

Implementing the Onerous Risk Management Standard for Accounting Firms – APES 325



Webinar commences at 12:30 Australian Eastern Standard / Daylight Saving time

Risk Management - Why Important?

- Increasing litigation
- Protection of:
 - Assets
 - Finances
 - Operations
 - Legal compliance, governance and due diligence
 - Reputation
 - Credibility
 - Status of firm



It is the foundation of your quality assurance program!

What are we looking at today?

- 1) **Mandatory requirements of Proposed Standard APES 325 *Risk Management for Firms***
- 2) **What is an effective Risk Management Framework?**
- 3) **How to establish, maintain, monitor and document an effective Risk Management Framework for your firm**
- 4) **Checklist of action items**

Background to APES 325

- CPA Australia *RMS 1 Risk Management Statement*
- ICAA *N3 Risk Management Guidelines*
- Issued by APESB
- Mandatory
- Formal **Risk Management Framework** to be in place by 1 April 2012
- No IESBA equivalent standard



My Initial Impressions of Standard

- No basis of conclusion
- Operative date unrealistic
- Public interest obligation not defined in standard or the Code
- Individual risks not defined
- There is no clear nexus with other standards e.g APES 320 (some duplication)
- No linkage to Standards Australia (ISO 31000:2009)



Key Requirements of APES 325

- Objectives of a RMF
- Establishing a RMF
- Monitoring policies and procedures
- Documentation



Objectives of Risk Management Framework

- Overarching Public Interest Obligations by:
 - Facilitating business continuity
 - High quality services offered
 - Protect reputation and credibility of firm
- Need to establish polices to meet objectives
- Embed in strategic and operation practices



