Risk Assessment as per ISO 27005

Presented by **Dharshan Shanthamurthy,**
Risk Assessment Evangelist
WWW.SMART-RA.COM

What is Risk Assessment?

- NIST SP 800-30

  Risk Assessment is the analysis of threats in conjunction with vulnerabilities and existing controls.

- OCTAVE

  A Risk Assessment will provide information needed to make risk management decisions regarding the degree of security remediation.

- ISO 27005

  Risk Assessment = Identification, Estimation and Evaluation

Why Risk Assessment?

Regulatory Compliance

Compliance Standard	Risk Assessment Requirement
PCI DSS Requirement 12.1.2	Formal and structured risk assessment based on methodologies like ISO 27005, NIST SP 800-30, OCTAVE, etc.
HIPAA Section 164.308(a)(1)	Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.
FISMA 3544	Periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed at least annually.
ISO 27001 Clause 4.1	Risk assessments should identify risks against risk acceptance criteria and organizational objectives. Risk assessments should also be performed periodically to address changes in the security requirements and in the risk situation.
GLBA, SOX, FISMA, Data Protection Act, IT Act Amendment 2008, Privacy Act, HITRUST……	

Why Risk Assessment?

Business Rationale

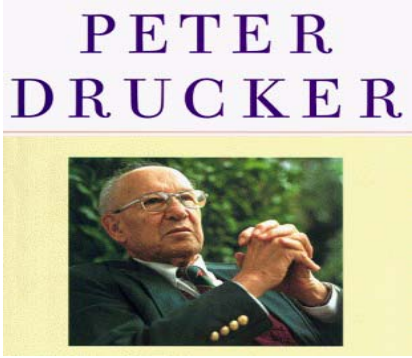
Function	Explanation
Return on Investment	Structured RA Methodology follows a systematic and pre-defined approach, minimizes the scope of human error, and emphasizes process driven, rather than human driven activities.
Budget Allocation	Assists in controls cost planning and justification
Controls	Cost and effort optimization by optimizing controls selection and implementation
Efficient utilization of resources	Resource optimization by appropriate delegation of actions related to controls implementation.

What is IS-RA?

Risk assessment is the cornerstone of any information security program, and it is the fastest way to gain a complete understanding of an **organization's** security profile – its strengths and weaknesses, its vulnerabilities and exposures.

"IF YOU CAN'T MEASURE IT

...YOU CAN'T MANAGE IT!"



Reality Check

- ISRA– a need more than a want
- Each organization has their own ISRA
- ISRA learning curve
- Cumbersome – 1000 assets, 20 worksheets
- Two months efforts
- Complicated report

Exercise

- Threat Scenarios
- Threat Profiles to be filled.

Risk Assessment reference points

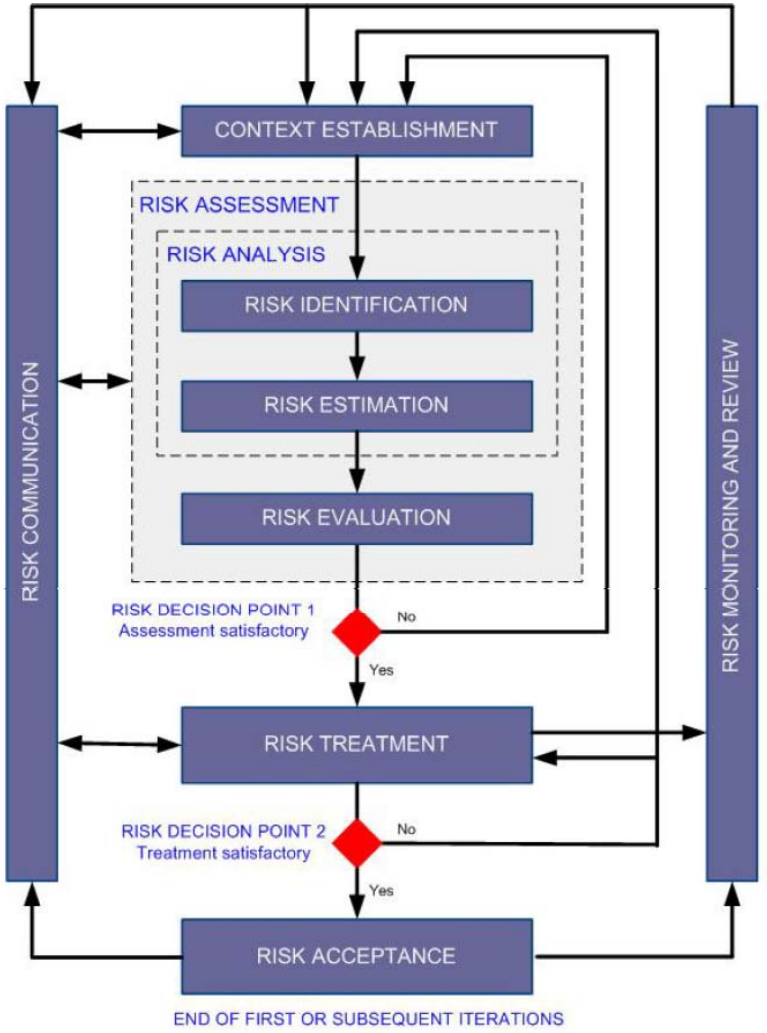
- **OCTAVE**
- **NIST SP 800-30**
- **ISO 27005**
- COSO
- Risk IT
- ISO 31000
- AS/NZS 4360
- FRAP
- FTA
- MEHARI

