ENTERPRISE CYBER SECURITY

MANAGEMENT

University of Glasgow

MANAGEMENT

- cyber security will be **beyond the core competencies** of many different organisations.

- **economies are increasingly reliant on cyber space** and cyber systems and need to ensure they are dependable and secure.

- **standards and frameworks** provide support for enterprises at different sizes and capabilities to manage cyber security.

STANDARDS

STANDARDS

- typically motivated to support **compatibility** and **interoperability**.
- simply because something is a standard does not mean it is **optimal** or **correct**.
- **documentation** regarding the standard itself, may be private, public or hybrid.
- **geographic** difference between regional, nationals and international.
- can be categorised as **de jure** or **de facto** standards.

FRAMEWORKS

FRAMEWORKS

- **methodology** for discussing, debating and considering cyber security within an enterprise.

- frameworks adopt different approaches with **different** focus and priority.

- **similarities** are stronger than the differences when it comes to these frameworks.

- there are many aspects and elements the frameworks **share**.

FRAMEWORKS

- numerous **families** of objectives or areas of interest and/or function.

- typically rely on **risk management** in terms of understanding context, assets, threats and processes.

- evangelise **controls** as an approach to improve cyber security, but these can take many different forms.

- **review** of controls and countermeasures to continually improve the cyber security process.

FIPS200 FAMILIES

AC	ACCESS CONTROL	**CP**	CONTINGENCY PLANNING
AT	AWARENESS AND TRAINING	**IA**	IDENTIFICATION AND AUTHENTICATION
AU	AUDIT AND ACCOUNTABILITY	**SA**	SYSTEMS AND SERVICES ACQUISITION
PL	PLANNING	**MA**	MAINTENANCE
CM	CONFIGURATION MANAGEMENT	**RA**	RISK ASSESSMENT

FRAMEWORKS

- National Institute of Standards and Technology (NIST)
- $(ISC)^2$ common body of knowledge (CBK)
- Centre for Internet Security Critical Security Controls (CSC)
- Common Criteria
- International Organisation for Standardisation (ISO) 27001/27002

NIST

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

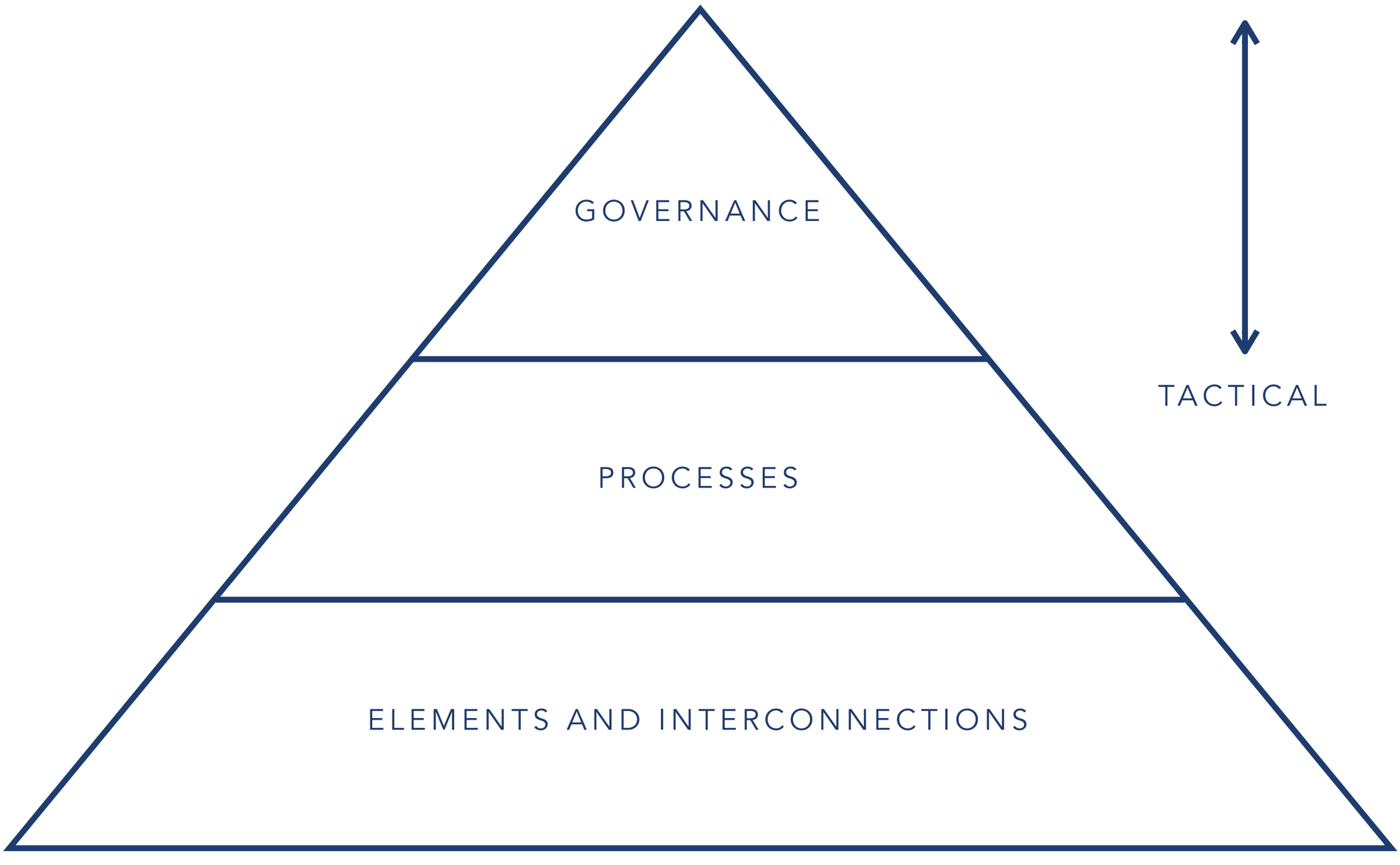
- **non-regulatory** US organisation that is tasked with advancing capability of industry.

- refining and **advocating** best practice, standards and measurement.

