Take a (Closer) Look at Business Continuity

IIA/ISACA Dallas

Robert Giffin (CBCP, CISA)
Director, Avalution Consulting

AVALUTION CONSULTING

Agenda

- Business Continuity Defined
- Current Trends in Business Continuity
- Current Trends in Disaster Recovery
- Top 10 Considerations when Auditing Business Continuity
- Additional Resources

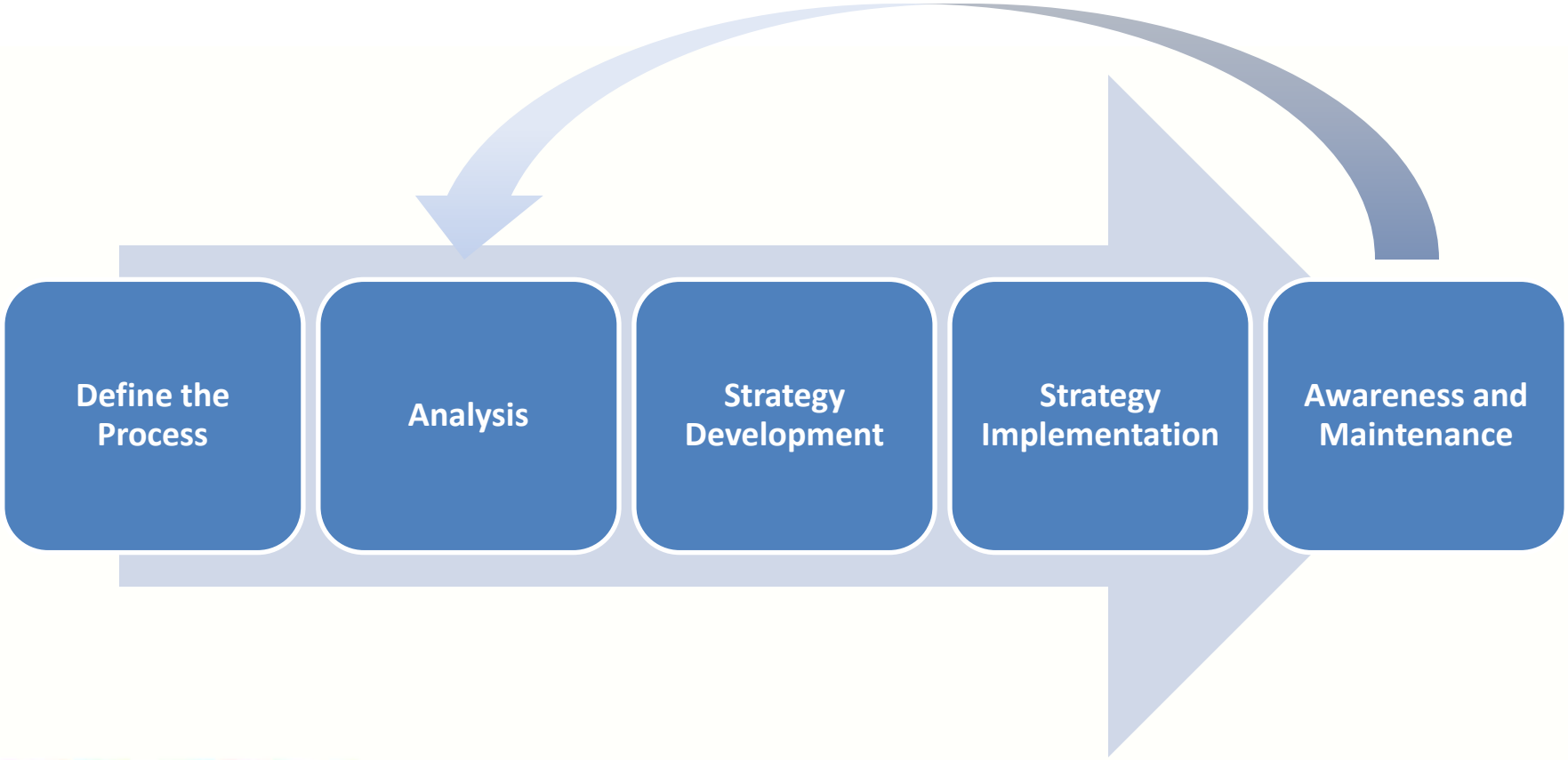
AVALUTION CONSULTING

Business Continuity Defined

Recurring activities designed to mitigate the risk associated with disruptive incidents and enable the organization to recover its most important business processes in a timely manner.

AVALUTION CONSULTING

“Traditional” Business Continuity



AVALUTION CONSULTING

Trends in Business Continuity

- Departure from an IT centric view
  - Loss of all critical resources – facilities, equipment, people, technology, information/data, business partners
  - Strong focus on vendor and third party reliability following events in Japan and Thailand (2011)
- Less emphasis on financial loss as the singular driver for investment in preparedness
- Plans aren't enough – (proven) capabilities matter

AVALUTION CONSULTING

Trends in Business Continuity (cont.)

- The bottom-up and top-down BIA:
  Product and service-driven scoping

- The role for senior management is defined:
  International standards and management system concepts driving maturity

- PS-Prep program may become a key driver for highly critical B2B organizations
  - Regardless, most preparedness activity is driven by regulatory mandates, customer inquiry and **audit pressure**

AVALUTION CONSULTING

Disaster Recovery Trends

- “Environment of Control” Drives Adoption
- ITIL = Standardization
- Virtualization = Simplification
- “Cloud Backup and Recovery”
- DR Built into Operations

AVALUTION CONSULTING

Common Cloud Assumptions

- Clouds are ‘always on’ and include high availability and/or disaster recovery
- Data is protected in a cloud
- Data is retrievable from a cloud
- Clouds are available from anywhere

AVALUTION CONSULTING

Top 10 Audit Considerations

I. Management meaningfully engaged
   - Scope, objectives, resources and prioritization of improvement opportunities

II. Prioritization confirmed by management (BIA)

III. Consideration of the most likely threats/scenarios

IV. Capabilities in place
   - Alternate sites, alternate processes, manual workarounds, communications, alternate vendors

V. Capabilities demonstrated
   - Through exercises/testing, or actual responses to disruption

AVALUTION CONSULTING

Top 10 Audit Considerations (cont.)

VI. Governance mechanisms to set expectations
  - Policy, SOP/framework, etc.

VII. Look beyond DRI and BCI best practices

VIII. Identify “artificialities”

IX. Employees know their role
  - Including management, who must build unique capabilities to manage a response to a disruptive incident

X. Preparedness embedded in organizational change processes

AVALUTION CONSULTING

Where Can I Learn More?

Standards & Frameworks

- BS 25999-2 (2007)
- NFPA 1600 (2010)
- ISO 22301 (Future)
- ITIL Framework (Service Continuity)
- COBIT (DS4)
- ISO 27031
- ISO 27001 (Partial)

Professional Associations

- DRI International (DRI)
- The Business Continuity Institute (BCI)

Regulations

- Mainly for: Financial Services, Energy, Healthcare, Life Sciences, and Government

www.avalution.com/Resources/Standards

AVALUTION CONSULTING

Questions? Contact Information…

Robert Giffin

Director of Technology

robert.giffin@avalution.com

866.533.0575

www.avalution.com

perspectives.avalution.com

AVALUTION CONSULTING