Emerging IT Trends and their Implications to the C&A Process

Annual Computer Security Applications Conference (ACSAC ’07)

12 December 2007

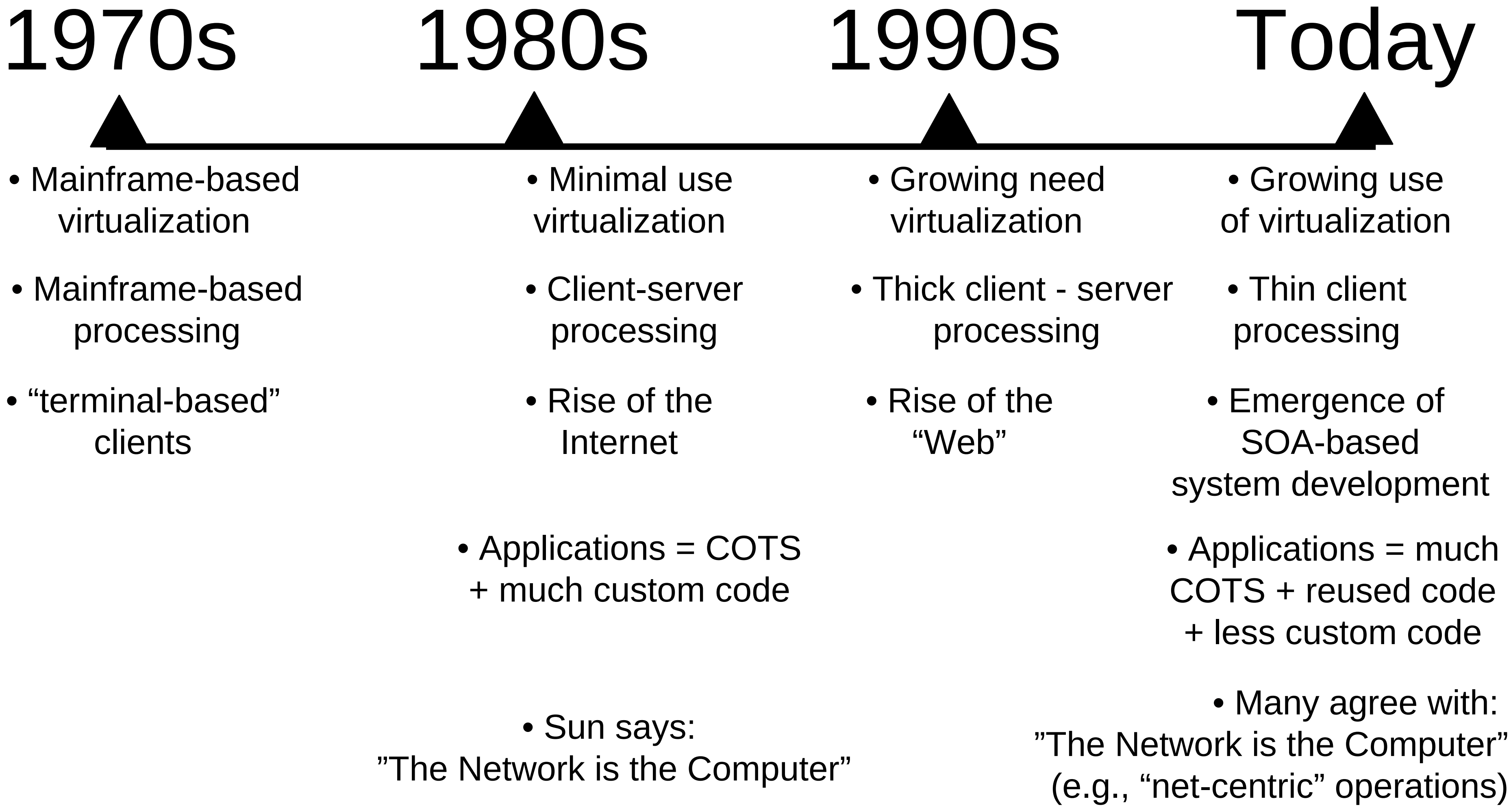
Edward Rodriguez
Booz Allen Hamilton

Booz | Allen | Hamilton

Agenda

- IT Technological Trends
- Evolution of C&A and Current Revitalization Efforts
- C&A Challenge
- Candidate Concepts

Evolution of IT



1970s

- Mainframe-based virtualization
- Mainframe-based processing
- “terminal-based” clients

1980s

- Minimal use virtualization
- Client-server processing
- Rise of the Internet
- Applications = COTS + much custom code
- Sun says: ”The Network is the Computer”

1990s

- Growing need virtualization
- Thick client - server processing
- Rise of the “Web”