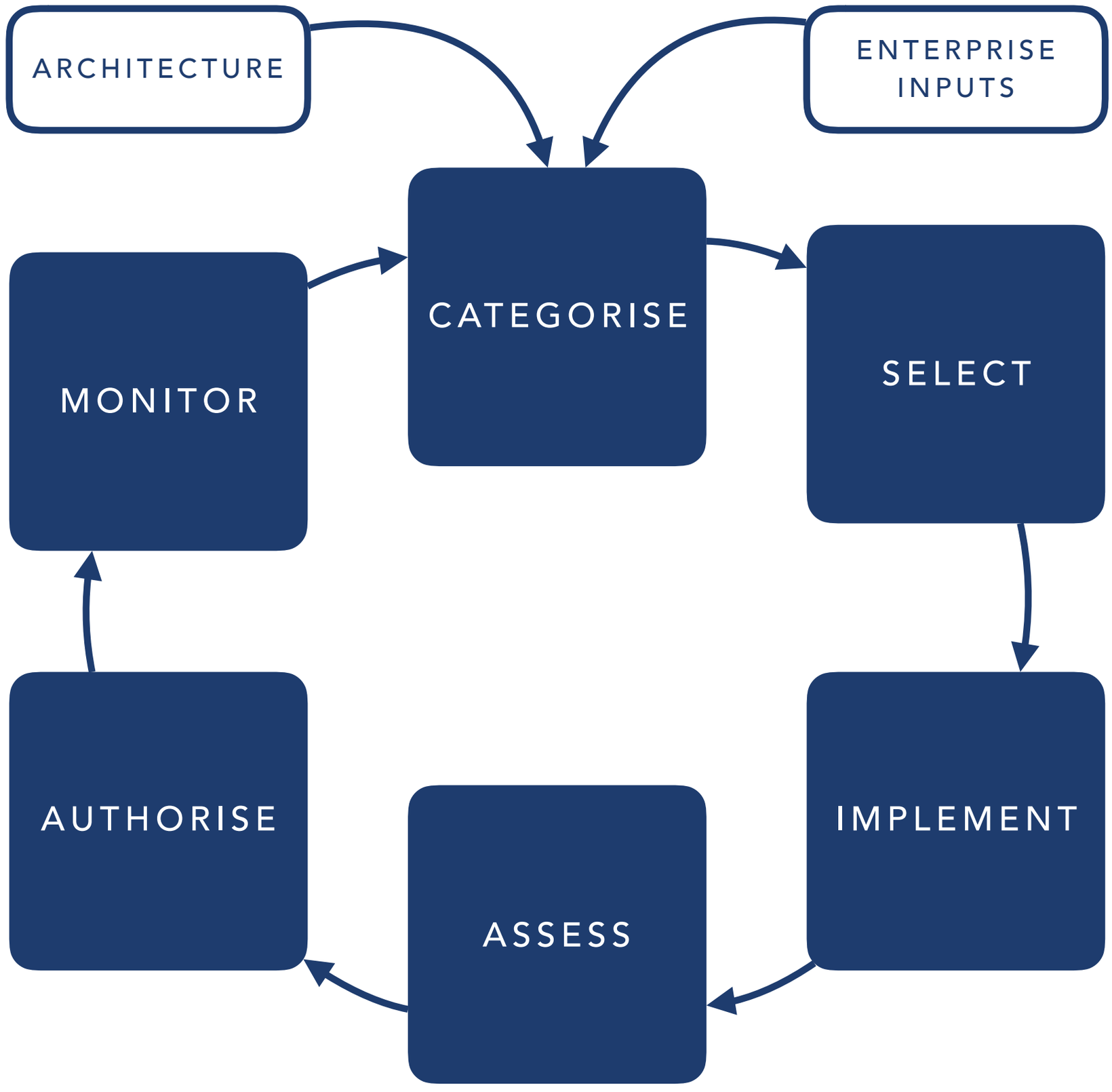
- formally referred to as the **National Standards Bureau** (NSB).

- provides non-mandatory guidance to federal organisations on systems in the form of **special publications** (SP).

