Provisions and Guidelines for Business Continuity Management

Dhr. C. Walters

June 28, 2010

Why impose rules for Business Continuity Management ?

- Supervised institutions have been requesting rules;
- Rules promotes clarity amongst all stakeholders;
- Rules supports safe and sound practices; and
- Promotes the maturity level.

Which supervised institutions should comply?

- All institutions supervised by the BNA should comply to the new rules;
- However, the rules set out only high level principles supervised institutions need to adhere to;
  - The BNA does not imply how much money should be invested; or
  - What systems need to be bought; or
  - What physical security features should be in place; or
  - If an institution needs a cold, warm or hot site.

Responsibilities for stakeholders

- The extent to which inherent risks are mitigated is the responsibility of the supervised institution;
- The institution's external auditor, its internal auditor and the Bank's supervision auditor will verify if the principles provided in the Provisions for BCM are adhered to and if controls are in place to ensure that inherent risks are managed adequately.

Principle 1

- **The Board of Supervisory Directors and the Board of Managing Directors should establish effective management oversight with respect to potential events that threatens the continuity of the business operations of supervised institutions.**

Principle 2

- **Supervised institutions should prepare business continuity plans to recover from disruptive events in a timely and controlled fashion.**

Principle 3

- **Supervised Institutions should train personnel and test the business continuity plans, evaluate their effectiveness, and update the plans as appropriate.**

Principle 4

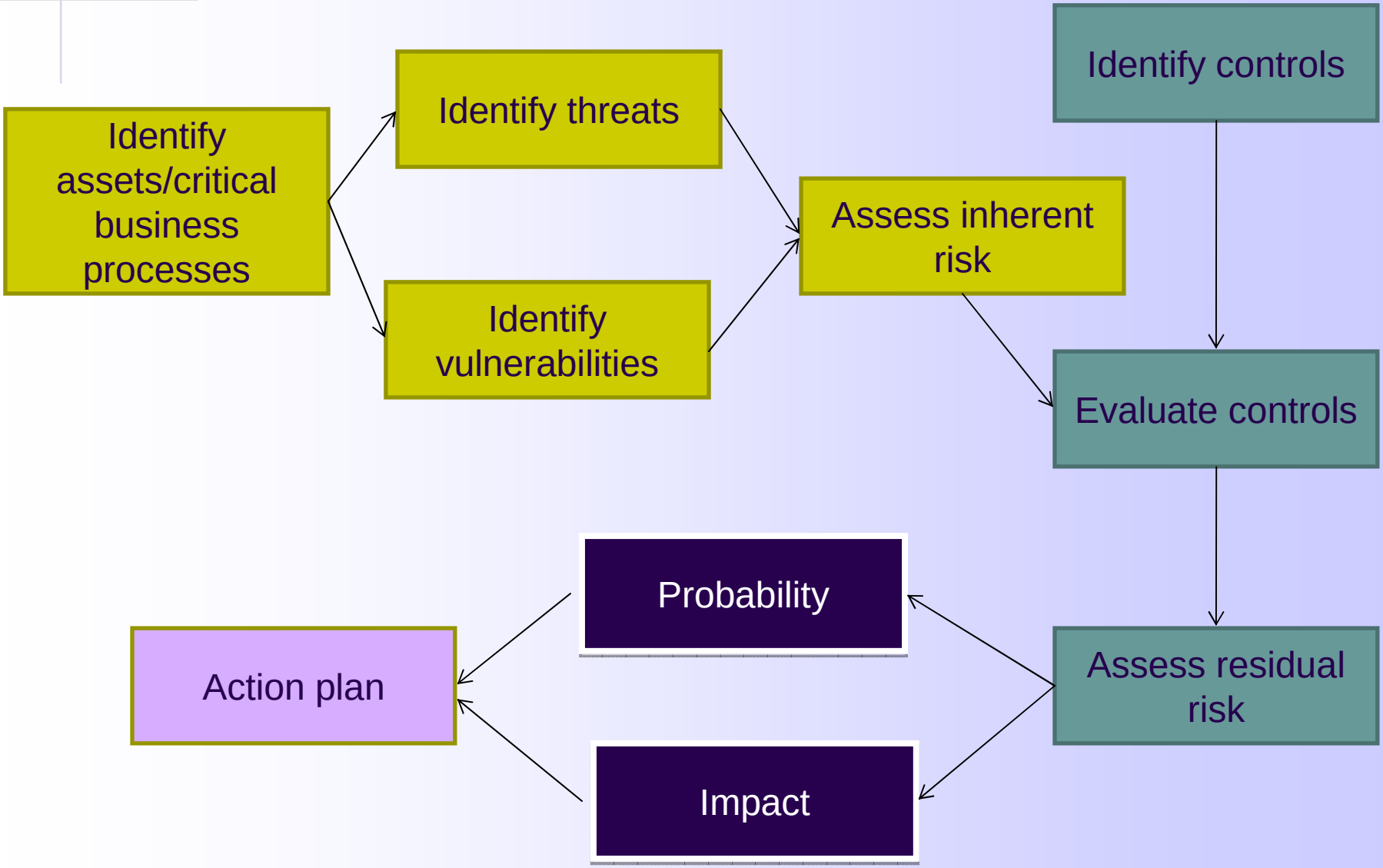
- **Supervised Institutions should embed the update of business continuity plans into policies, standards and procedures of activities/processes which affect the plans**

