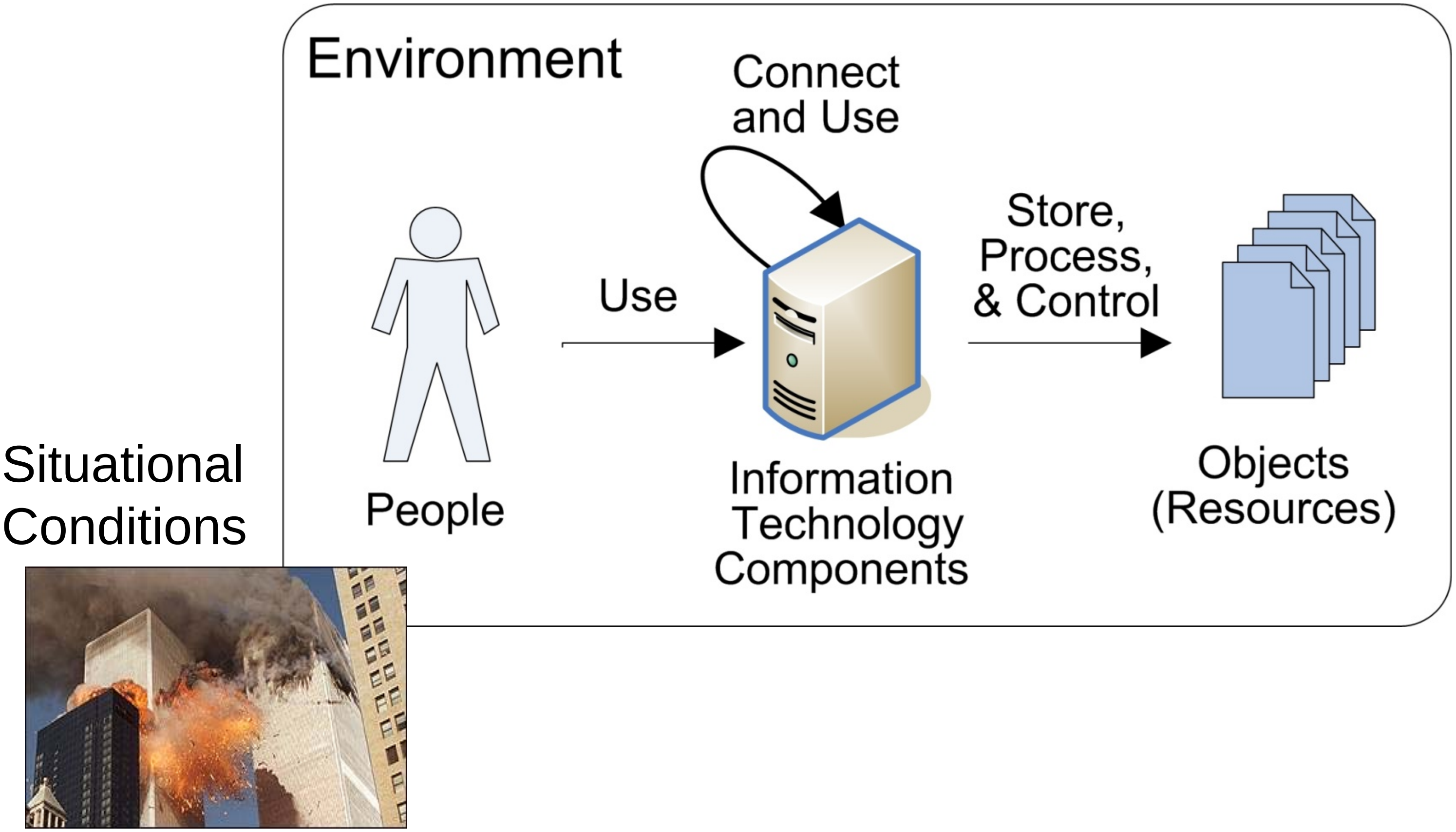
- To Share or Not?
  - Is it more important to share information or preserve its security controls?
  - Is accomplishing the mission more important than preserving the security controls on information?
  - Why not give everyone access to whatever information they request and just monitor for inappropriate behavior?
- What's the Risk?
  - How does the risk of maintaining the confidentiality of a given piece of information change as each properly cleared person is given access to it?
  - How likely is it that the confidentiality of information will be preserved after 1000 properly cleared people have been given access to it?
  - 1 million cleared people?
  - 10 uncleared but otherwise trusted people?
- Explicitly Indicate Sharing?
  - Should information include an indicator of the importance of sharing it rather than just an indicator of the consequence of loss of its confidentiality?