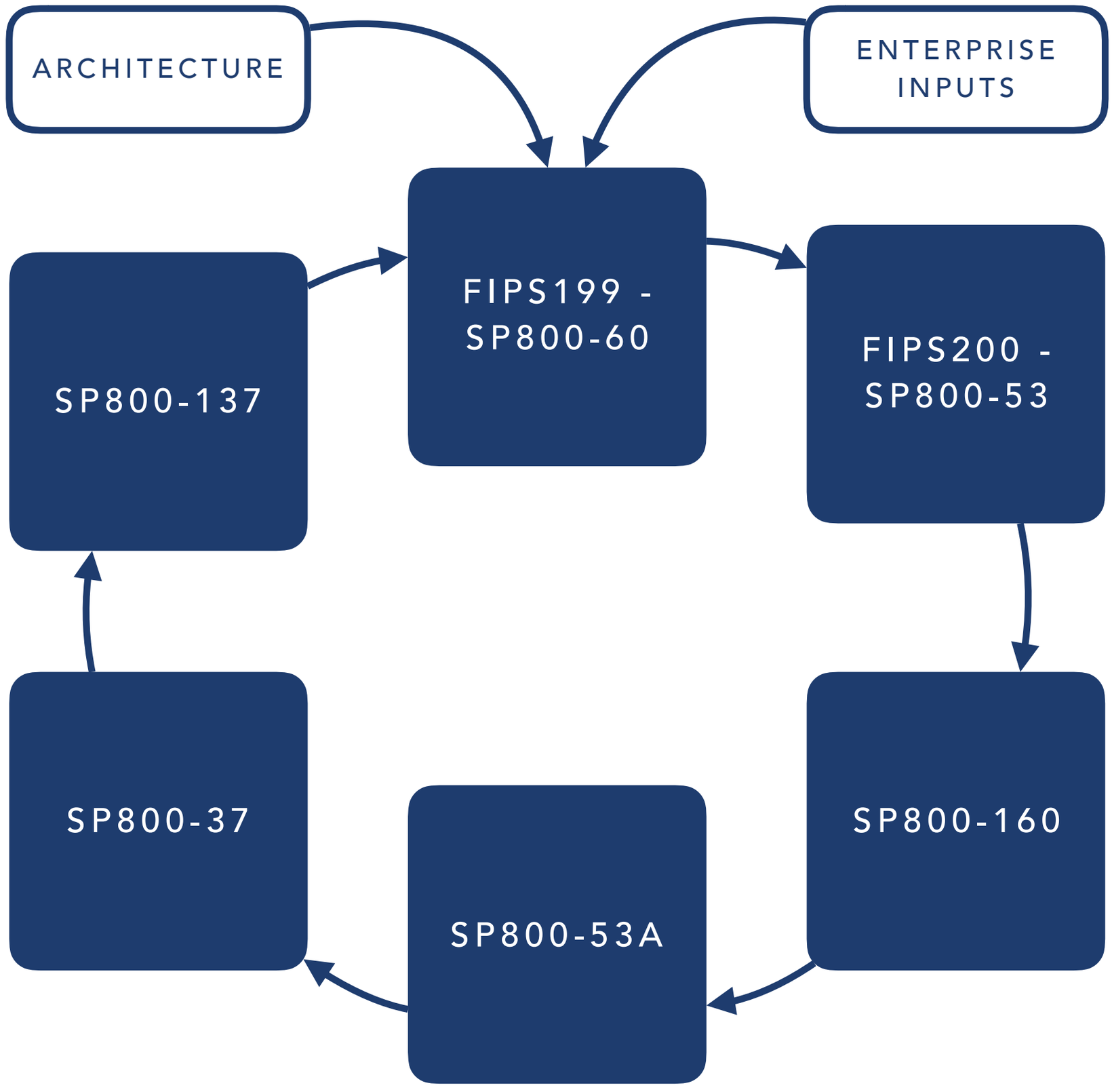
NIST RISK MANAGEMENT



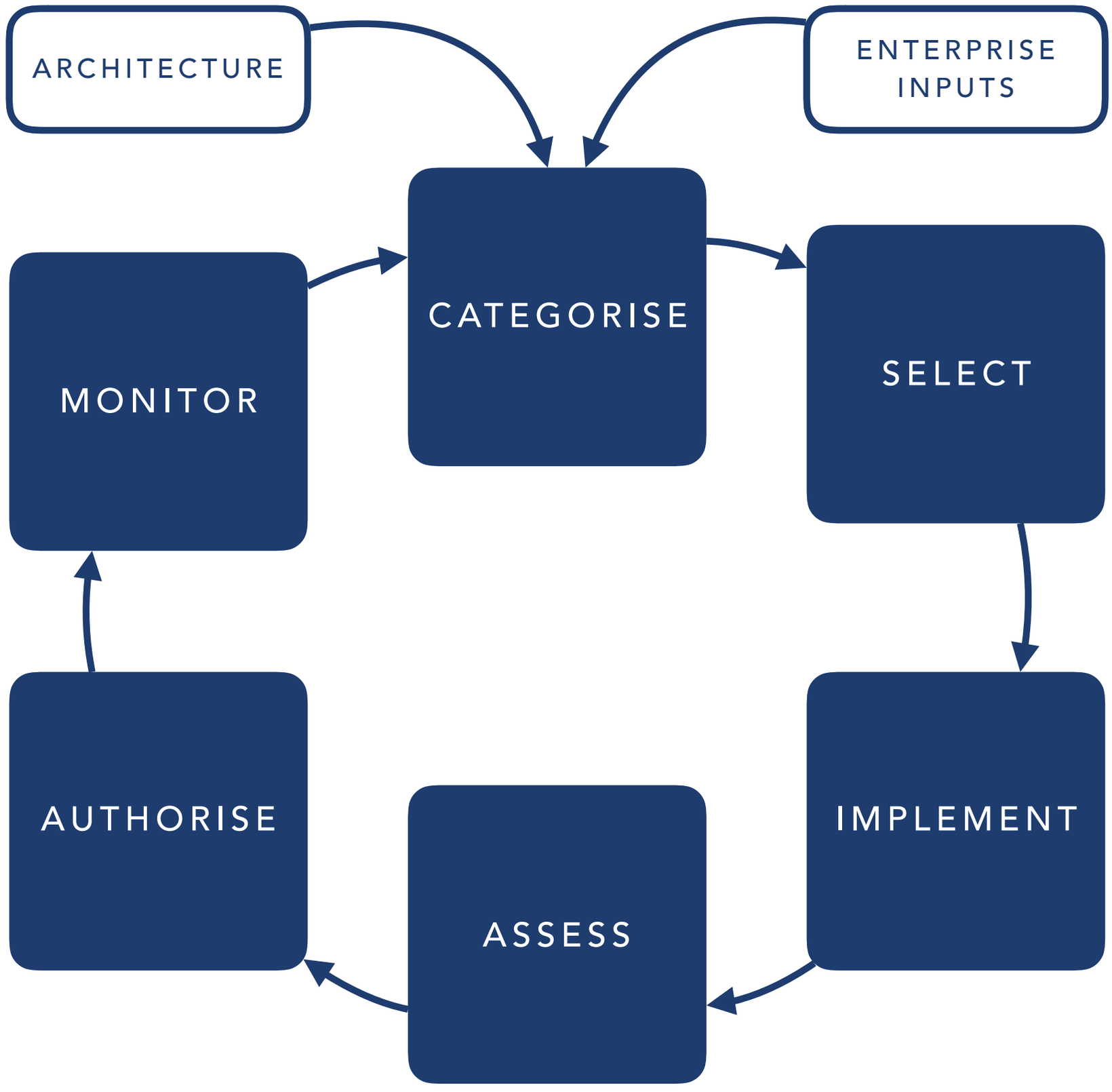
NIST RISK MANAGEMENT FRAMEWORK



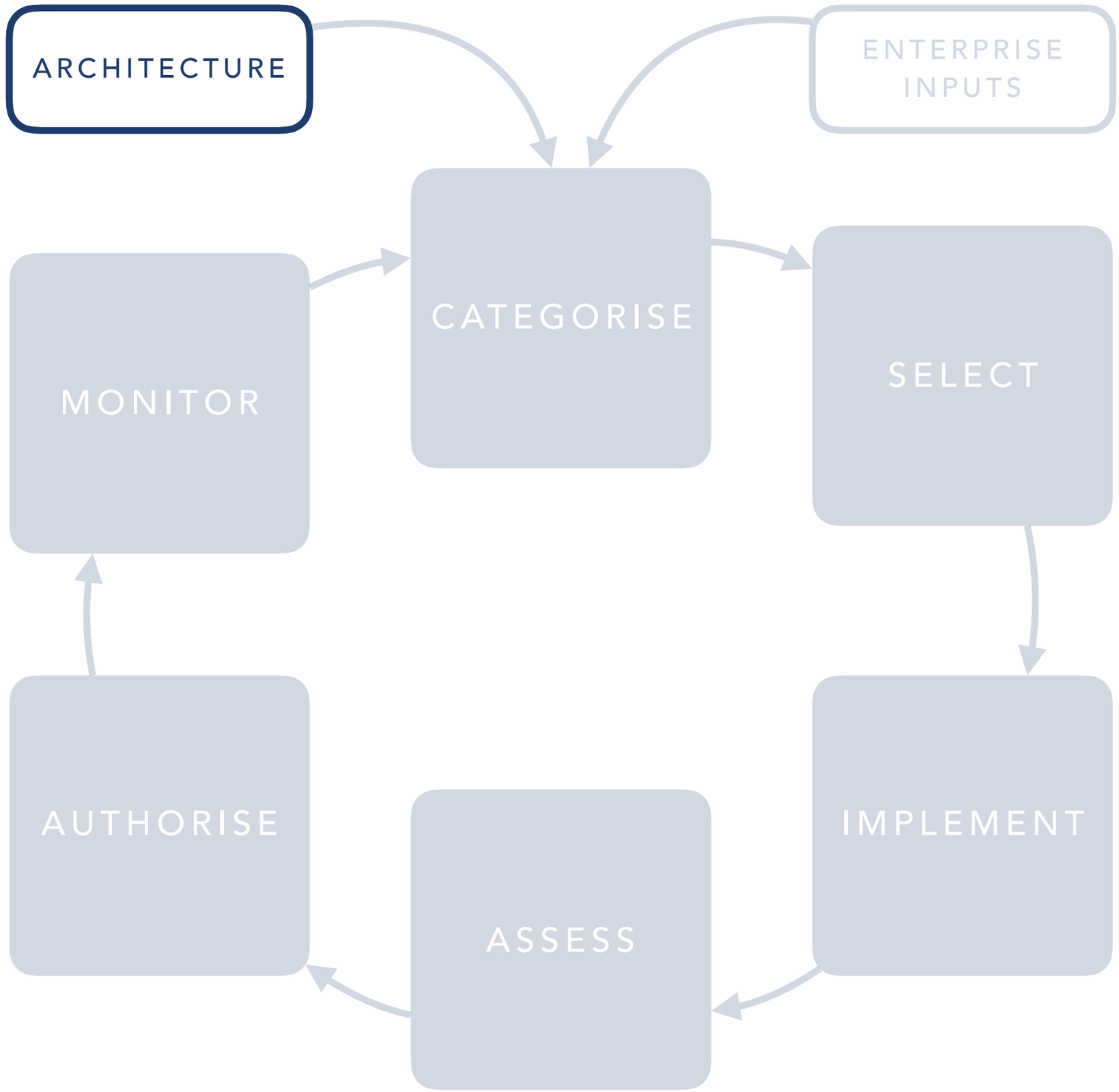
NIST RISK MANAGEMENT FRAMEWORK



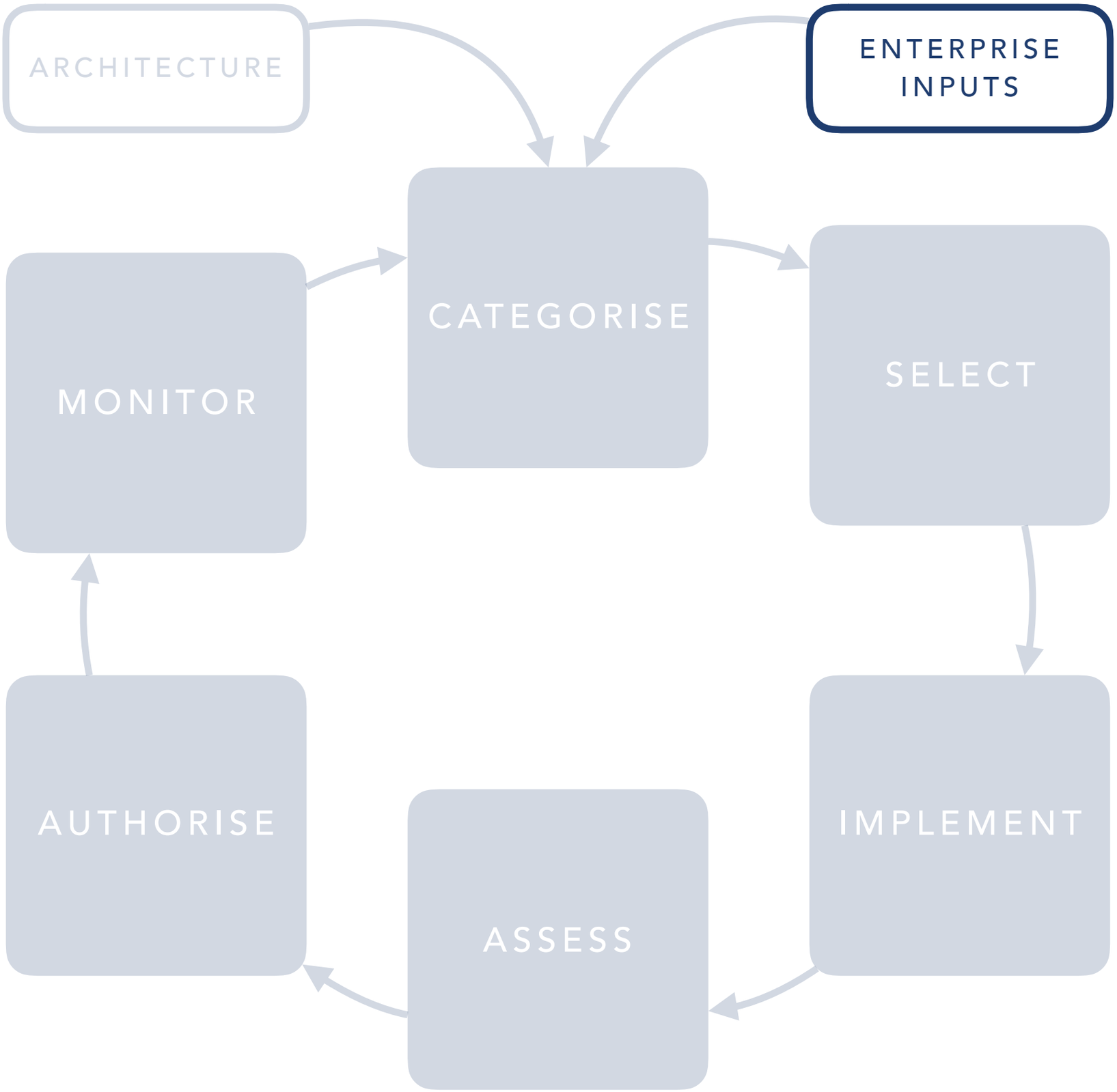
NIST RISK MANAGEMENT FRAMEWORK



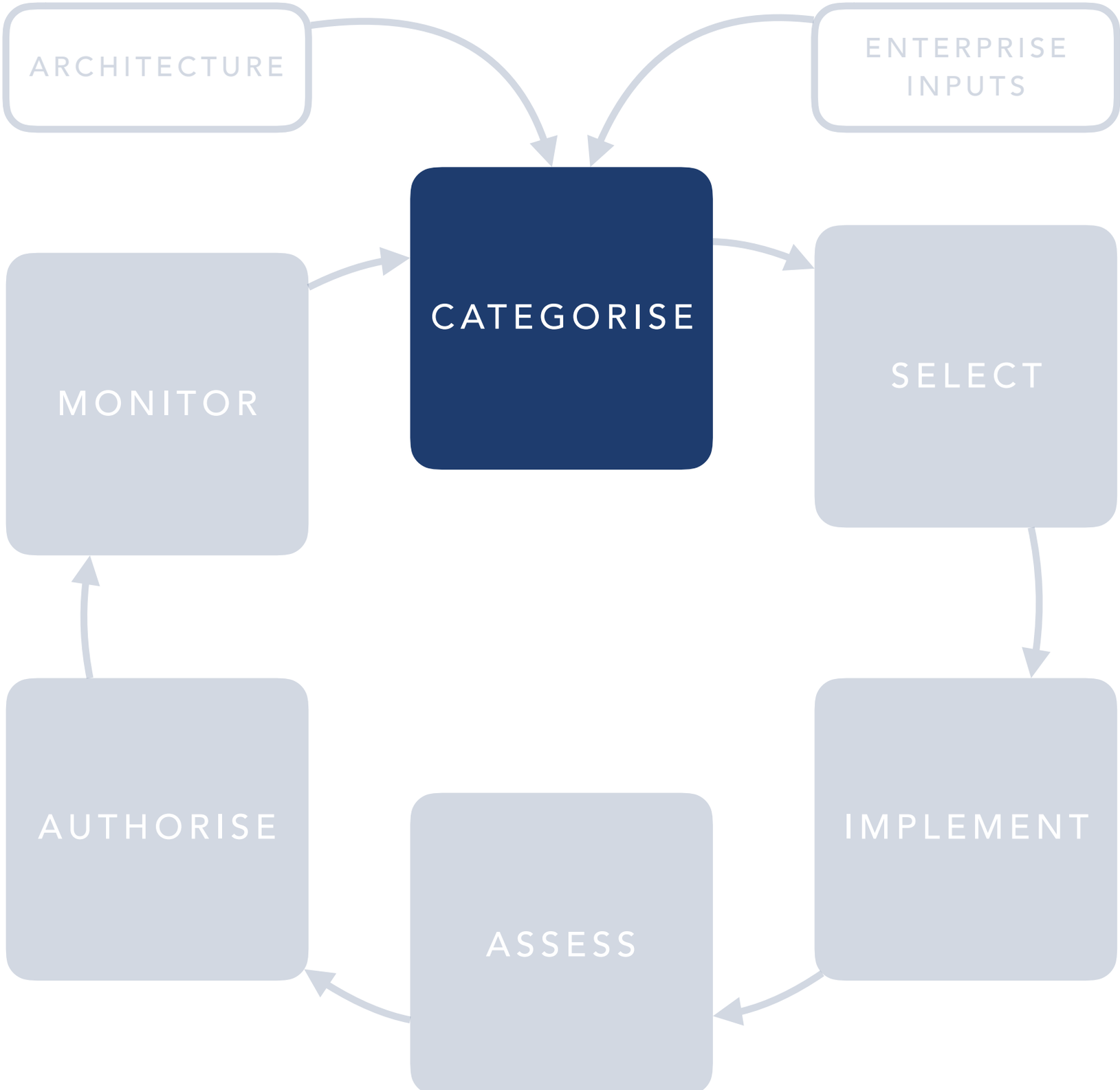
NIST RISK MANAGEMENT FRAMEWORK



