LUMIFY work

This is not an ADB material. The views expressed in this document are the views of the author/s and/or their organizations and do not necessarily reflect the views or policies of the Asian Development Bank, or its Board of Governors, or the governments they represent. ADB does not guarantee the accuracy and/or completeness of the material's contents, and accepts no responsibility for any direct or indirect consequence of their use or reliance, whether wholly or partially. Please feel free to contact the authors directly should you have queries.

Vendor Management in ISO27001

An Overview

Vlad de Ramos, CISSP, CISA, CDPO

Chief GRC and Cybersecurity Director

MIDDCO Inc.

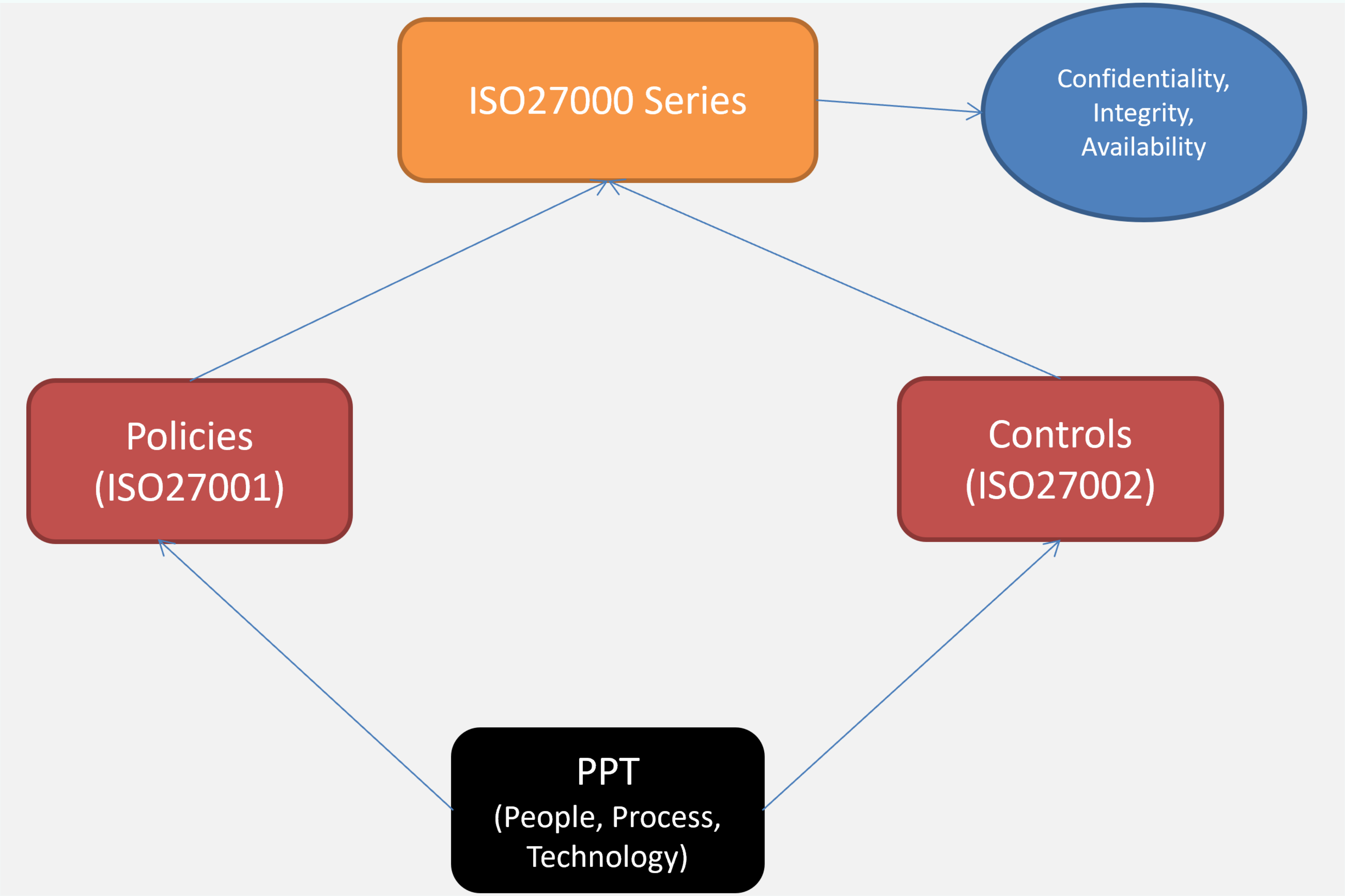
Trainer – Cybersecurity and Standards

Lumify Work Philippines

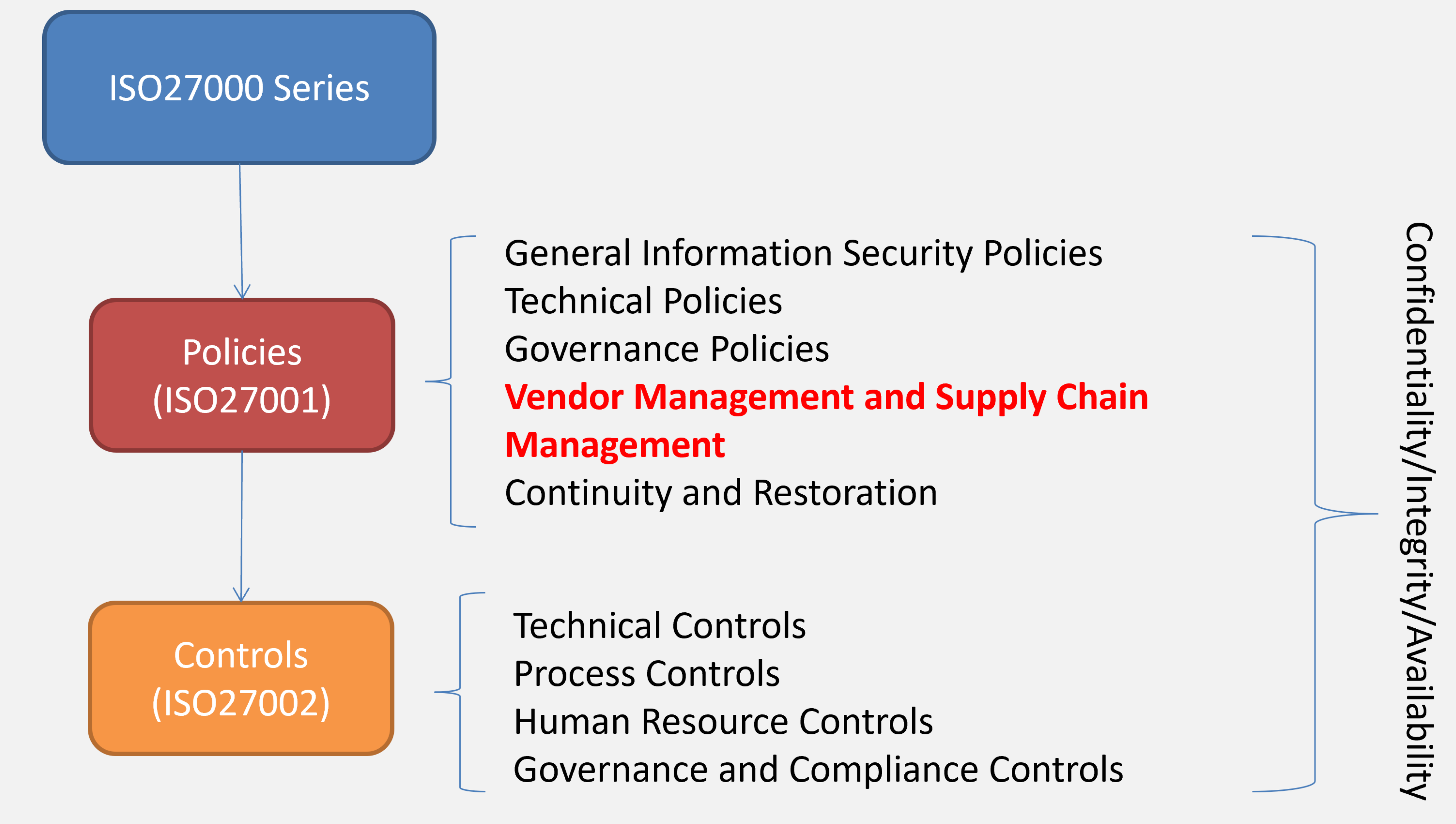
What is ISO27001?