ISO 27005 Introduction

- ISO 27005 is an Information Security Risk Management guideline.
- Lays emphasis on the ISMS concept of ISO 27001: 2005.
- Drafted and published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)
- Provides a RA guideline and does not recommend any RA methodologies.
- Applicable to organizations of all types.

ISO 27005 Workflow

- Advocates an iterative approach to risk assessment
- Aims at balancing time and effort with controls efficiency in mitigating high risks
- Proposes the Plan-Do-Check-Act cycle.



Source: ISO 27005 Standard

ISO 27005 Risk Assessment

Information Security Risk Assessment = Risk Analysis + Risk Evaluation

Risk Analysis:

Risk Analysis = Risk Identification + Risk Estimation

1. Risk Identification

Risk characterized in terms of organizational conditions

- **Identification of Assets:** Assets within the defined scope
- **Identification of Threats**: Based on Incident Reviewing, Asset Owners, Asset Users, External threats, etc.

ISO 27005 Risk Assessment Contd.

- **Identification of Existing Controls**: Also check if the controls are working correctly.
- **Identification of Vulnerabilities**: Vulnerabilities are shortlisted in organizational processes, IT, personnel, etc.
- **Identification of Consequences:** The impact of loss of CIA of assets.

2. Risk Estimation

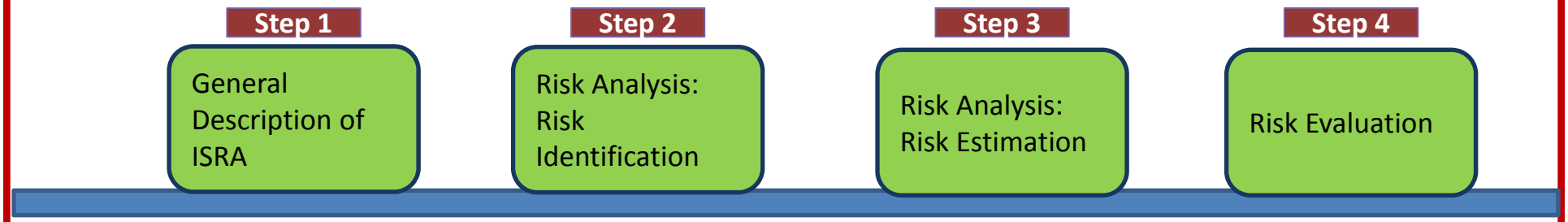
– Specifies the measure of risk.