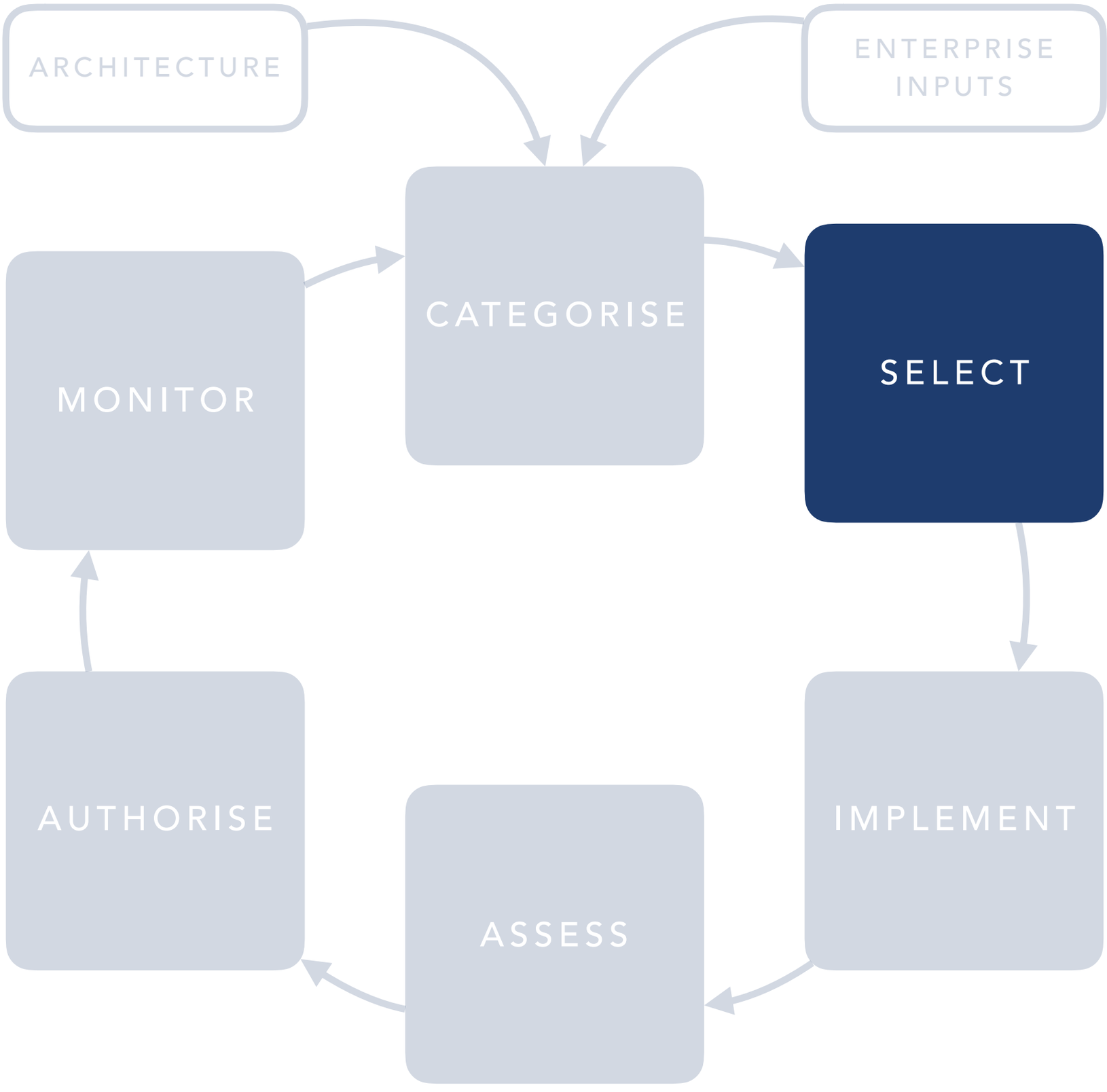
NIST RISK MANAGEMENT FRAMEWORK



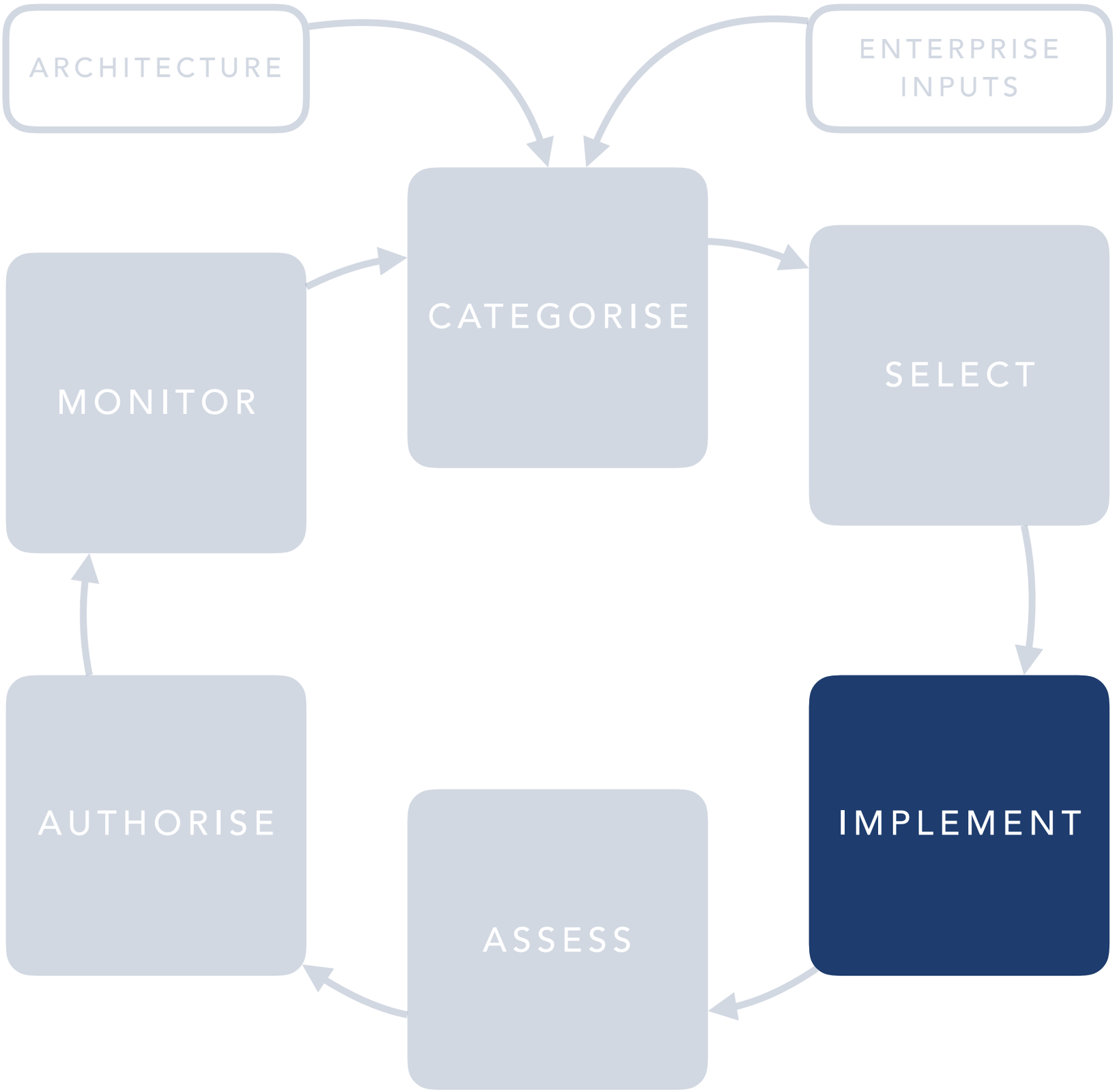
NIST RISK MANAGEMENT FRAMEWORK



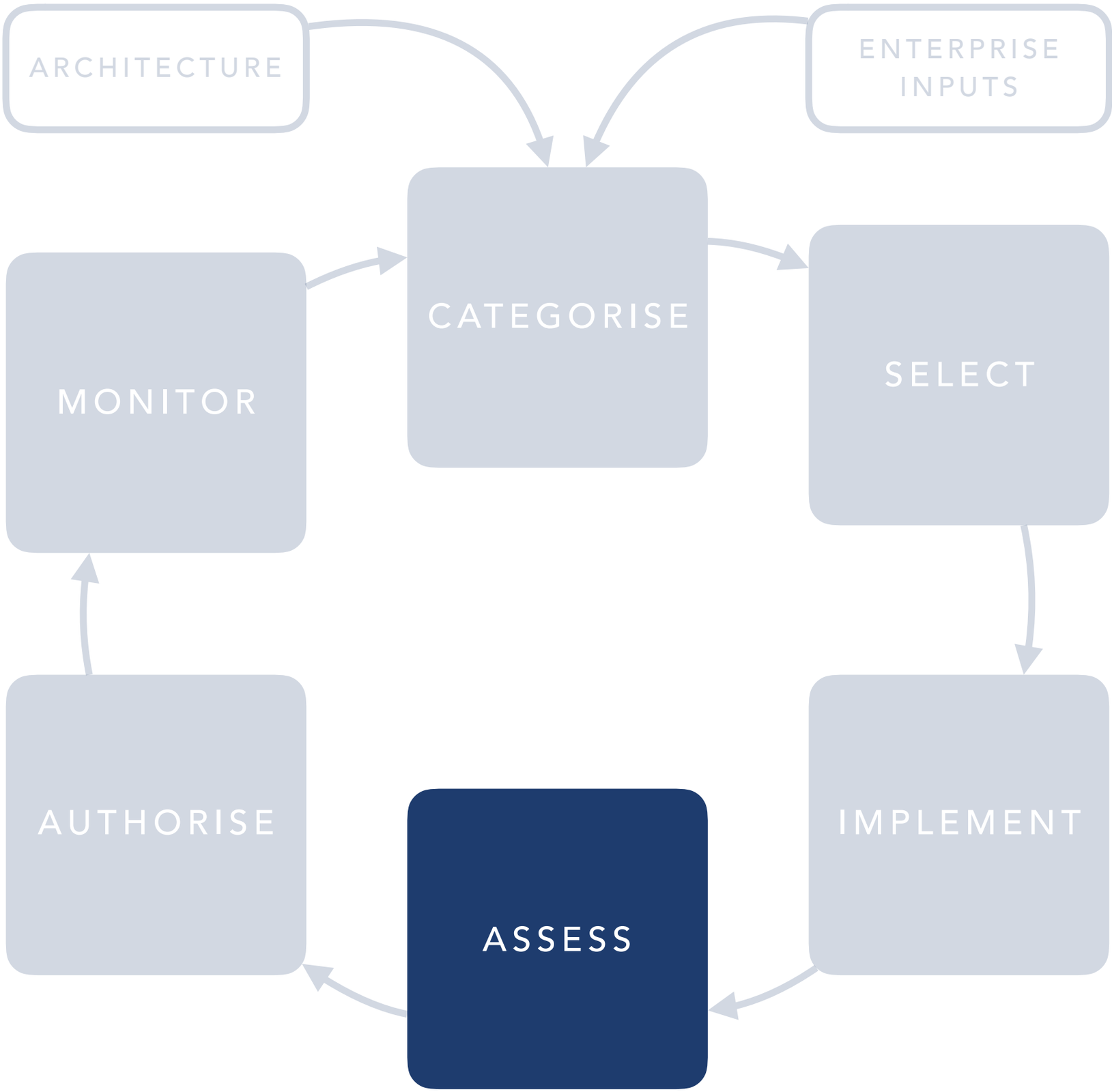
NIST RISK MANAGEMENT FRAMEWORK



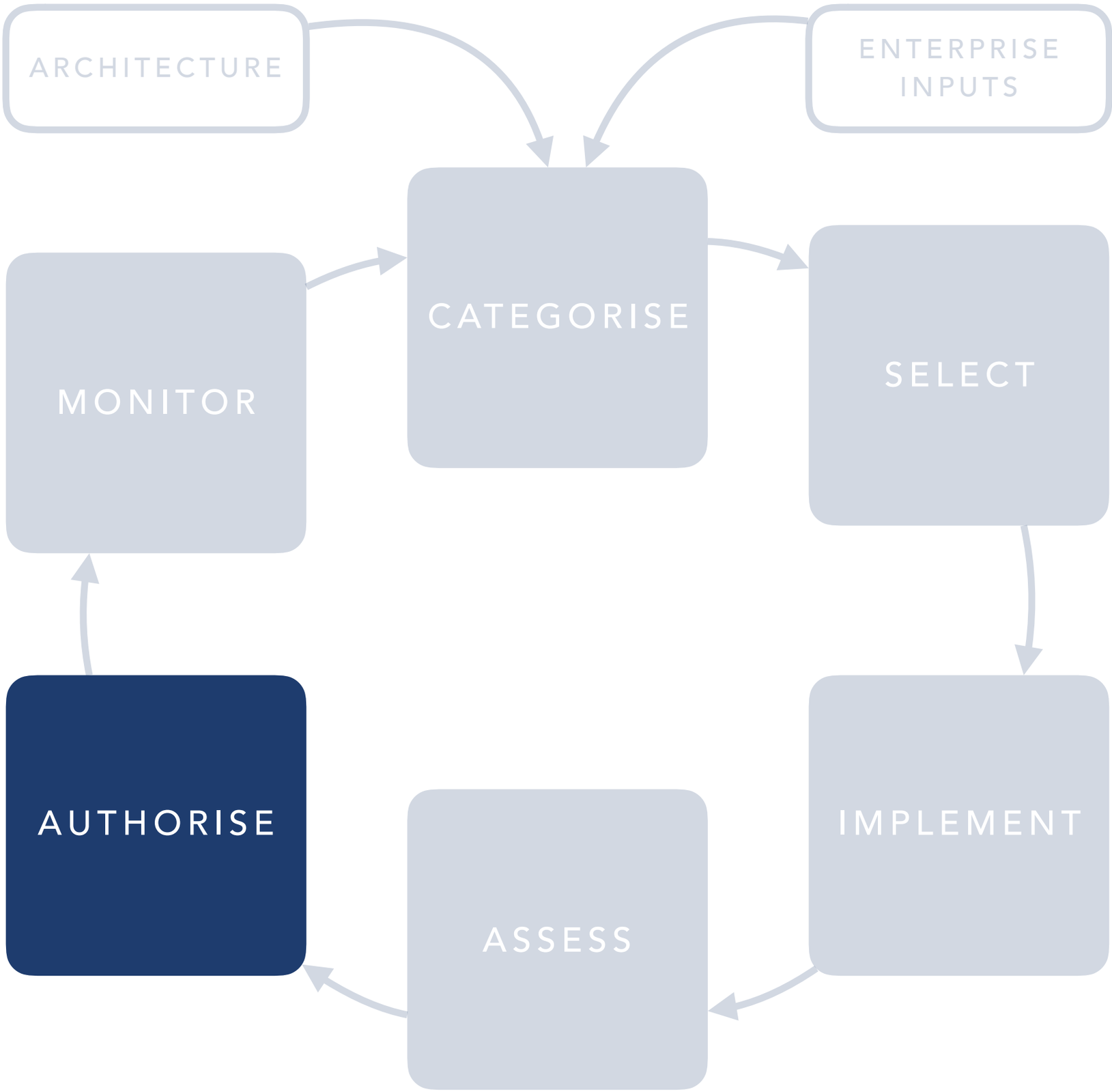
NIST RISK MANAGEMENT FRAMEWORK



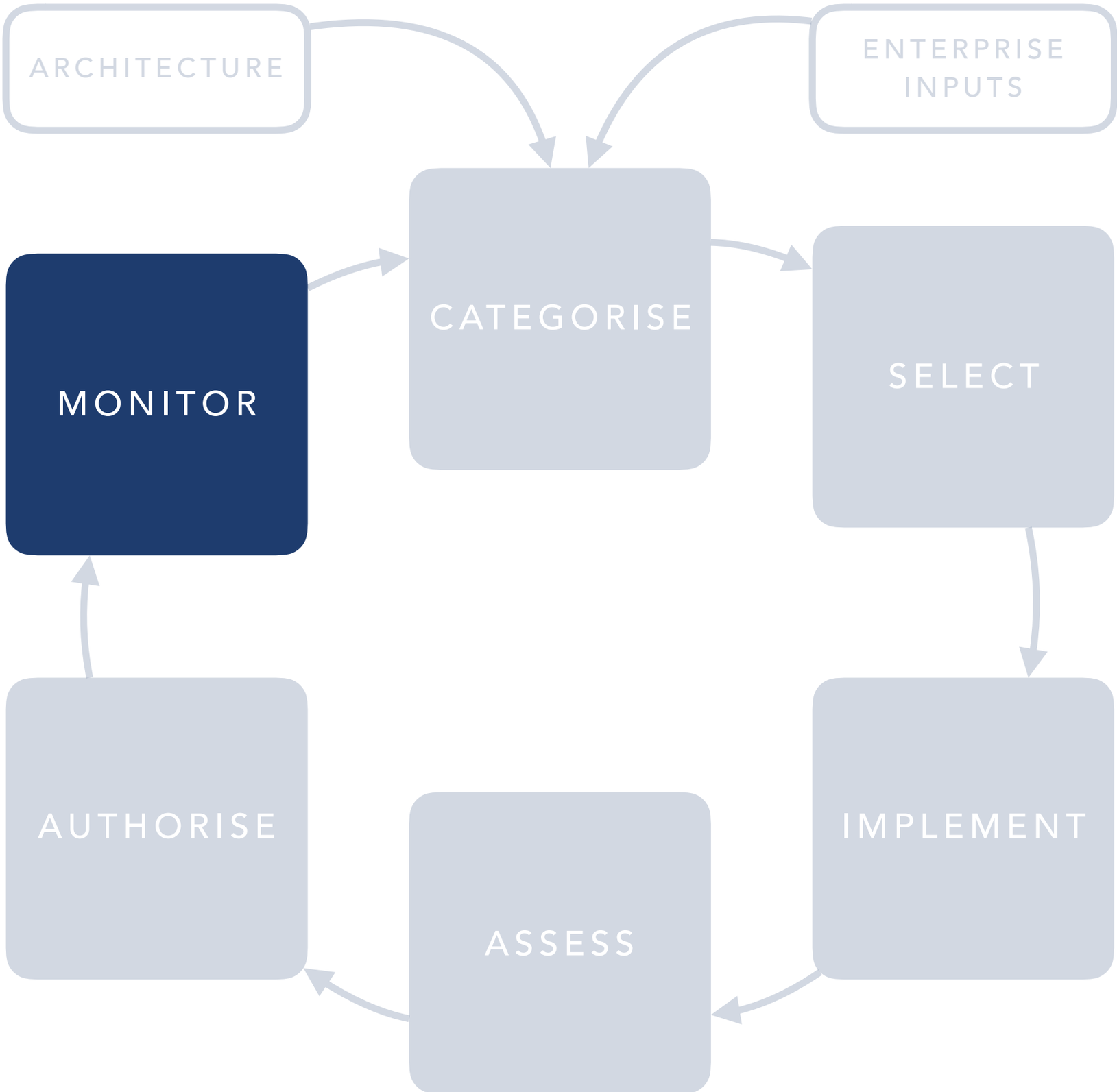