Traditional Access Control



- Traditional access control approaches:
  - Demand satisfaction of security controls and need-to-know
  - Assume that the risk of granting access is unacceptable if not met – no exception, protect access at all costs
  - Are inflexible – security policy is typically hard-coded into decision logic
  - Assume uniformity of people, IT components, environments and situational conditions, etc across the enterprise and time

Simple Model – Access Considerations



Environment

Connect and Use

Use

Store, Process, & Control

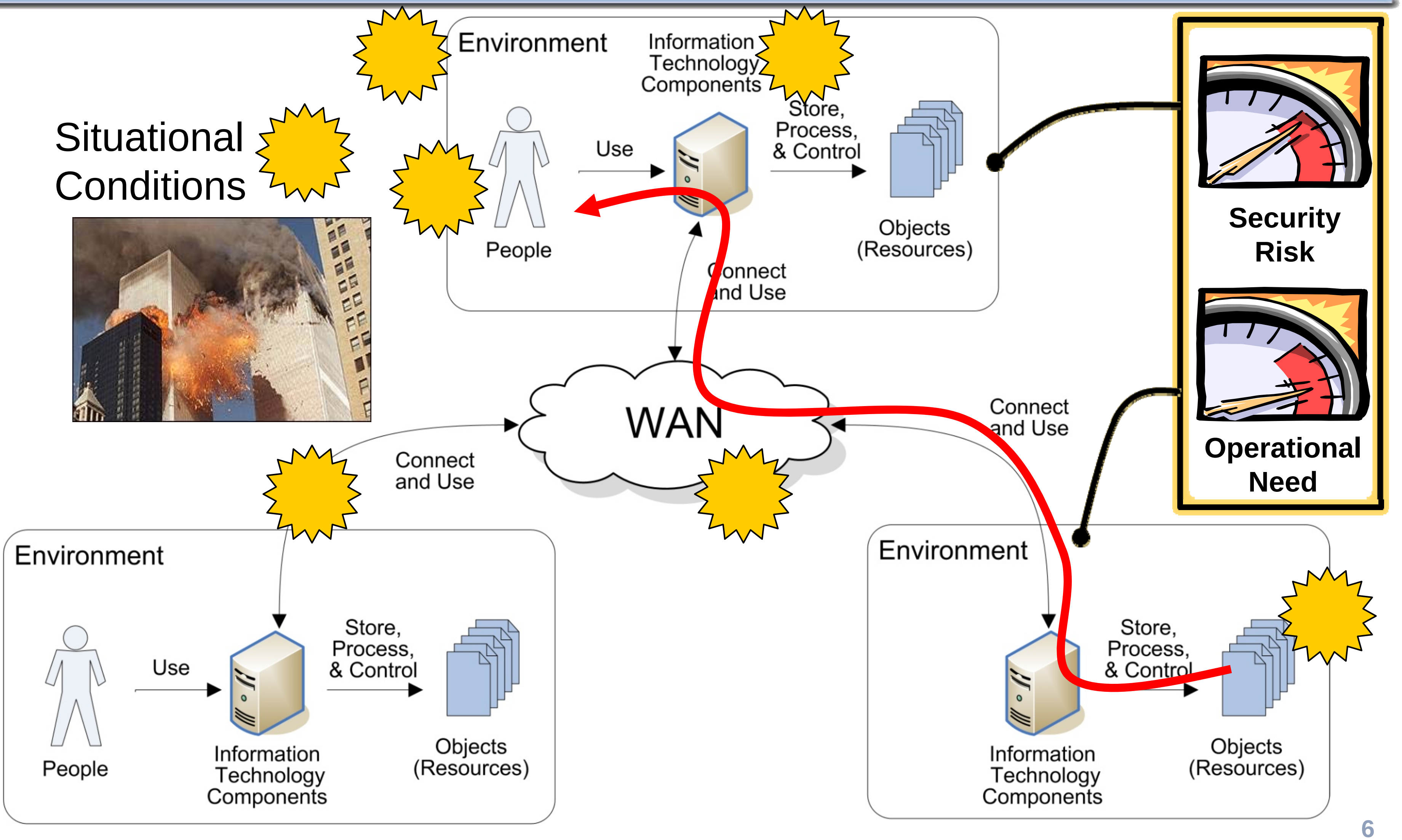
People

Information Technology Components

Objects (Resources)