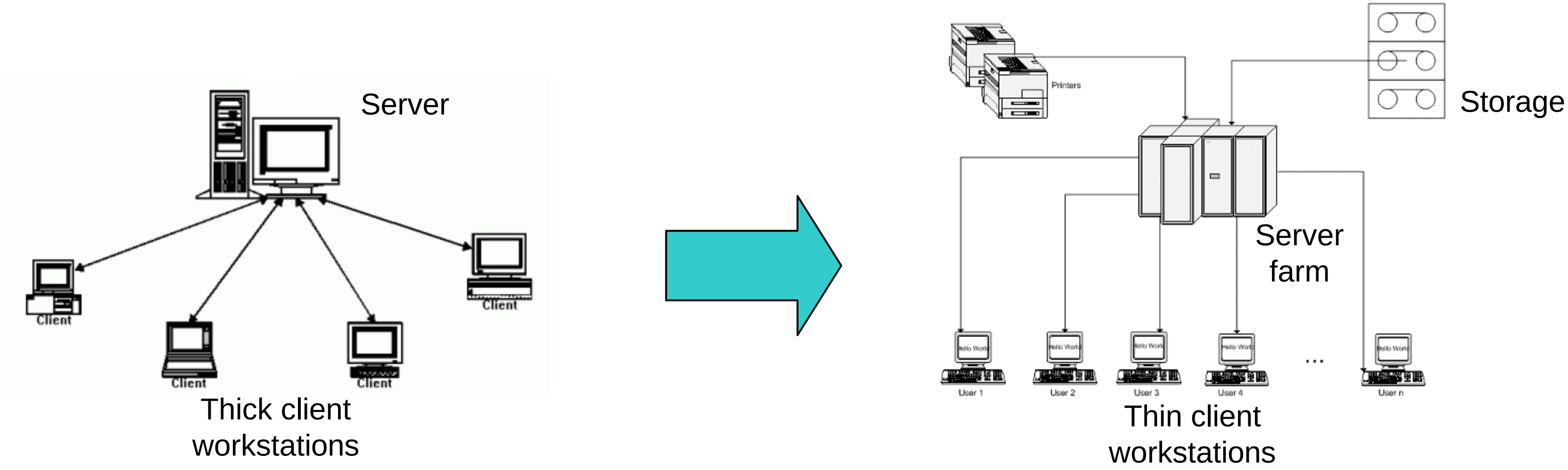
Today

- Growing use of virtualization
- Thin client processing
- Emergence of SOA-based system development
- Applications = much COTS + reused code + less custom code
- Many agree with: ”The Network is the Computer” (e.g., “net-centric” operations)

Significant Threads in that Evolution

- Greater emphasis on establishing a measurable Return on Investment (ROI) for IT investments and lowering the Total Cost of Ownership (TCO)

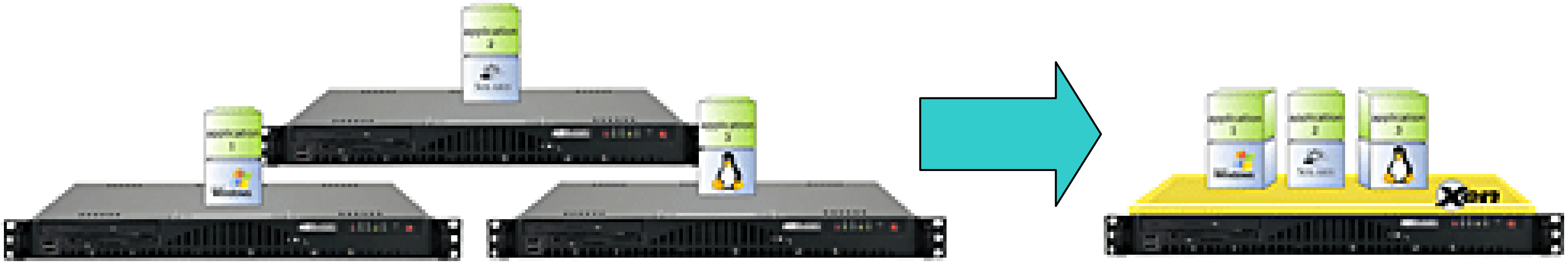
  RESULT: Migration back toward thin client processing which in turn requires ***more server-based processing*** capability



Significant Threads in that Evolution

- Majority of deployed servers are based on commodity X86 CPUs that are relatively inexpensive and substantially underutilized (typically 10%-20%)

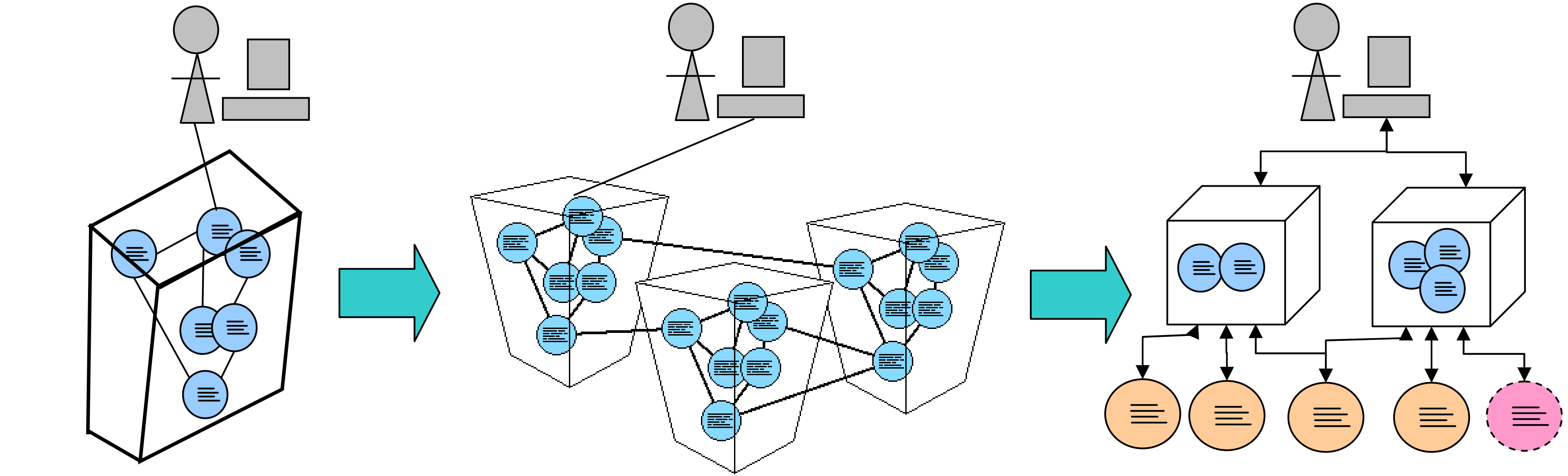
  RESULT: Growing appreciation for the increasing infrastructure costs associated with these large number of servers (e.g., space, cooling, and power). Major motivator for the ***virtualization of computer resources***



Significant Threads in that Evolution

- Growing use and evolution of software "components". Further those components over time have grown in complexity.