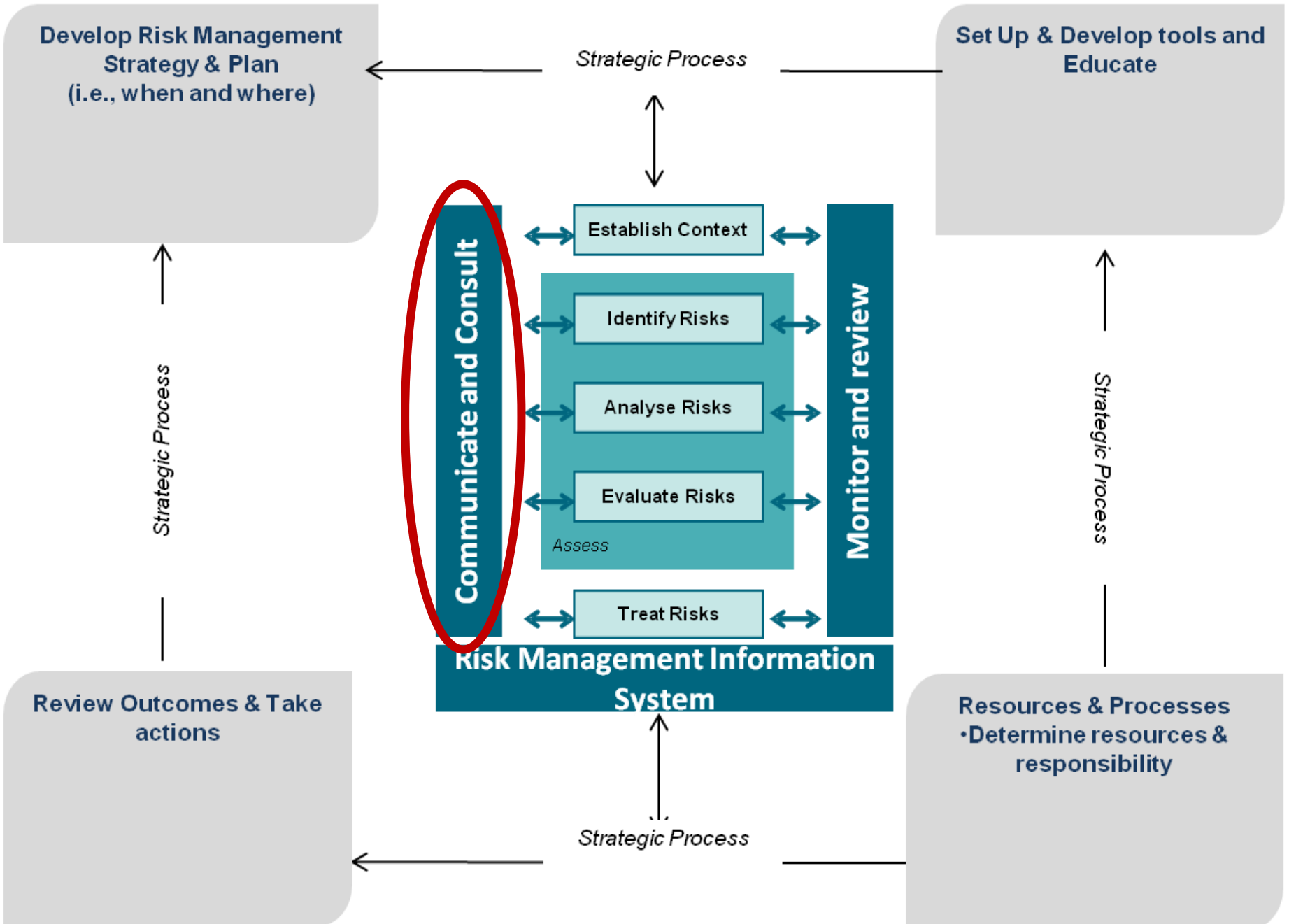
Risk Management Framework: APES 325



Definitions

- **Risk** – Effect of uncertainty on objectives
- **Risk Management** – Coordinated activities to direct and control an organisation with regard to risk
- **Consequence** – Outcome of an event affecting objectives
- **Likelihood** – Chance of something happening
- **Risk Treatment** – Process to modify risk
- **Residual Risk** – Risk remaining after risk treatment

RISK MANAGEMENT: FRAMEWORK & PROCESS (Adapted from ISO 31000:2009)



Communication and Consultation

- During all stages of risk management
- Develop communication and consultation plans early
- Help establish context
- Interests of stakeholders are understood
- Identify expertise in organisation
- Secure endorsement and support for a treatment plan
- Develop an appropriate external and internal communication and consultation plan
- Facilitate truthful, relevant, accurate and understandable exchanges of information



Establish the Context

General

- Articulates objectives
- Defines internal and external parameters
- Sets the scope and risk criteria

External Context

- External environment
- Organisation wide context
- Social and cultural, political, legal, regulatory, financial, technological, economic, natural, whether international, national or regional
- Key drivers and trends on organisation
- Relationships with external stakeholders

Internal Context

- Internal context in which the organisation seeks to achieve its objectives



Risk Criteria

When defining risk criteria, factors to be considered should include:

- The nature and types of causes and consequences that can occur
- How they will be measured
- Likelihood to be defined
- The timeframe of the likelihood and/or consequence
- How the level of risk is to be determined
- The views of the stakeholders
- The level at which risk becomes acceptable or tolerable



Risk Identification

- Identify sources of risk, areas of impact, their causes and potential consequences
- Identify risks associated with not pursuing an opportunity
- Identify risks, whether or not their source is under the organisations control
- All significant causes and consequences should be considered