Situational Conditions

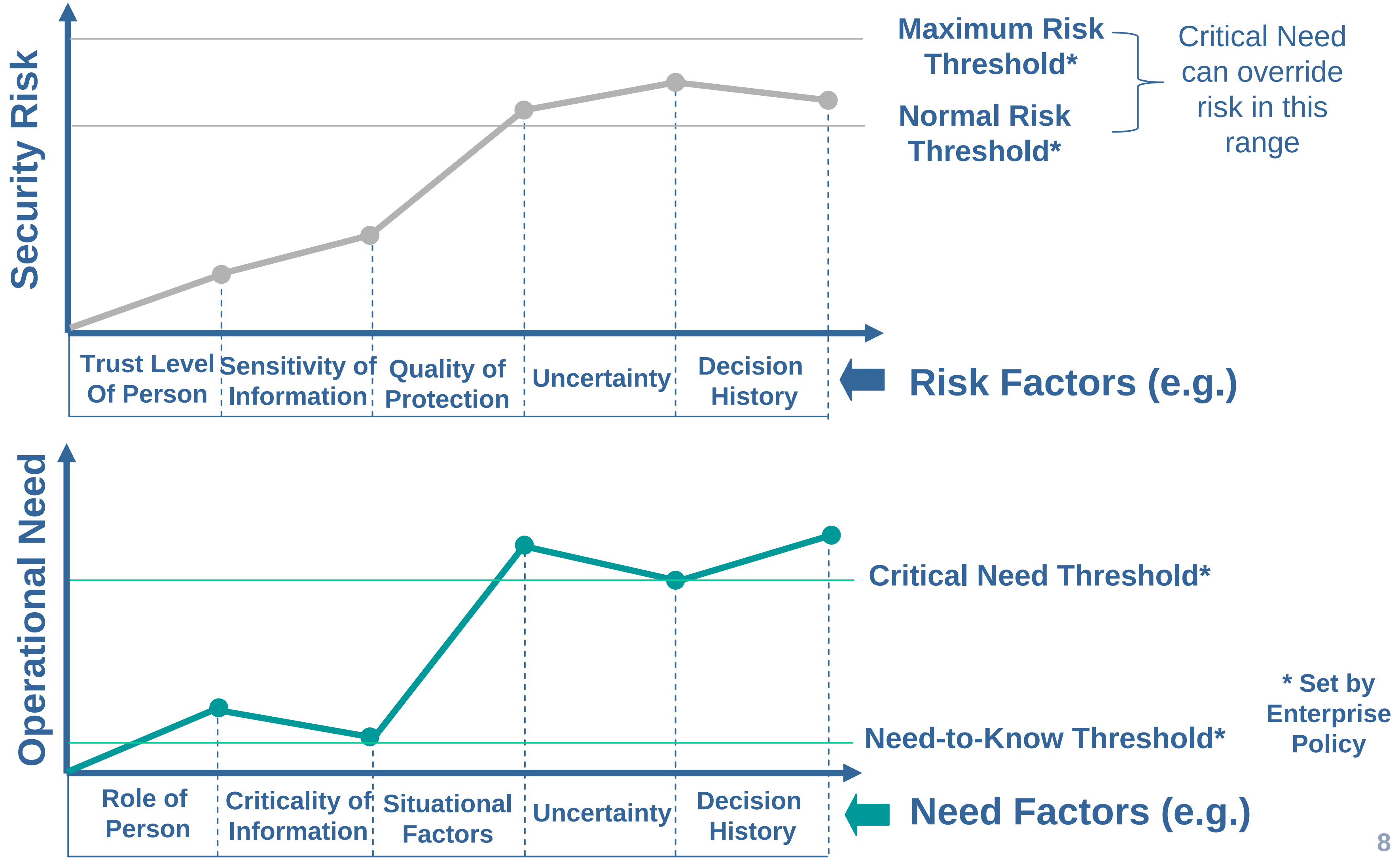
Simple Model Expanded



What is RAdAC?