  RESULT: Evolution of target systems from highly stove piped implementations toward ***integrated systems that are adaptive, component-based and maximize reuse***.



Standalone, stove piped system

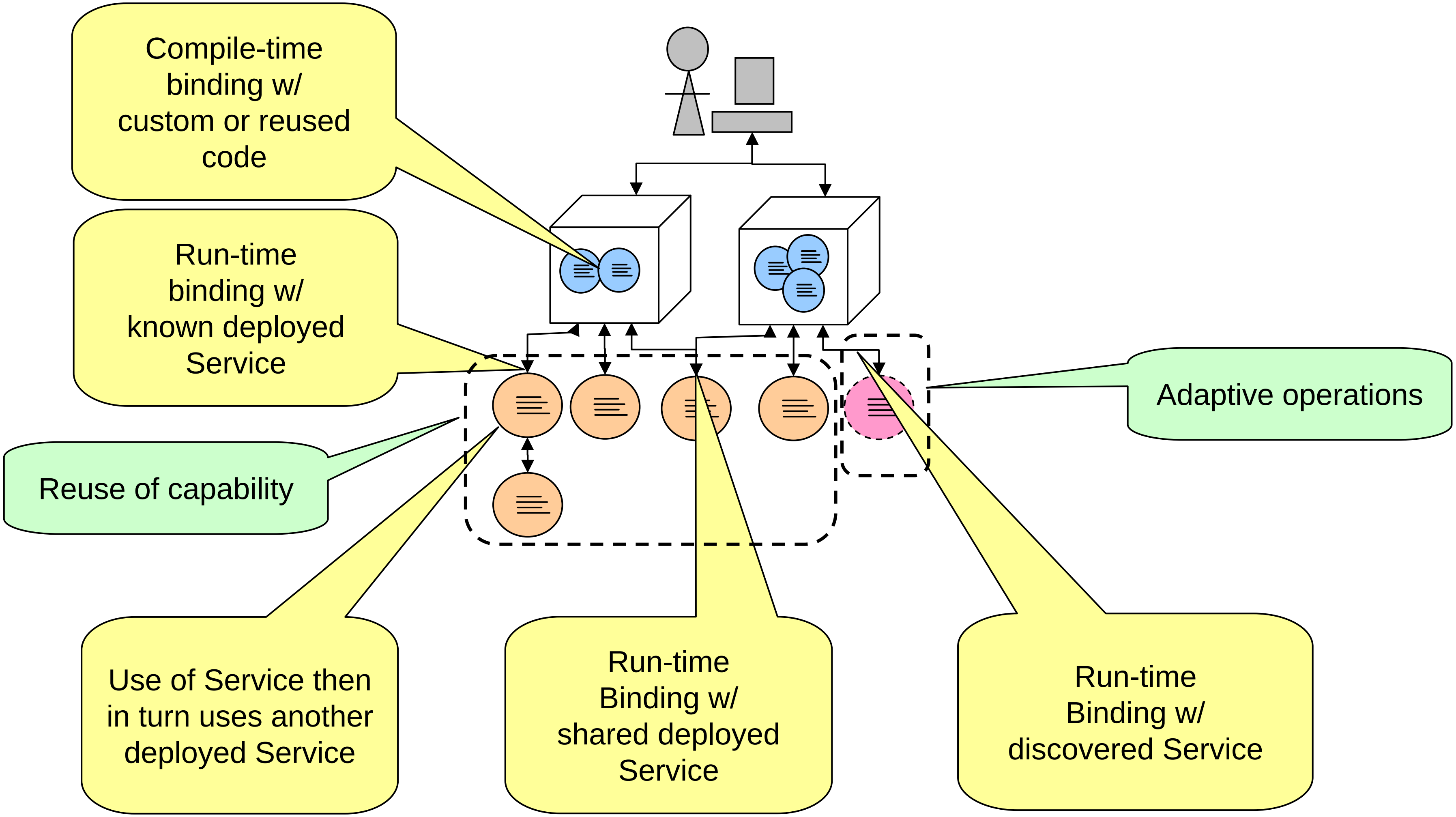
Integrated, stove piped enterprise

Component-based, adaptive enterprise

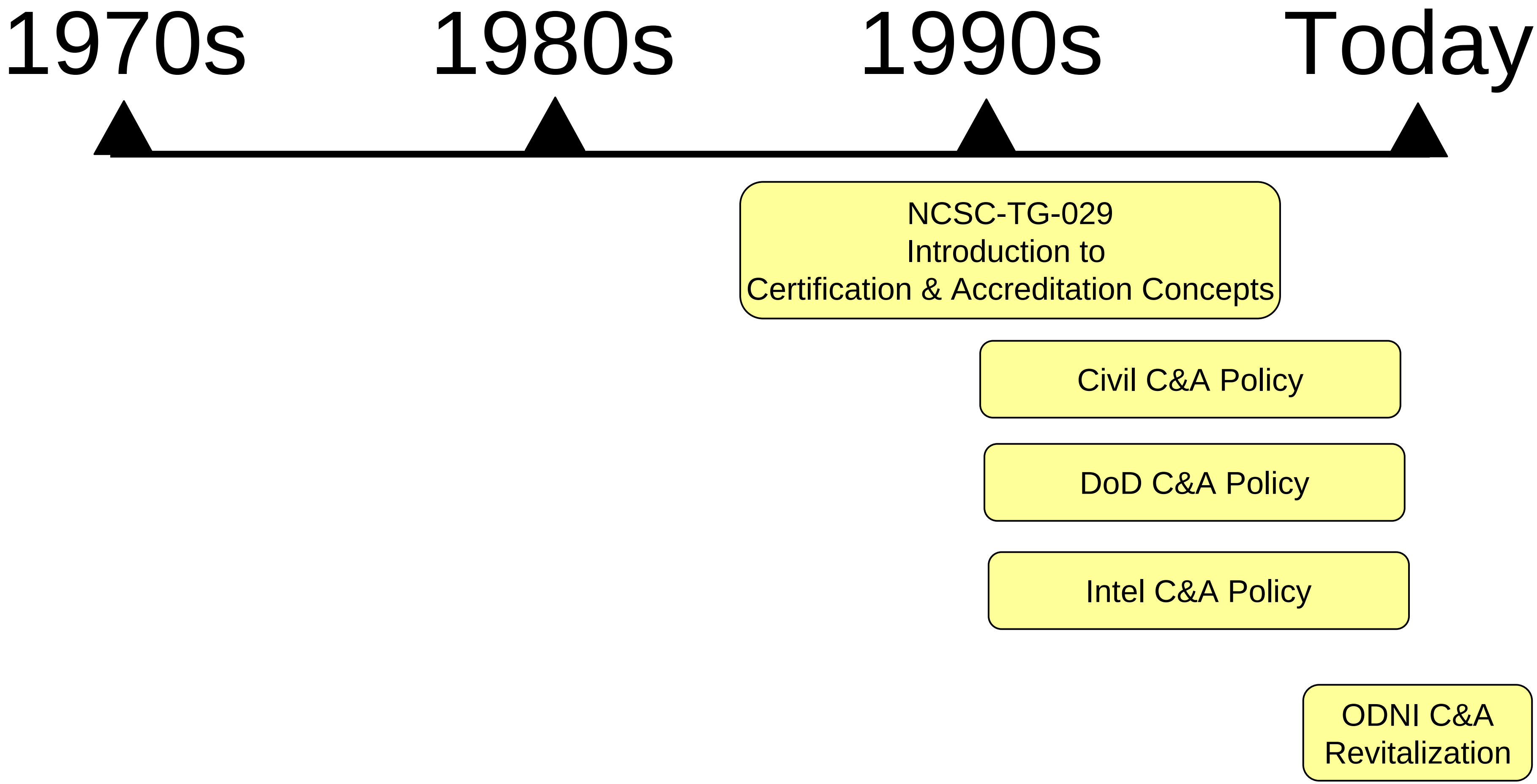
Booz | Allen | Hamilton

More on this later

Key Architectural Features


Compile-time binding w/ custom or reused code
Run-time binding w/ known deployed Service
Reuse of capability
Adaptive operations
Use of Service then in turn uses another deployed Service
Run-time Binding w/ shared deployed Service
Run-time Binding w/ discovered Service