- International standard for information security management systems (ISMS).
- Developed to help organizations protect information/manage risks in a systematic way.
- Defines requirements in which specific ISMS must meet.

ISO27001 Series Structure


ISO27000 Series
Confidentiality, Integrity, Availability
Policies (ISO27001)
Controls (ISO27002)
PPT (People, Process, Technology)

ISO27000 Components



ISO27000 Series

Policies (ISO27001)

- General Information Security Policies
- Technical Policies
- Governance Policies
- **Vendor Management and Supply Chain Management**
- Continuity and Restoration

Controls (ISO27002)

- Technical Controls
- Process Controls
- Human Resource Controls
- Governance and Compliance Controls

Confidentiality/Integrity/Availability

Importance of Vendor Management in Information Security

1. Data-sharing
2. Data ownership
3. Process ownership
4. Reliance
5. Risks
6. Incident Management and response
7. Continuity

Vendor Management in Cybersecurity

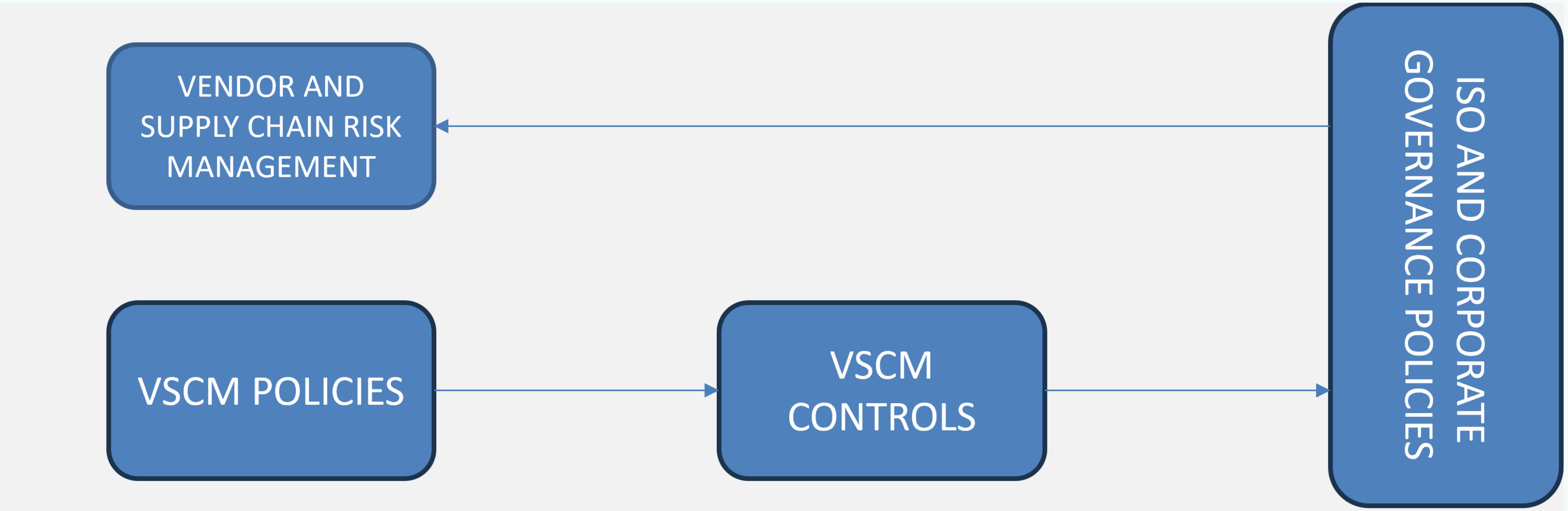
If the suppliers are affected by a cyberattack, YOU are affected.