Principle 5

- **Supervised Institutions should ensure the quality of all aspects of BCM by assessing independent audits**

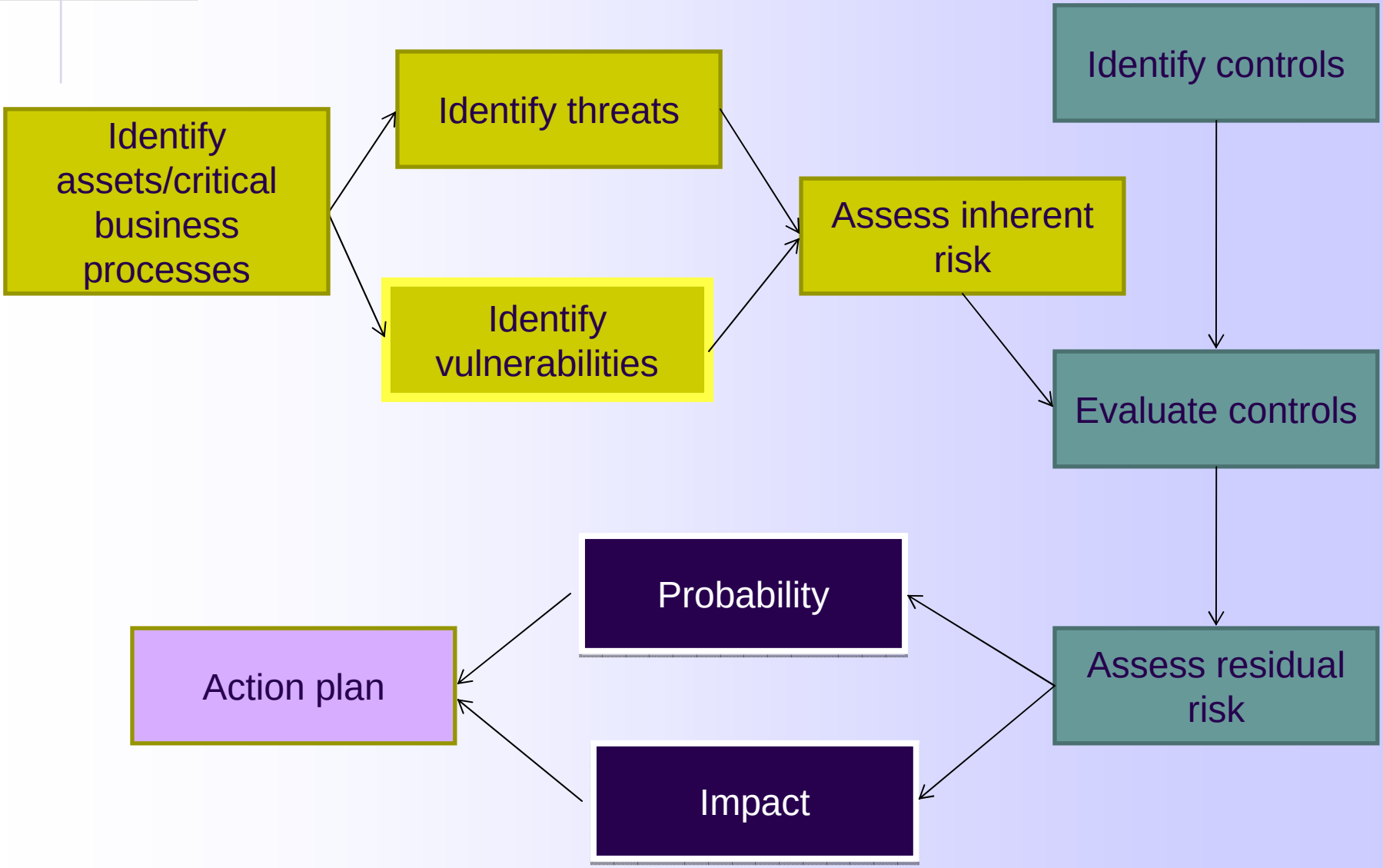
Start of any BCM plan

1. Initiate a project and allocate sufficient knowledgeable personnel;
2. Perform a risk assessment and business impact analyses;


Identify assets/critical business processes
Identify threats
Identify vulnerabilities
Assess inherent risk
Identify controls