Evolution of C&A



1970s

1980s

1990s

Today

NCSC-TG-029
Introduction to
Certification & Accreditation Concepts

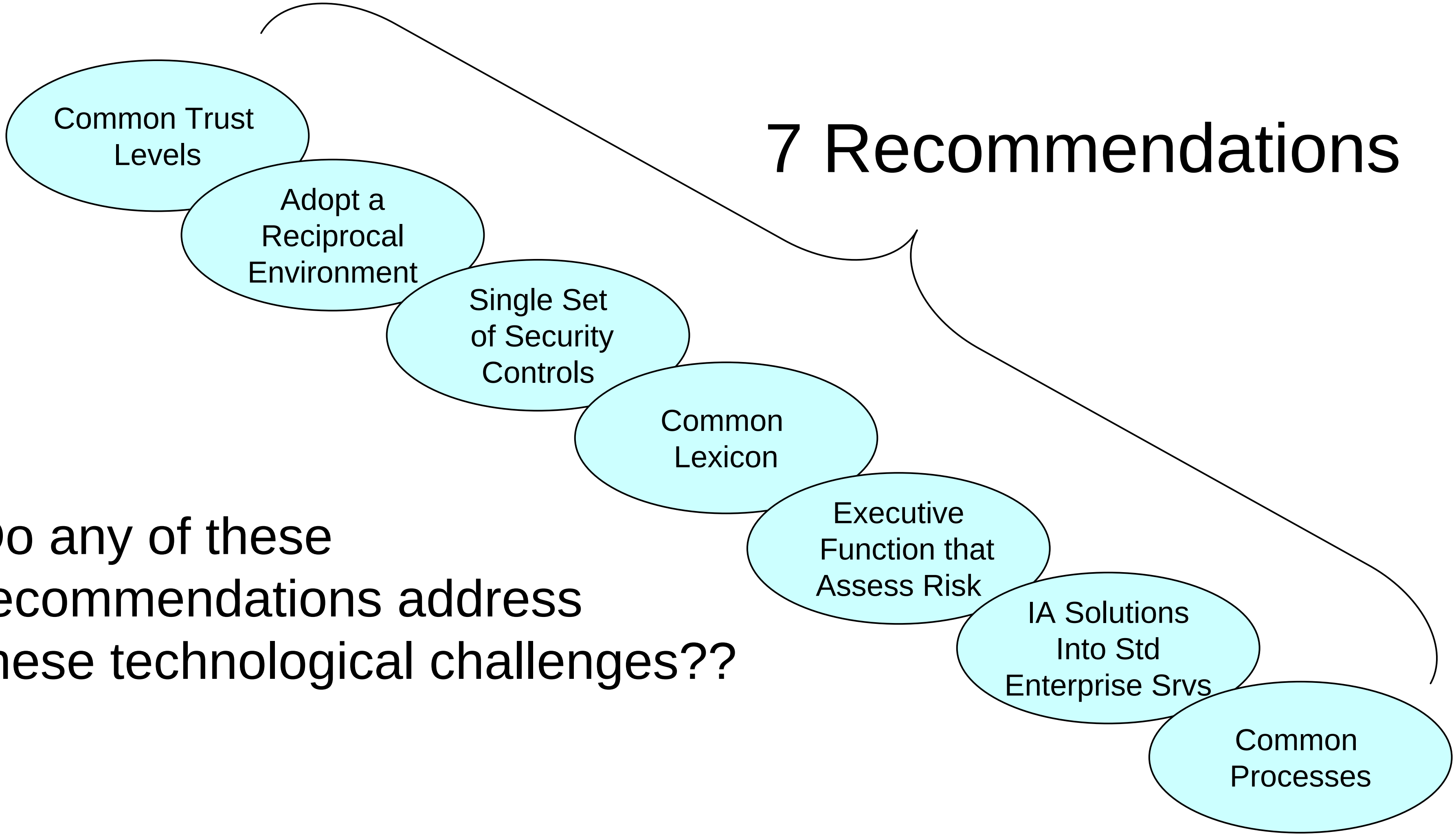
Civil C&A Policy

DoD C&A Policy

Intel C&A Policy

ODNI C&A
Revitalization

Expectations from this C&A Revitalization Effort



7 Recommendations