- Your shared data can be compromised.
- Suppliers' delivery of services to you are affected.
- They may not be there when you need them the most (such as when you are operating in an emergency or in a continuity environment)

Vendor Management in ISO27001

- Recognize, assess and manage risks posed by vendors throughout the procurement and contract cycle.
- Ensure minimal to no effect on your organization in case there are failures or breaches on your suppliers, vendors or partners.

VENDOR AND SUPPLY CHAIN RISK MANAGEMENT



VENDOR AND SUPPLY CHAIN RISK MANAGEMENT

VSCM POLICIES

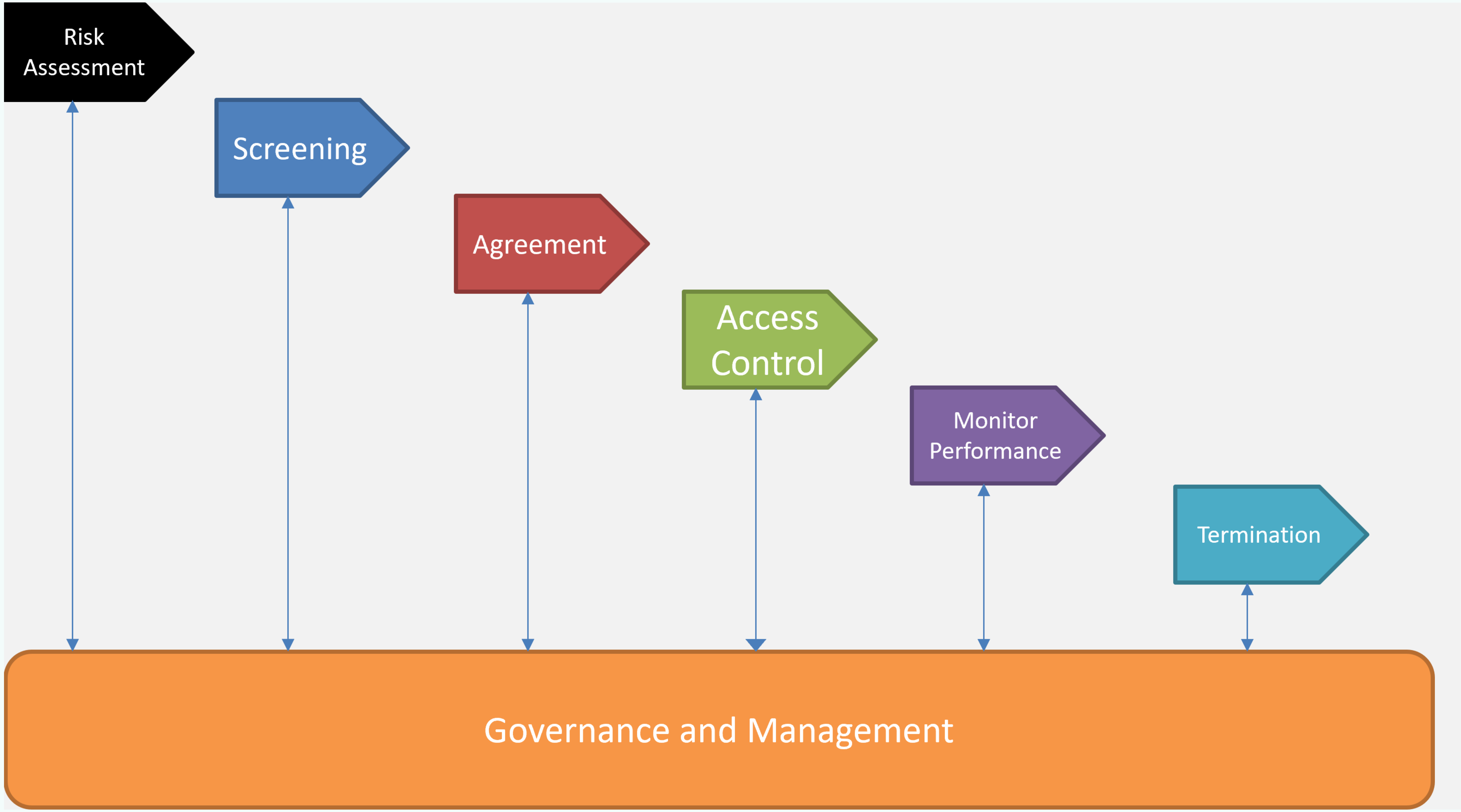
VSCM CONTROLS

ISO AND CORPORATE GOVERNANCE POLICIES

Compliance
Risk Management
Selection
Risk Mitigation
Performance monitoring
Contractual agreements
Vendor Assessment
SLA

Cybersecurity Risk
Security Clauses
Payments
Right to Audit
Performance of Audit
Continuous Improvement
Accountability
Data Ownership

ISO27001 VENDOR MANAGEMENT



ISO27001 VENDOR MANAGEMENT

- Risk Assessment

– Assess C.I.A. of information if you outsource part of your process or allow a third-party to access your information.

– Take necessary actions to mitigate the risk.

ISO27001 VENDOR MANAGEMENT

- Screening

– Background checks.

– The more risks, the more thorough the checks need to be.

– If possible, audit supplier information security controls and processes.

ISO27001 VENDOR MANAGEMENT

- Agreement

– Insert security clauses within your agreement.

– Examples (access control, handling of confidential information, data ownership, deletion requirements, etc.)

ISO27001 VENDOR MANAGEMENT

- Access Control

– Limit access to your data on a “per need” basis.

– Access to data only needed to perform their responsibilities/job.

ISO27001 VENDOR MANAGEMENT

- Monitor Performance

– Compliance of supplier to clauses in the agreement.

– Regular audit of performance to such clauses.

– “Are they performing based on what is in the contract and what is expected of them?”

ISO27001 VENDOR MANAGEMENT

- Termination

– Assets and data is returned.

– No data is left in suppliers premises.

– Audit or accept certification.

– Removal of access rights.