- RAdAC is an access control concept that:
  - Determines access based on a **computation of *security risk* and** *operational need*, not just proper comparison of attributes
  - Considers multiple factors to determine the *security risk* and *operational need* of each access decision:
    - Trust of person requesting access
    - Sensitivity of information to be accessed
    - Quality of protection that can be afforded the information
    - Role of the person
    - Criticality of information to the operation
    - Uncertainty
    - History of access decisions
  - Can adapt its decision thresholds such that ***operational need* can trump *security risk*** when appropriate
  - Uses enterprise policies for establishing thresholds for *security risk* and *operational need* under various conditions

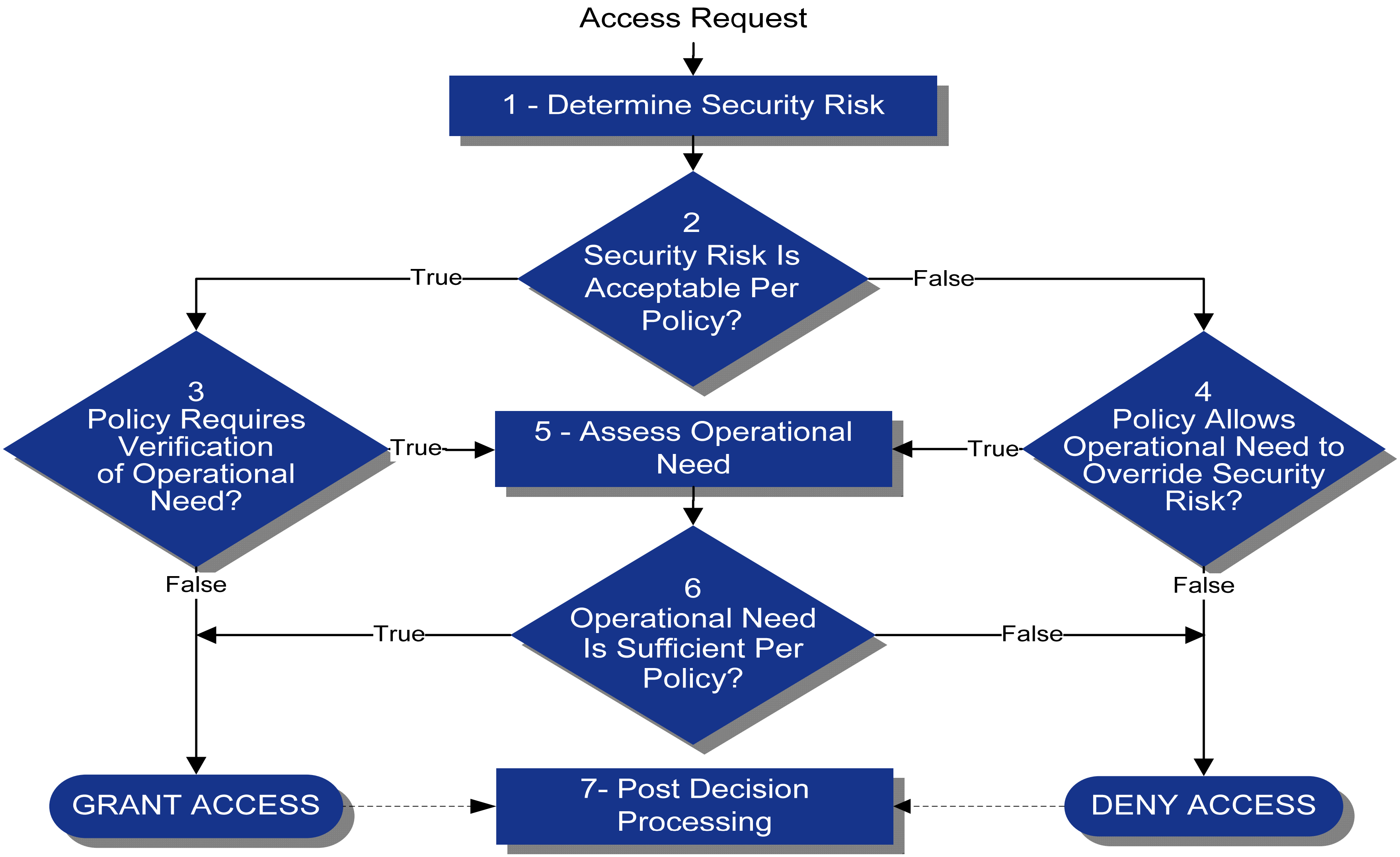
Notional Determination of Security Risk and Operational Need