Evaluate controls
Assess residual risk
Probability
Impact
Action plan

Threats

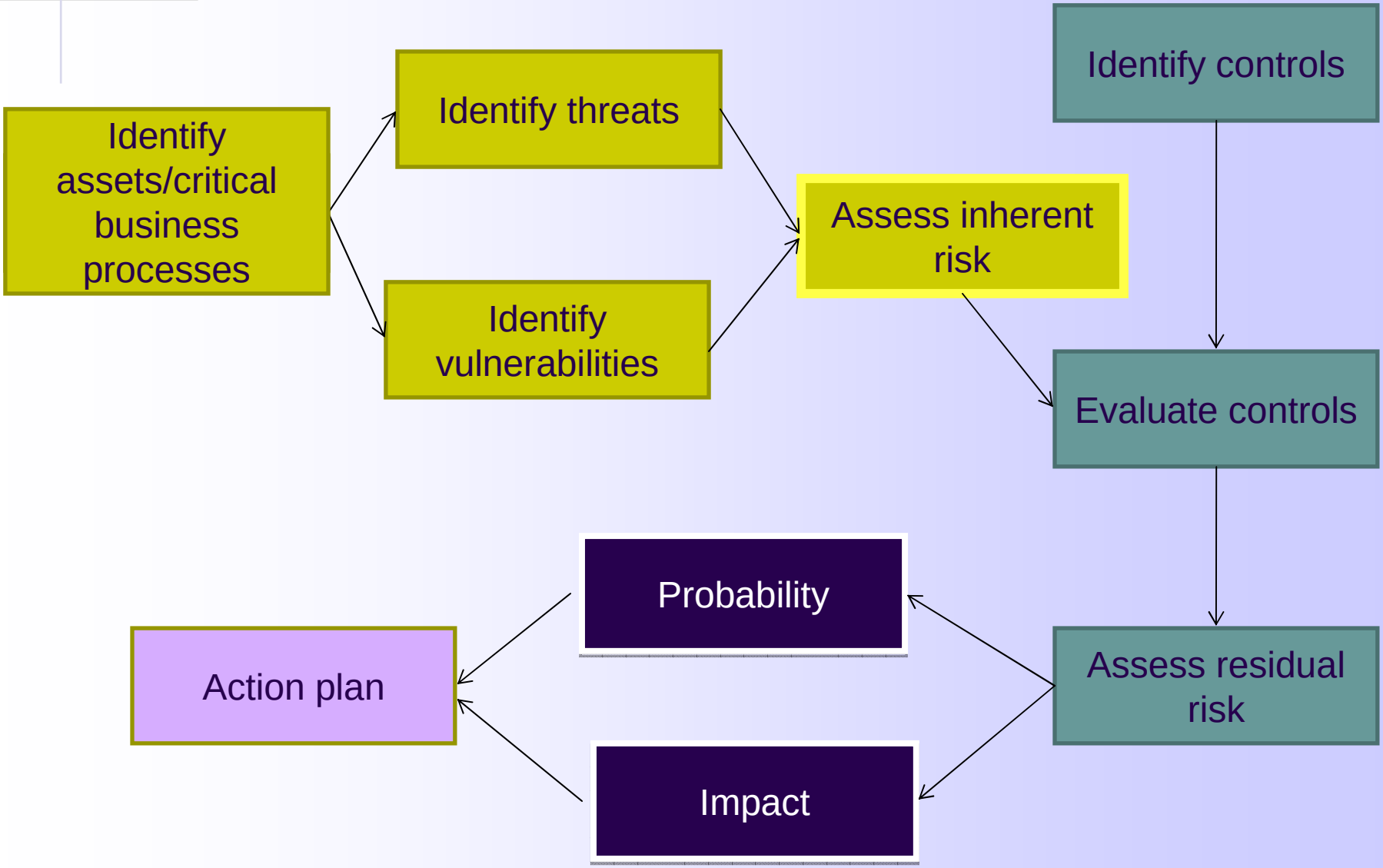
- Natural events such as hurricanes, floods, lighting and other severe weather conditions;
- Technical events such as power outage and fluctuations, communication failure, equipment and software failure;
- Malicious activities including network security attacks, fraud, assaults and public riot; and
- Fires