Common Trust Levels

Adopt a Reciprocal Environment

Single Set of Security Controls

Common Lexicon

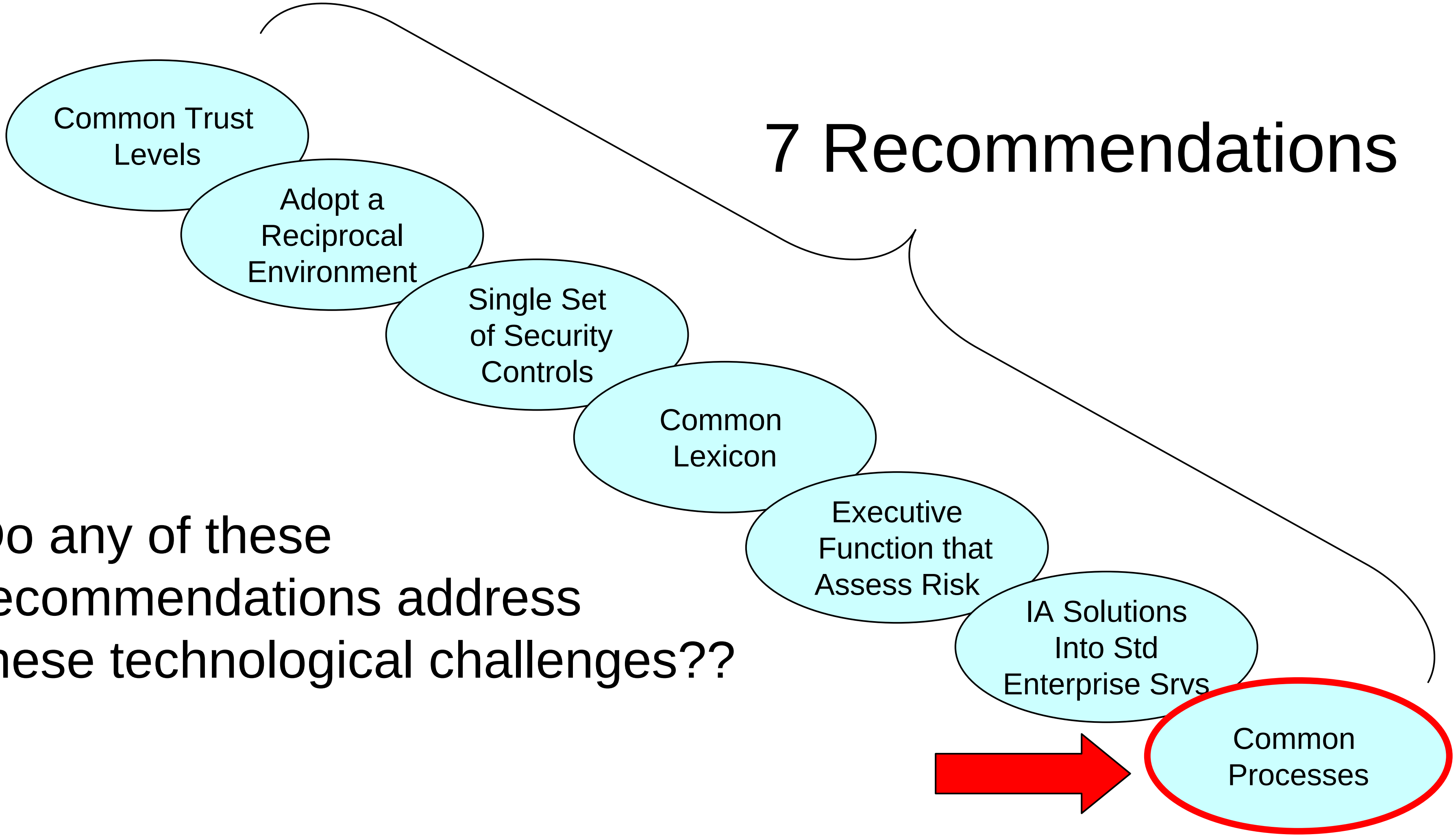
Executive Function that Assess Risk

IA Solutions Into Std Enterprise Srvs

Common Processes

Do any of these recommendations address these technological challenges??