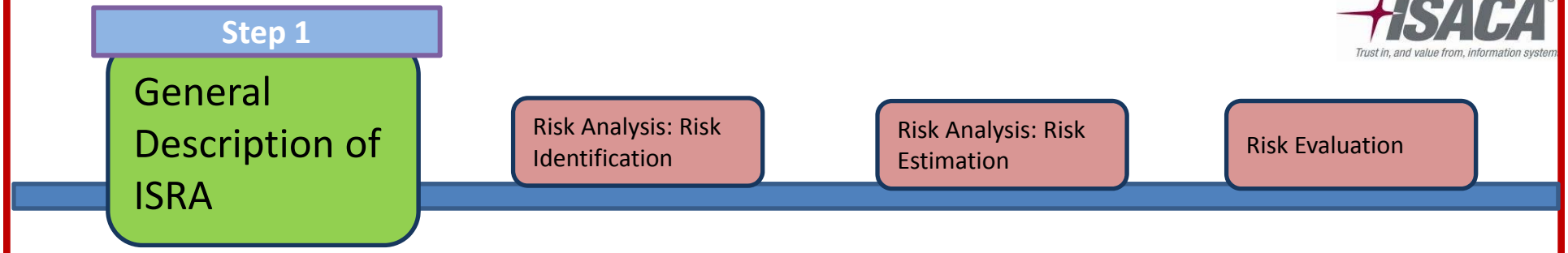
- **Qualitative Estimation**
- **Quantitative Estimation**

Risk Evaluation:

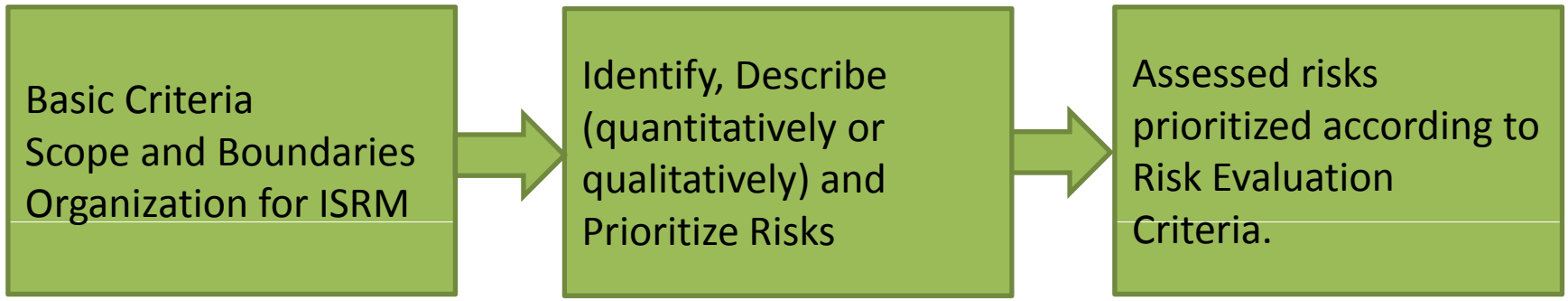
- Compares and prioritizes Risk Level based on Risk Evaluation Criteria and Risk Acceptance Criteria.