Identify assets/critical business processes
Identify threats
Identify vulnerabilities
Assess inherent risk
Identify controls
Evaluate controls
Assess residual risk
Probability
Impact
Action plan

Vulnerabilities: Single points of failure

Supervised institutions should review single points of failure:

- **Organizational spread;**
- **Data Center;**
- **Paper files;**
- **Tacit knowledge and specific expertise of personnel;**
- **Hardware equipment;**
- **Power sources;**
- **Tele-communication;**
- **Internet providers or other outsourced services.**

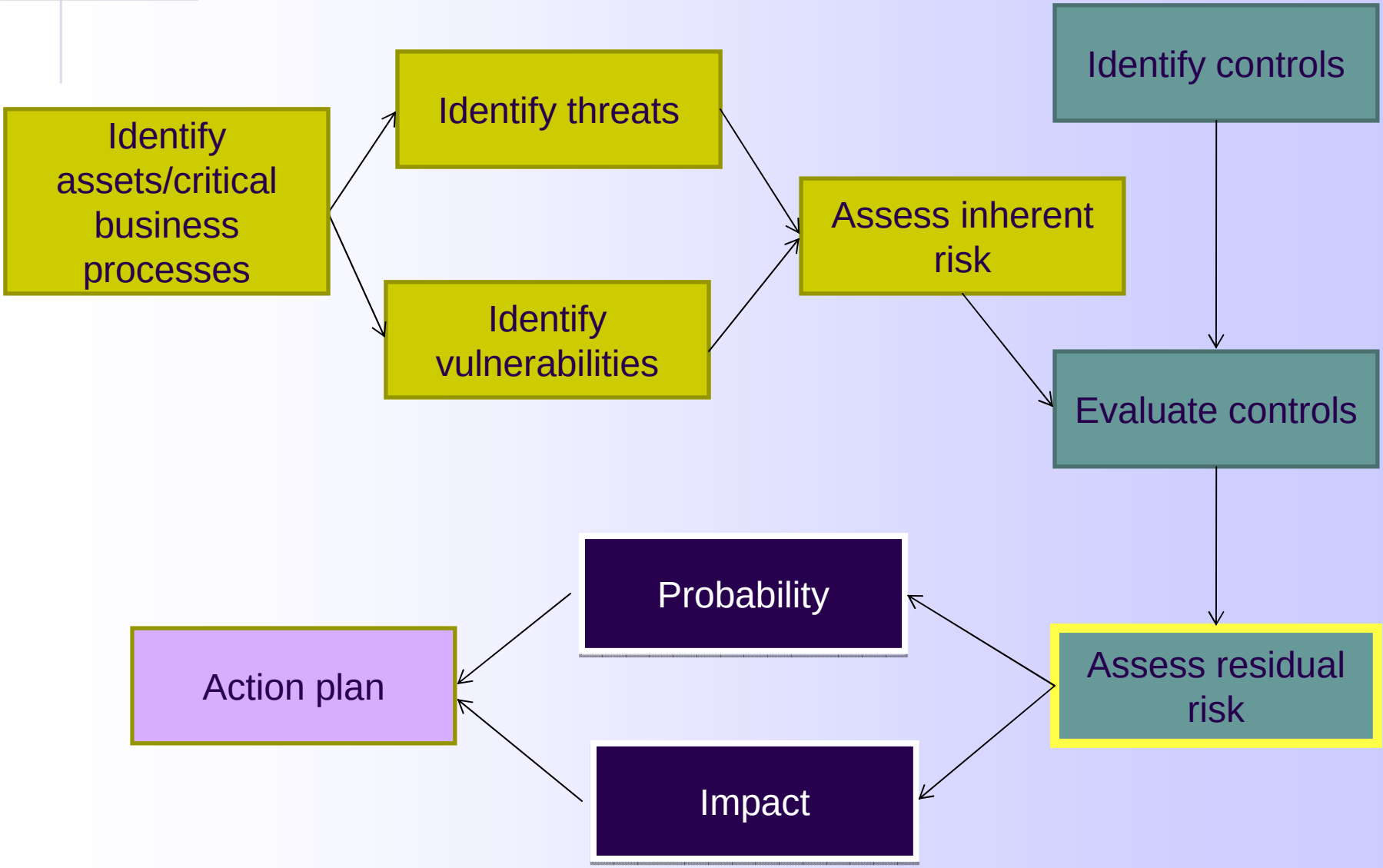

Identify assets/critical business processes
Identify threats
Identify vulnerabilities
Assess inherent risk
Identify controls
Evaluate controls
Assess residual risk
Probability
Impact
Action plan

Asses inherent risk

The process should determine what and how much is at risk by identifying critical business functions and prioritizing them.