Expectations from this C&A Revitalization Effort



7 Recommendations

Common Trust Levels

Adopt a Reciprocal Environment

Single Set of Security Controls

Common Lexicon

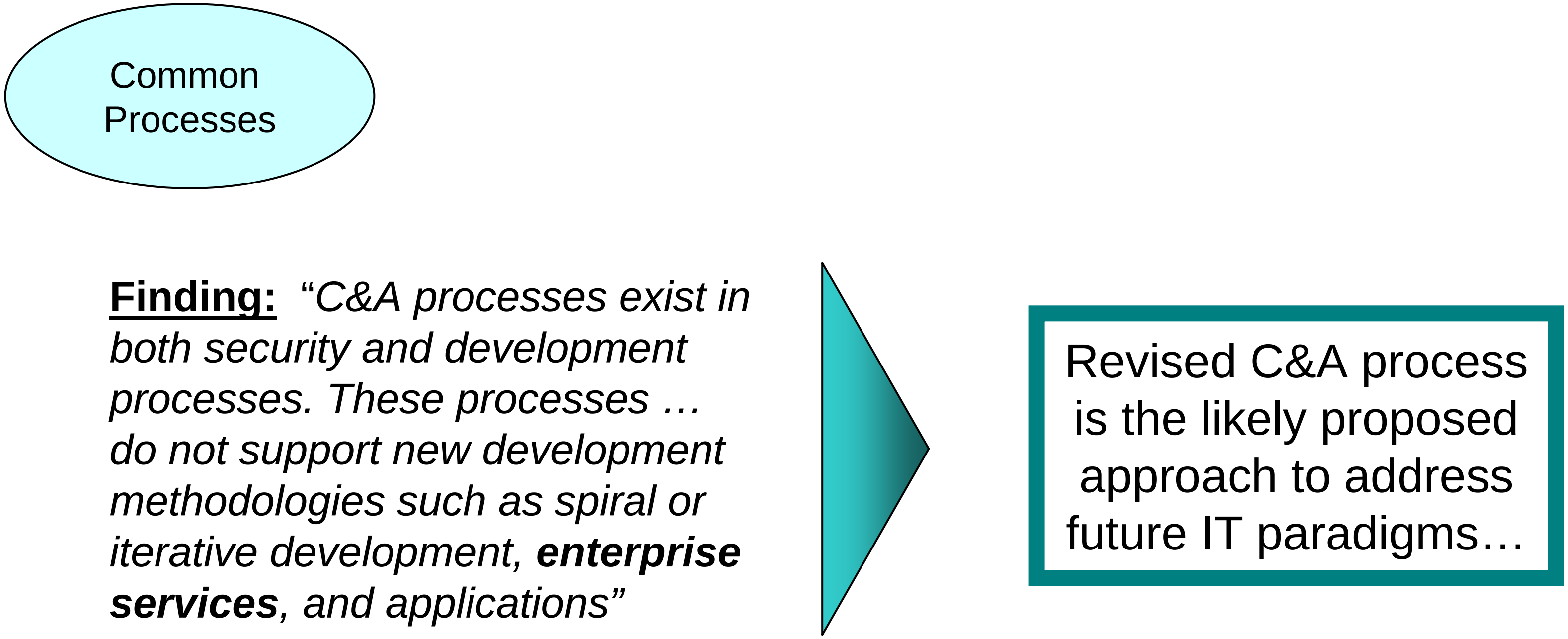
Executive Function that Assess Risk

IA Solutions Into Std Enterprise Srvs

Common Processes

Do any of these recommendations address these technological challenges??

“Common Processes” Recommendation
- Findings



Common Processes

<u>Finding:</u> *“C&A processes exist in both security and development processes. These processes … do not support new development methodologies such as spiral or iterative development, **enterprise services**, and applications”*

Revised C&A process is the likely proposed approach to address future IT paradigms…

<u>Source</u>: Certification and Accreditation Revitalization Findings and Recommendations Report – May 2007

“Common Processes” Recommendation
- Recommendation

Common Processes

Recommendation: “… adopt a common process that uses as its basis an integrated approach to security reengineering within a *lifecycle* rather than a separate or parallel process…”

… however, (as expected in this type effort) there is no specific methodology or approach presented that addresses the identified IT challenges

Source: Certification and Accreditation Revitalization Findings and Recommendations Report – May 2007