ISO27001 VENDOR MANAGEMENT

- Governance

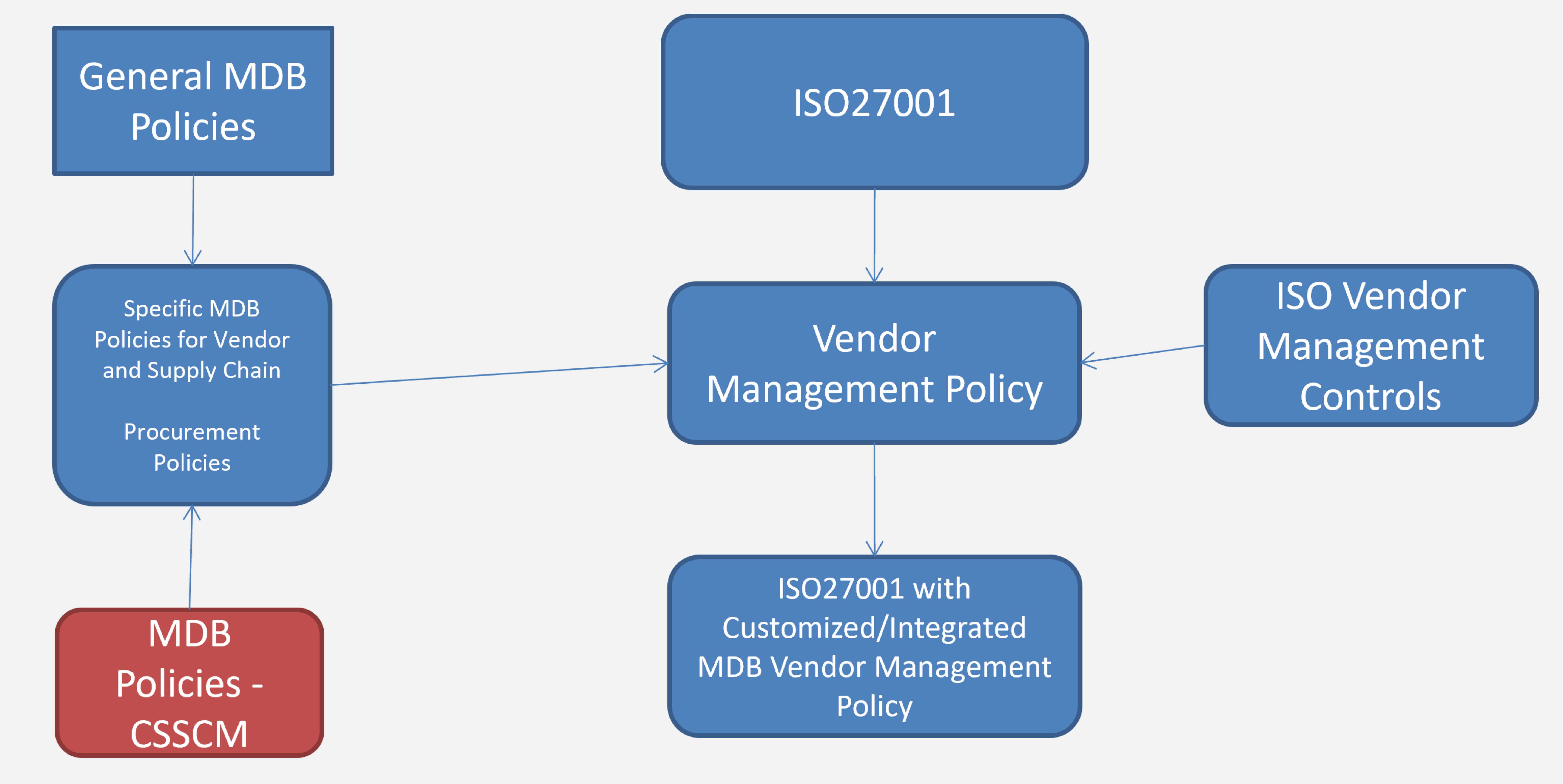
– Policies are present and communicated to suppliers.

– Regular monitoring and reporting for compliance.

– Controls effectiveness.

– Continuous improvement.