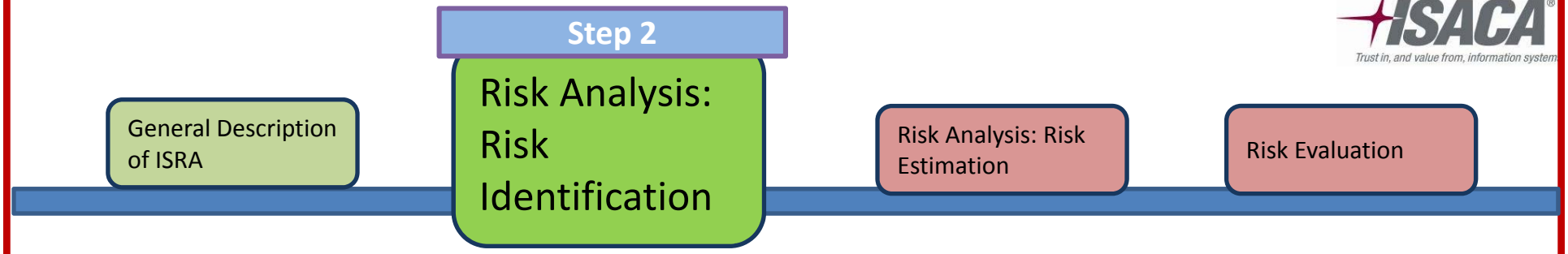
ISO 27005 RA Workflow





1. General Description of ISRA





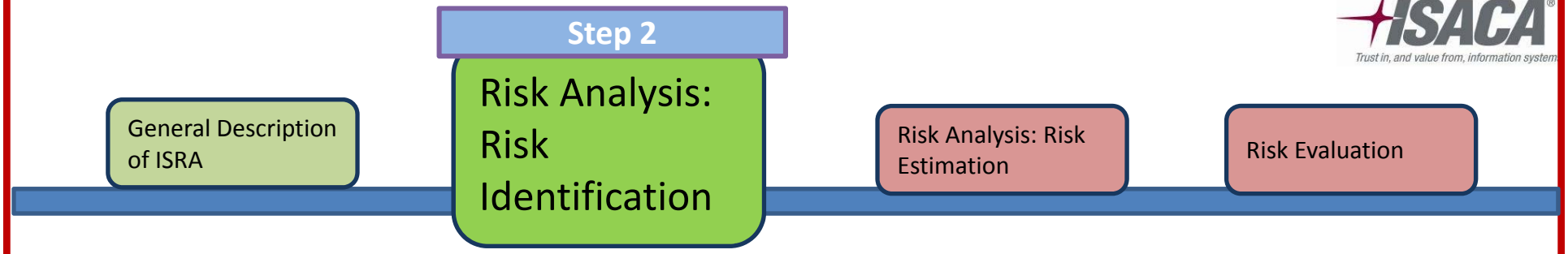
2. Risk Analysis: Risk Identification

Identification of Assets

Scope and Boundaries
Asset owners
Asset Location
Asset function

→ Assets are defined →

List of Assets.
List of associated business processes.



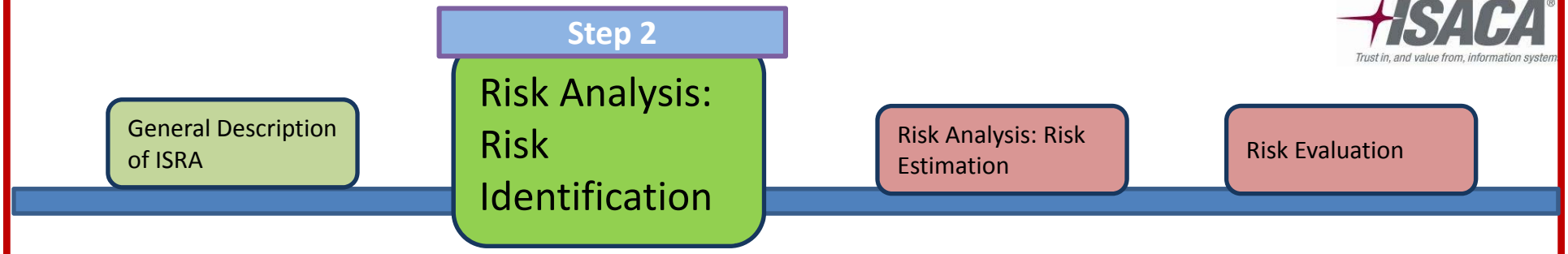
2. Risk Analysis: Risk Identification

Identification of Threats

Threat Information from
- Review of Incidents
- Asset Owners
- Asset Users, etc.