Booz | Allen | Hamilton

C&A Challenge

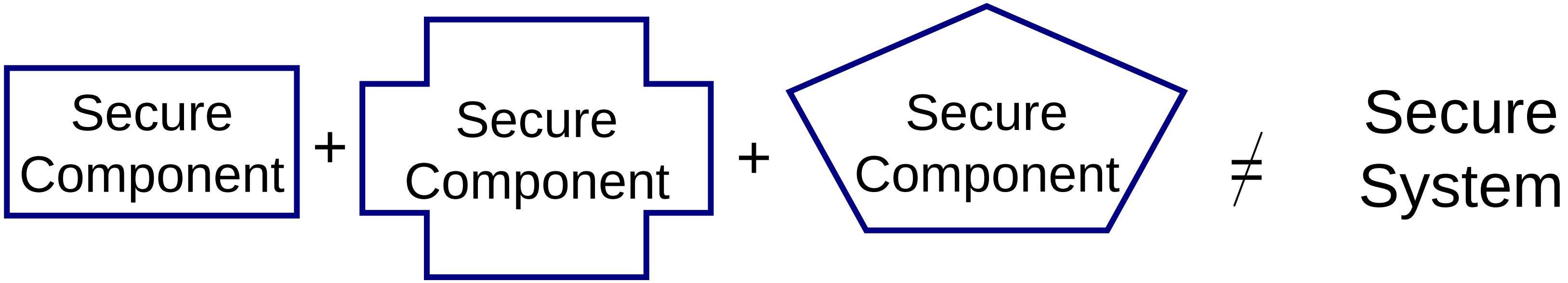
- C&A practitioners accustom to addressing static systems
  - Functionality static at build time
  - Interfaces are also static as well as well defined

- C&A revitalization efforts recognizes the existence of challenges presented by emerging/future system that employ
  - reused shared services
  - real time, adaptive behavior

- Widely vetted, innovative security system engineering processes need to be developed that can be consistently used across the community

- Let’s recap a few important tenets…

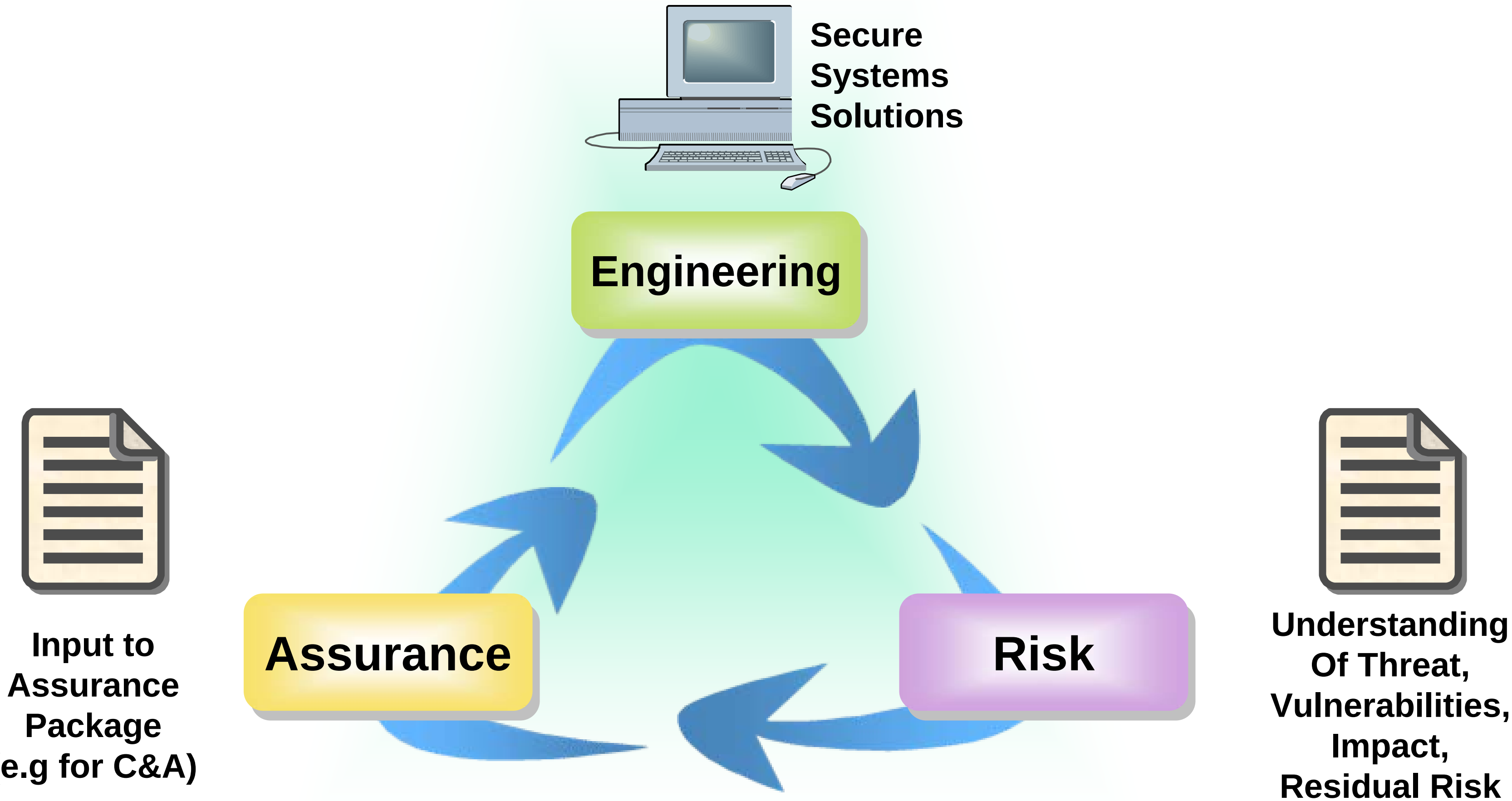
Security Tenet 1
– Sum of the parts…



Secure Component + Secure Component + Secure Component ≠ Secure System

When it comes to security,
the whole is **<u>not</u>** greater than the sum of the individual parts…
unless suitable Information System Security Engineering (ISSE)
is performed