ALIGNING MDB POLICIES WITHIN ISO27001 – VENDOR MANAGEMENT



General MDB Policies

ISO27001

Specific MDB Policies for Vendor and Supply Chain

Procurement Policies

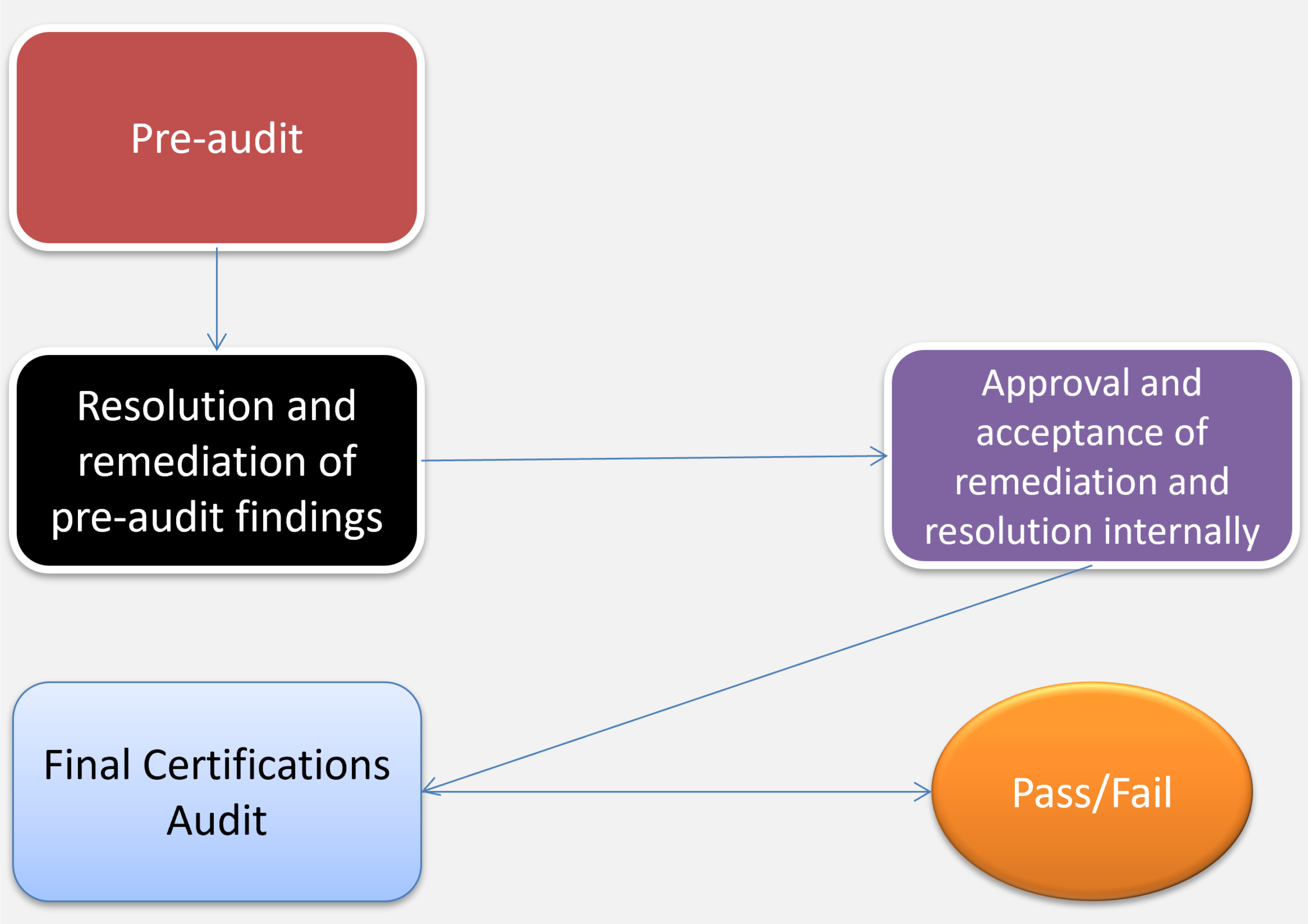
Vendor Management Policy

ISO Vendor Management Controls

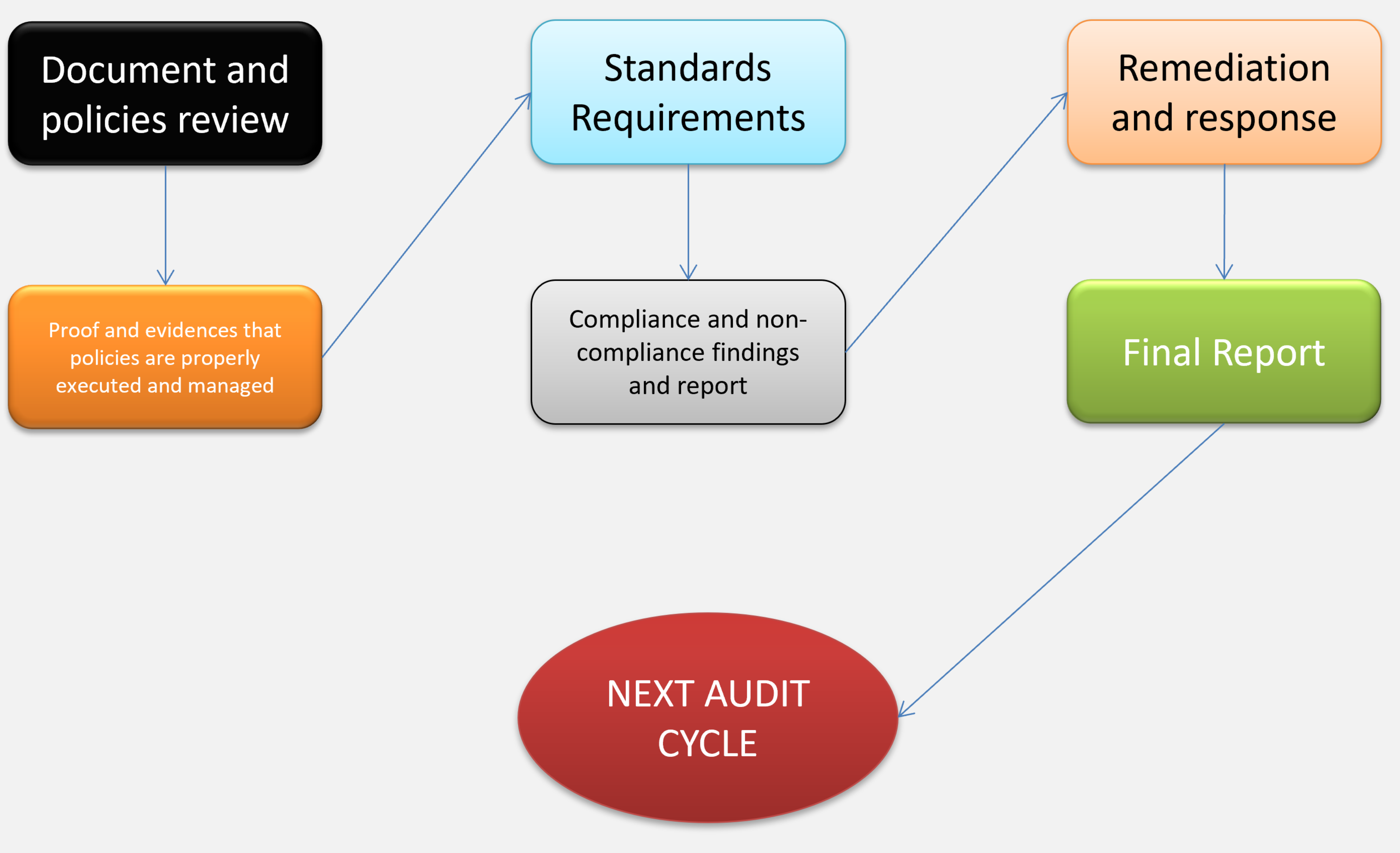
MDB Policies - CSSCM

ISO27001 with Customized/Integrated MDB Vendor Management Policy

STEPS FOR ISO27001 COMPLIANCE


Pre-audit
Resolution and remediation of pre-audit findings
Approval and acceptance of remediation and resolution internally
Final Certifications Audit
Pass/Fail

INTERNAL AUDIT PREPARATION FOR ISO27001



Document and policies review

Proof and evidences that policies are properly executed and managed

Standards Requirements

Compliance and non-compliance findings and report

Remediation and response

Final Report

NEXT AUDIT CYCLE

ISO27001 PRE-AUDIT PREPARATION

1. Set an agenda
2. Conduct an internal audit
3. Confirm scope
4. Update records and documentations
5. Check changes and processes
6. Answer adequately
7. Keep preparing

CONCLUSION

- Suppliers are part of your organization.
- Their security posture will affect your organization.
- It is important under ISO27001 – Vendor Management that you:

➢ know the supplier-related risks

➢ manage the supplier-related risks

➢ mitigate the supplier-related risks