→ Threats are defined →

- Threats
- Threat source
- Threat type



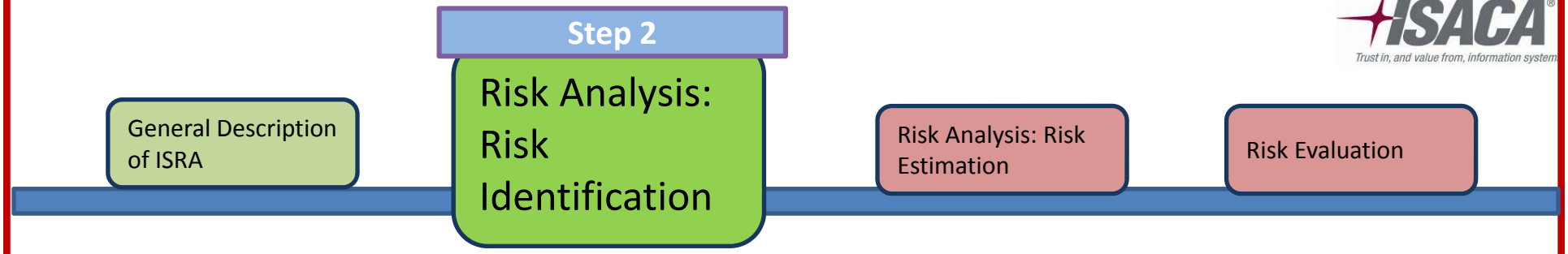
2. Risk Analysis: Risk Identification

Identification of Existing Controls

- Documentation of controls
- RTP

→ Existing and planned controls are defined →

- Existing and planned controls
- Implementation status
- Usage status



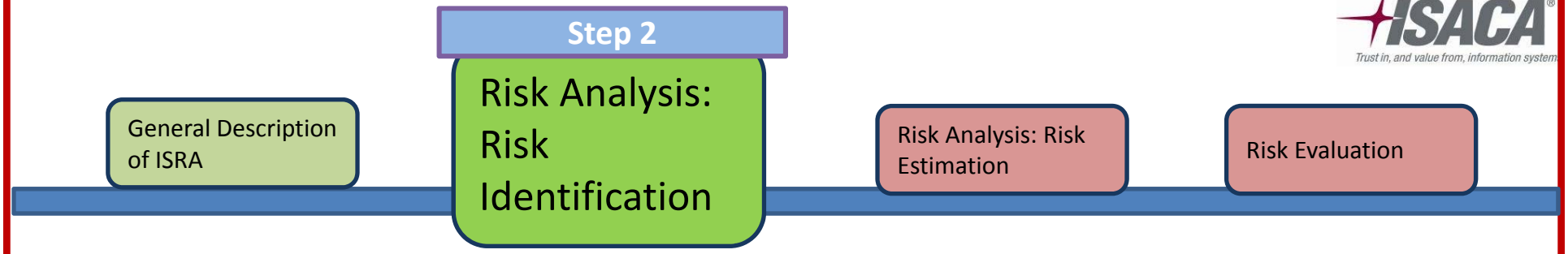
2. Risk Analysis: Risk Identification

Identification of Vulnerabilities

- Identified Assets
- Identified Threats
- Identified Existing Controls

→ Vulnerabilities are identified →

- Vulnerabilities related to assets, threats, controls.
- Vulnerabilities not related to any threat.



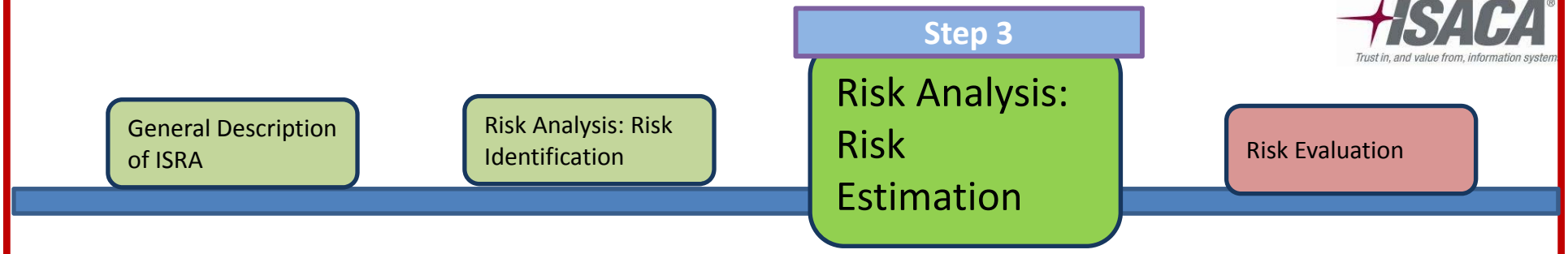
2. Risk Analysis: Risk Identification

Identification of Consequences

- Assets and business processes
- Threats and vulnerabilities

→ The impact of the loss of CIA is identified →

- Incident scenarios with their consequences related to assets and business processes