Security Tenet 2
– *Security Triad*



Secure Systems Solutions

Engineering

Assurance

Risk

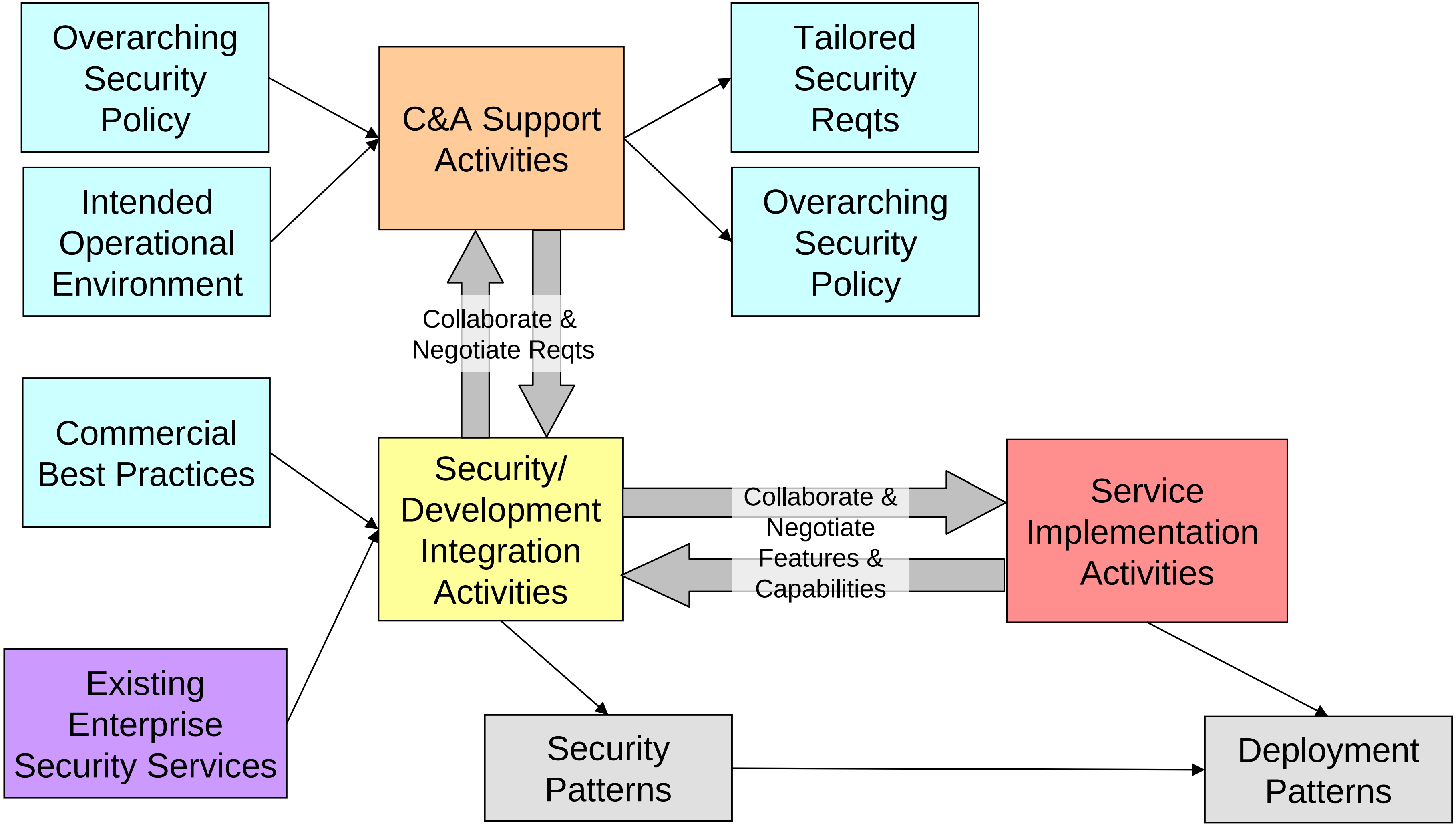
Input to Assurance Package (e.g for C&A)

Understanding Of Threat, Vulnerabilities, Impact, Residual Risk

Candidate Concepts

- Likely to include architectural guidelines (ala, architectural patterns or exemplars)
  - No share services across domains
  - Specific use and positioning of cross domain solutions (CDS)
  - TBD
- Likely to also include ISSE processes that address:
  - “type or platform certification”. A process that develops and subsequently certifies a specific reusable component or set of components for use by developers of new systems in an assured manner
  - the upgrade of COTS components due to deprecation or enhanced functionality
  - TBD

Some Process Related Thoughts


Overarching Security Policy
Intended Operational Environment
C&A Support Activities
Tailored Security Reqts
Overarching Security Policy
Collaborate & Negotiate Reqts
Commercial Best Practices
Security/ Development Integration Activities
Collaborate & Negotiate Features & Capabilities
Service Implementation Activities
Existing Enterprise Security Services
Security Patterns
Deployment Patterns

Booz | Allen | Hamilton

Final Thoughts

- The ability to efficiently and effectively perform C&A on increasingly complex target systems is a very hard problem
- C&A Revitalization initiative offers a window of opportunity to address these “game changing” new paradigms.
- Community wide involvement and participation will be required to develop these new processes as well as to get buy-in for subsequent use

Thanks

Ed Rodriguez
Senior Associate

Booz | Allen | Hamilton

Tel (301) 543-4660
rodriguez_ed@bah.com

Booz | Allen | Hamilton

delivering results that endure