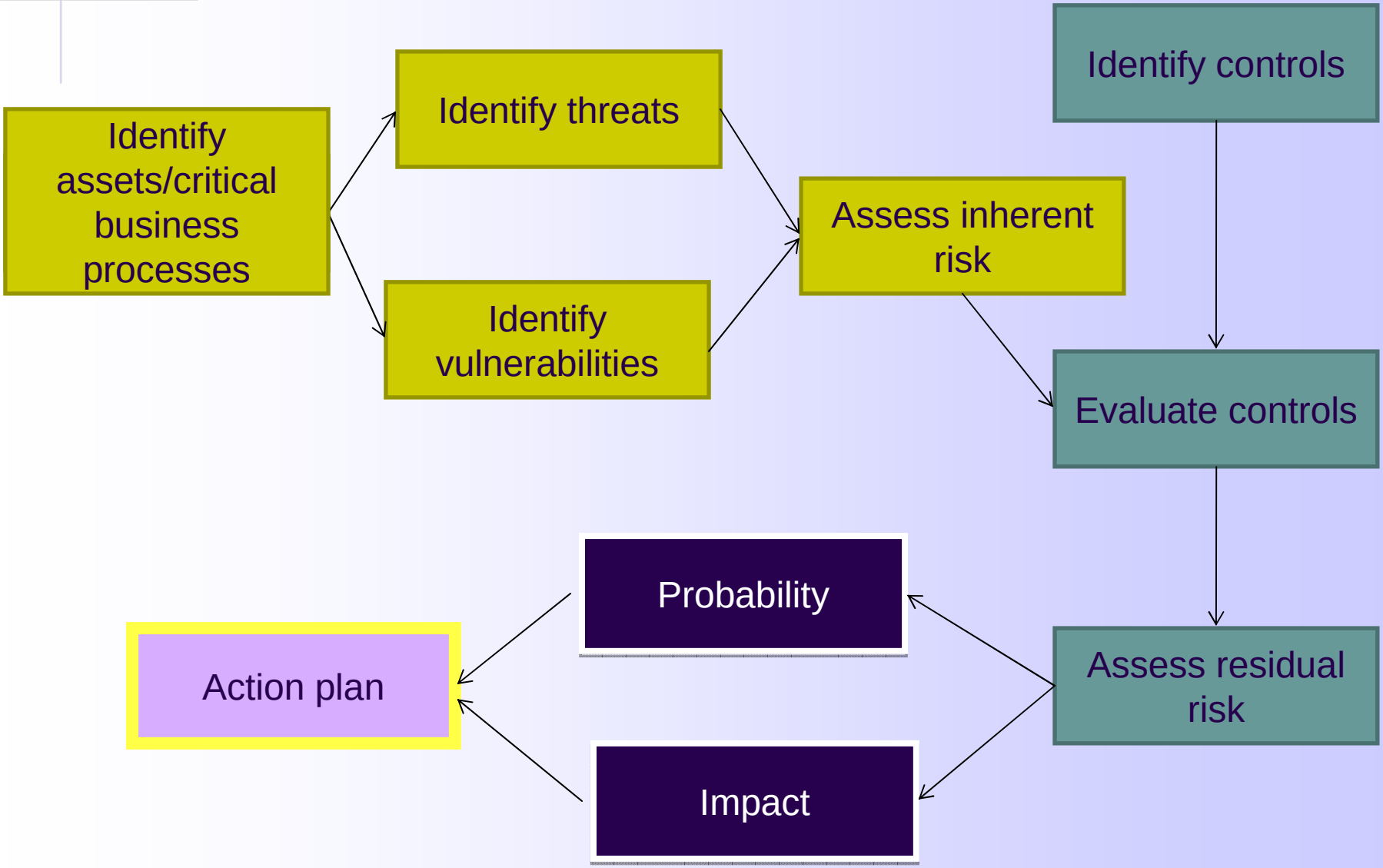
The process should at least identify:

- The maximum allowable unavailability per business function;
- The acceptable quantity of data loss;
- The acceptable recovery time per business function; and
- The acceptable recovery time per business application.


Identify assets/critical business processes
Identify threats
Identify vulnerabilities
Assess inherent risk
Identify controls
Evaluate controls
Assess residual risk
Probability
Impact
Action plan