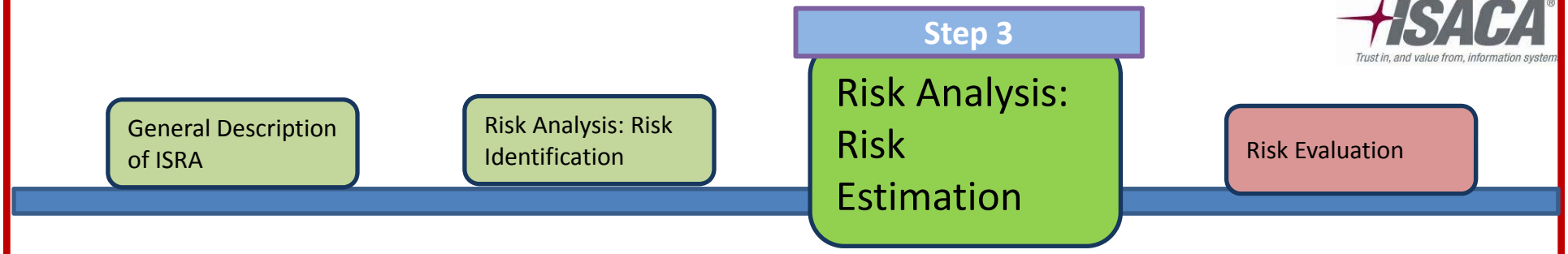


3. Risk Analysis: Risk Estimation

Risk Estimation Methodologies

(a) Qualitative Estimation: High, Medium, Low

(b) Quantitative Estimation: $, hours, etc.

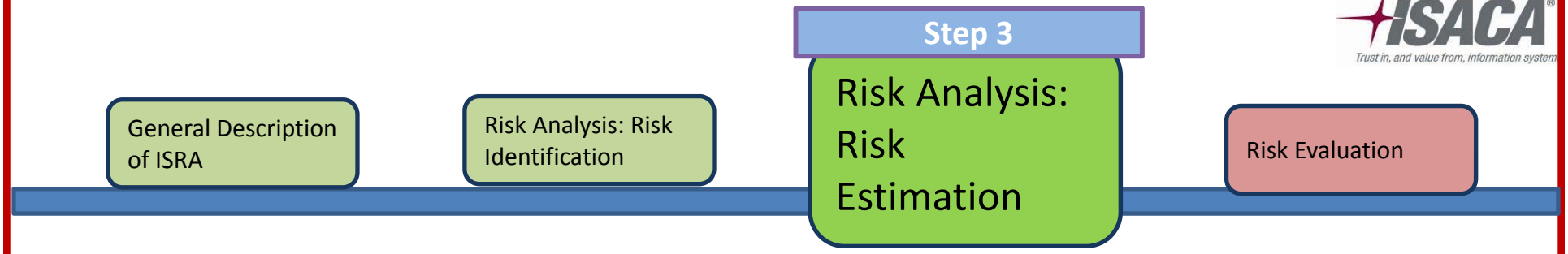


3. Risk Analysis: Risk Estimation

Assessment of consequences

- Assets and business processes
- Threats and vulnerabilities
- Incident scenarios

→ The business impact from information security incidents is assessed. → Assessed consequences of an incident scenario expressed in terms of assets and impact criteria.



3. Risk Analysis: Risk Estimation

Level of Risk Estimation

- Incident scenarios with their consequences
- Their likelihood (quantitative or qualitative).

→ Level of risk is estimated for all relevant incident scenarios

→ List of risks with value levels assigned.

4. Risk Analysis: Risk Estimation

Level of Risk Estimation

- Risks with value levels assigned and risk evaluation criteria.

→ Level of risk is compared against risk evaluation criteria and risk acceptance criteria

→ Risks prioritized according to risk evaluation criteria in relation to the incident scenarios.

Summary

- Keep it Simple and Systematic
- Comprehensive
- Risk sensitive culture in the organization.
- Drive security from a risk management perspective, rather only a compliance perspective.
- Help RA to help you…

Questions?

Be a Risk Assessment Evangelist!

IS-RA Forum on Linkedin

SMART-RA Forum on Linkedin

Dharshan Shanthamurthy,
E-mail: dharshan.shanthamurthy@sisa.in
Phone: +91-99451 22551