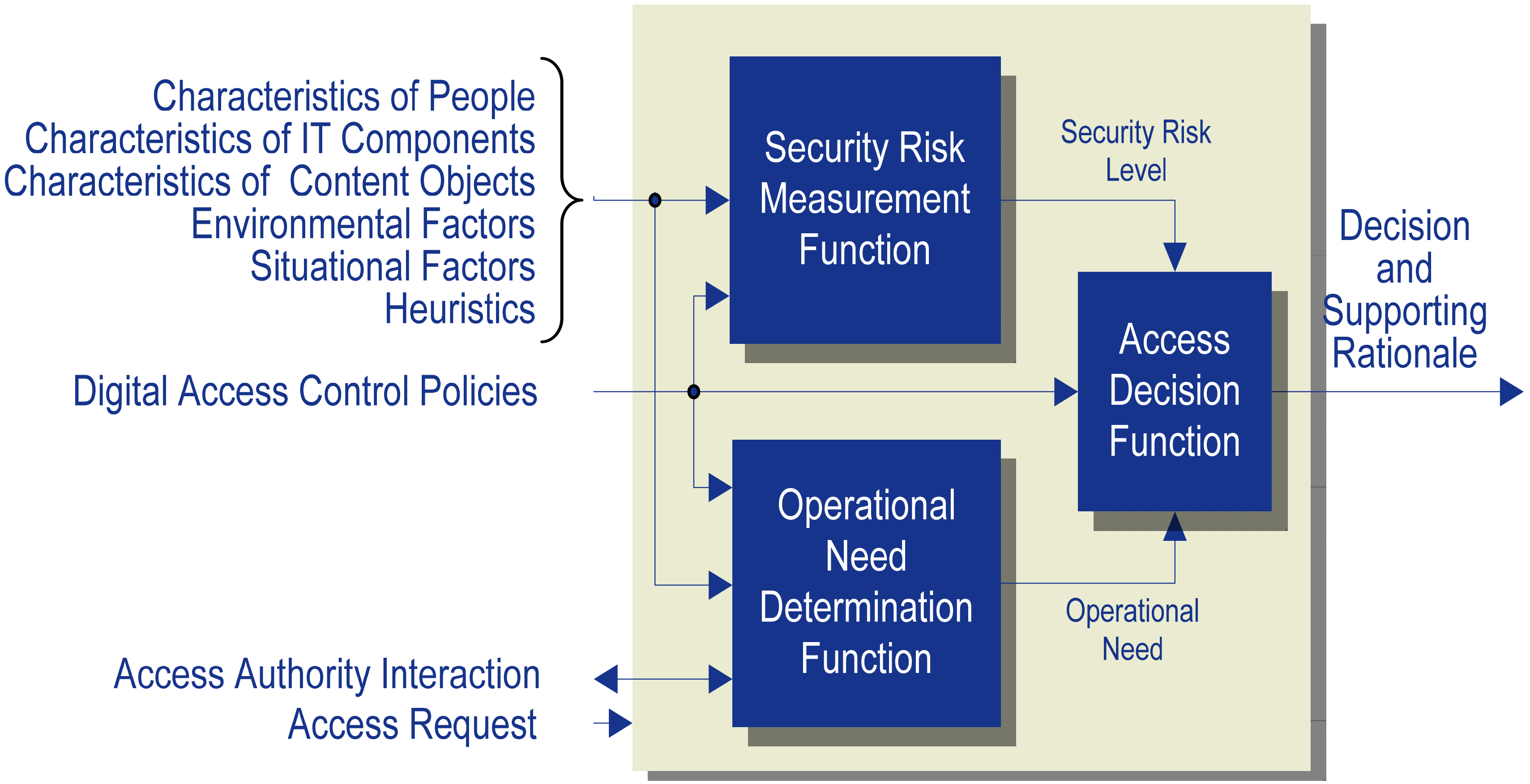
Critical Need can override risk in this range

* Set by Enterprise Policy

RAdAC Notional Process



RAdAC Functional View



Characteristics of People
Characteristics of IT Components
Characteristics of Content Objects
Environmental Factors
Situational Factors
Heuristics