Assess residual risks

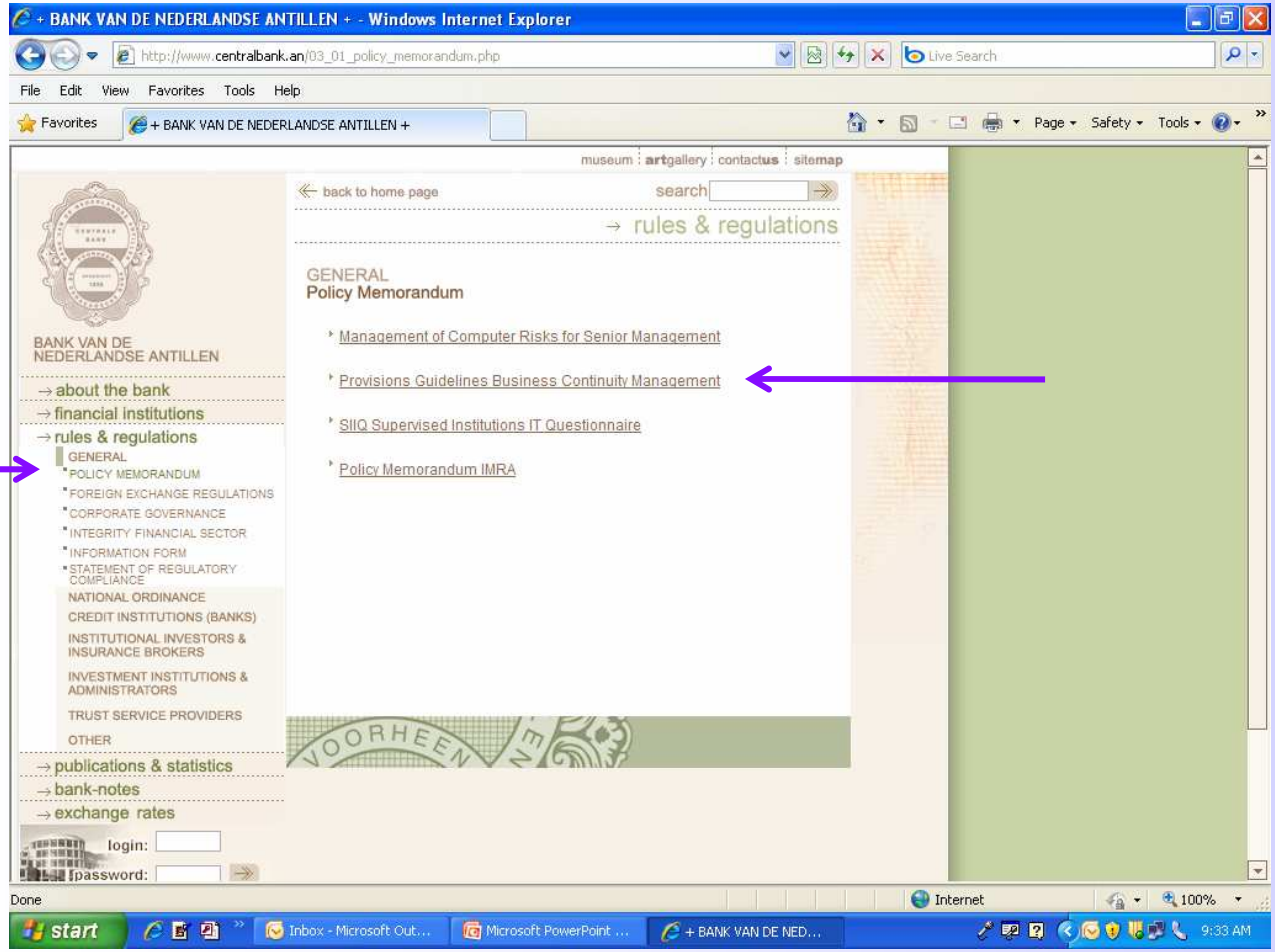
- **Risk Reduction;**
- **Risk Transfer;**
- **Risk Avoidance; or**
- **Risk Acceptance.**


Identify assets/critical business processes
Identify threats
Identify vulnerabilities
Assess inherent risk
Identify controls
Evaluate controls
Assess residual risk
Probability
Impact
Action plan

Action plans

- Principal business continuity plan (umbrella);
- Hurricane plan;
- Building evacuation plan;
- Business Recovery plan;
- Disaster recovery plan for the information technology environment;
- Network security defense and recovery plan; and
- Armed assault plan (only for financial institutions that handle cash).

Provisions and Guidelines for Business Continuity Management



Summary

- Why impose rules for Business Continuity Management?
- Which supervised institutions should comply?
- The principles for Business Continuity Management
- Risk assesment and BIA.

Implementation date

Implement by July 2011

Questions ?