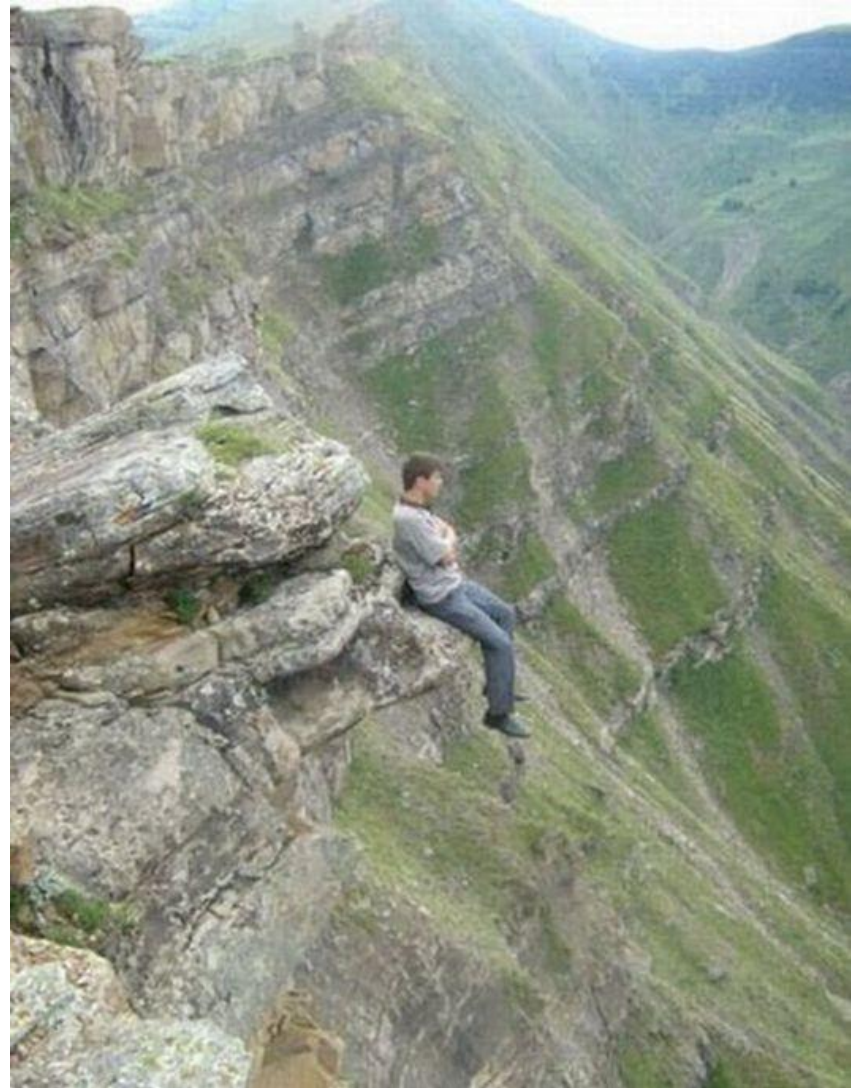


Risk Analysis

- Process to comprehend the nature of risk and to determine the level of risk
- Consider causes and sources of risk; positive and negative consequences and likelihood
- Level of risk means the magnitude of a risk of combination of risk, expressed in terms of the combination of consequences and their likelihood
- Consequence means outcome of an event affecting objectives
- Likelihood means chance of something happening
- Involves developing an understanding of the risk

Risk Evaluation

- Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable
- Decisions on priority for treatment
- Compare to risk criteria
- Consider tolerance for risk
- May lead to further analysis



Risk Treatment

General

- Process to modify risk
- Risk treatment involves a cyclical process of :
 - Assessing a risk treatment
 - Deciding whether residual risk levels are tolerable
 - If not tolerable, generating a new risk treatment, and
 - Assessing the effectiveness of that treatment



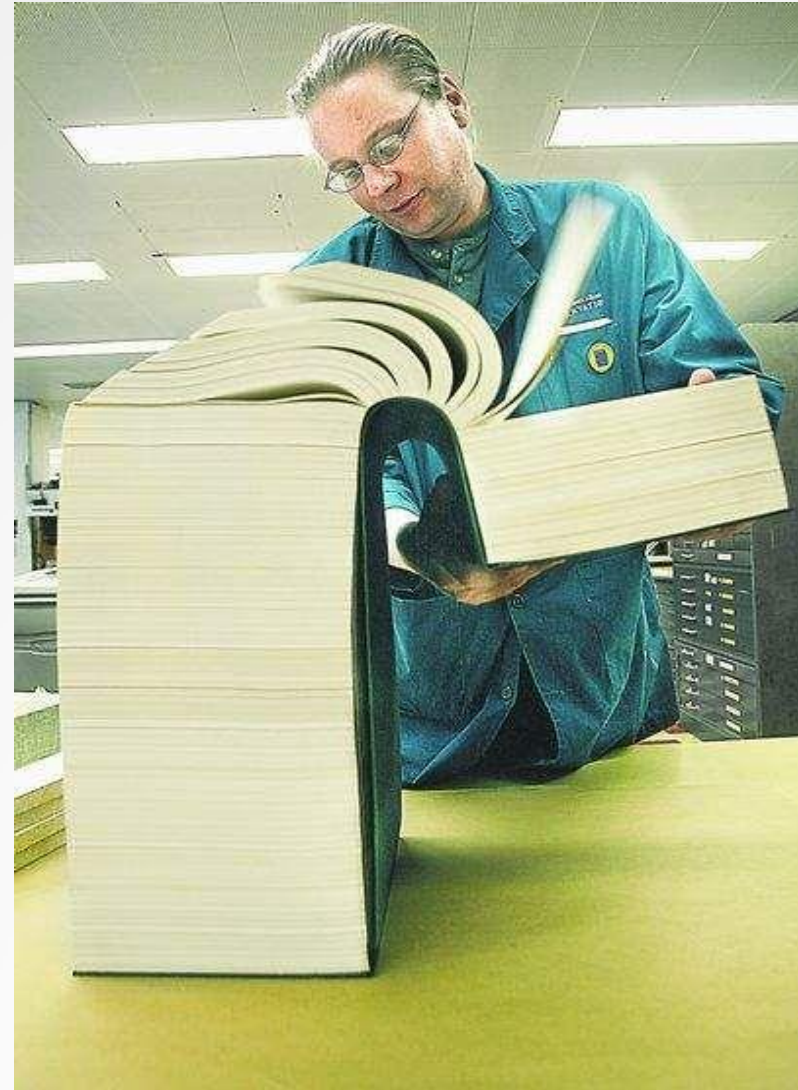
Monitoring

- Establish monitoring processes
- Test compliance
 - Relevant
 - Adequate
 - Operating effectively
- Non-compliance
 - Remedial action
 - Consequences
- Reporting & Communication



Documentation

- Shall document RMF
- Shall document risk management policies and procedures
- Shall communicate to personnel
- Retain relevant documentation to enable effective monitoring
- Training of staff



Action items to get moving!

- Monitor standard-setter
- Decide whether to address early
- Place on partners' agenda
- Assign responsibility
- Schedule risk management training and workshop
- Integrate existing policies
- Update QA and staff manuals
- Train staff on revised policies and procedures