Digital Access Control Policies

Access Authority Interaction
Access Request

Security Risk Measurement Function

Security Risk Level

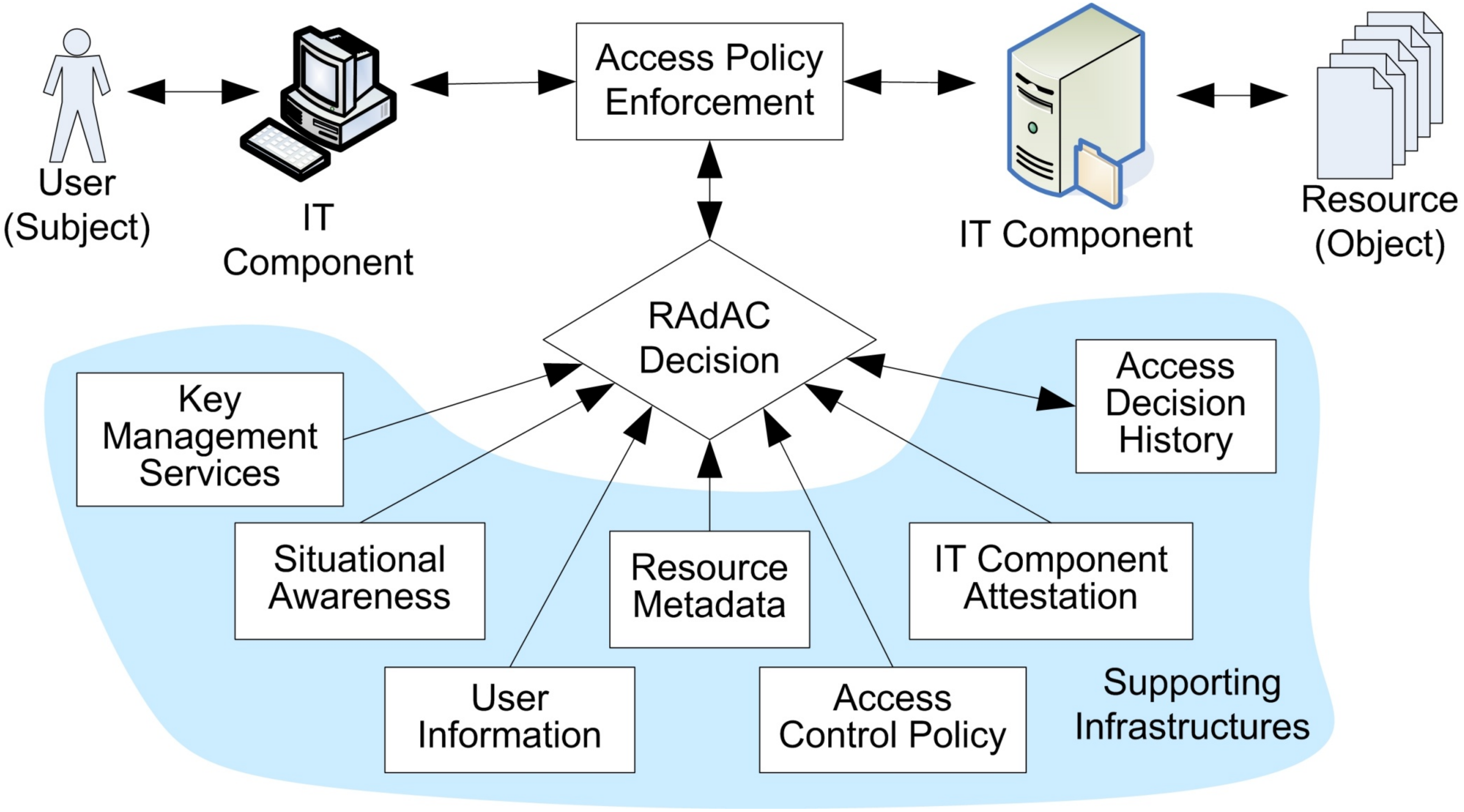
Access Decision Function

Decision and Supporting Rationale

Operational Need Determination Function

Operational Need

RAdAC and Supporting Infrastructures



Some Challenges

- Making all of the data available that would be needed to make a risk-based decision
- Calculating security risk of each access decision – real time
- Determining operational need
- Quantifying trust in people other than through a security clearance
- Quantifying the trust level of IT components and systems.
- Determining the location of IT components/client systems and quantifying the adversarial threat in that location
- Heuristics as applied to access control decisions and improving access control decisions
- Revoking access to information

Summary and Questions