NIST RISK MANAGEMENT FRAMEWORK



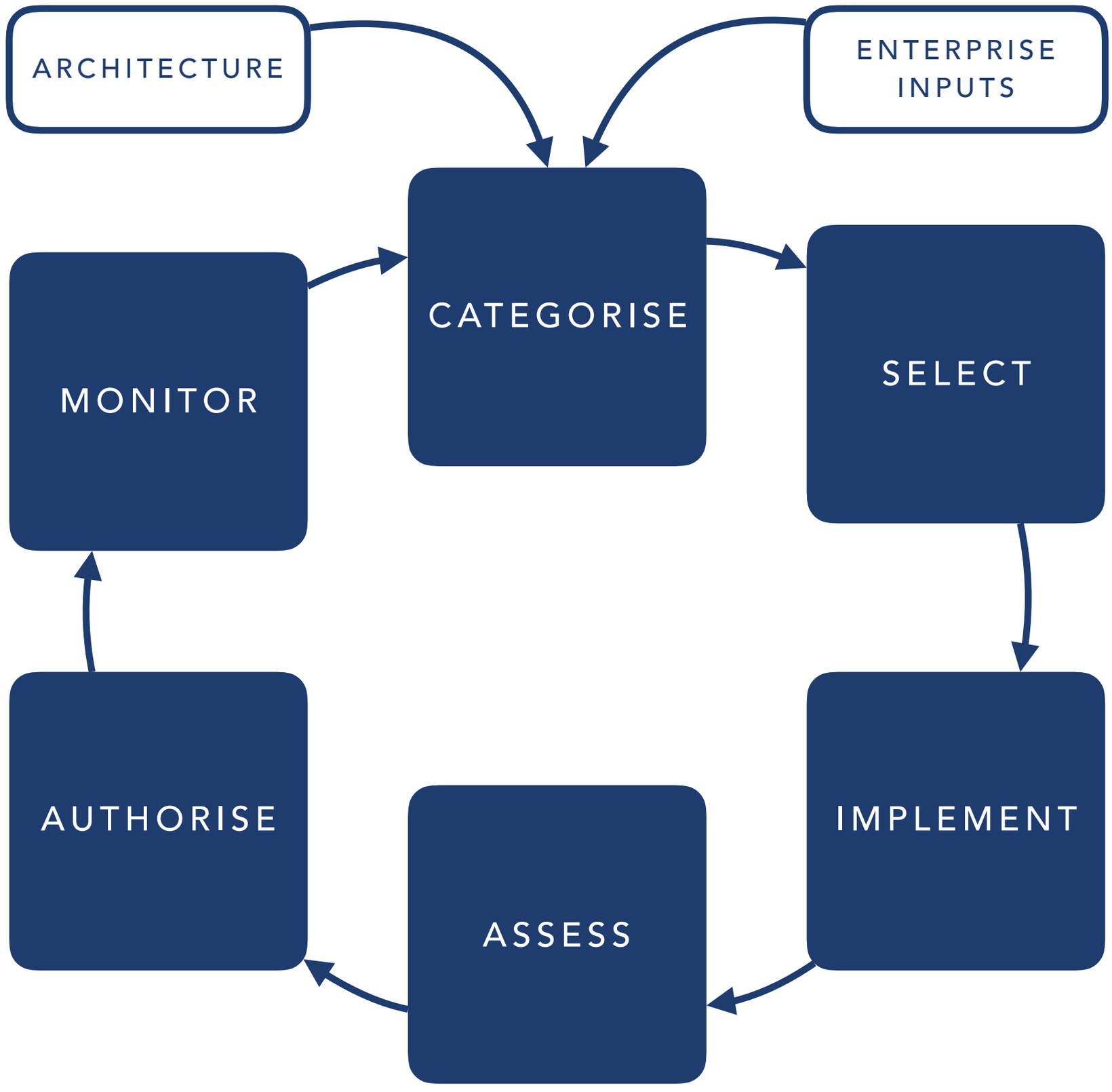
NIST RISK MANAGEMENT FRAMEWORK



NIST RISK MANAGEMENT FRAMEWORK



NIST RISK MANAGEMENT FRAMEWORK



NIST SP800-53

- Security and Privacy Controls for Federal Information Systems and Organisations
- as the title suggests, it is a **catalogue** of security and privacy controls.
- controls live at different tiers within the enterprise between **strategic** and **tactical** focus.
- catalogue advocates against the notion of a single, protection is the representation of **many controls**.
- generic in approach, but offers guidance on how to **tailor** it to specific industries and enterprises.

NIST SP800-53 TYPICAL STRUCTURE

- family and name of control itself.
- detailed statement of control
- supplement guidance and related controls
- enhancements to the baseline control

CONCERNS

CONCERNS

- debatable **scalability** as the process focuses more on single systems rather than systems of systems.

- considerable **focus on prevention**, less attention is on monitoring and detection as controls for strengthening an enterprise.

- **assessment** is subjective rather than scientific and/or prioritised.

- **constraining requirements** on vendors, partners as well as systems and components.

- debatable if accessible to smaller subsystems.

BENEFITS

(ISC)² COMMON BODY OF KNOWLEDGE

(ISC)² COMMON BODY OF KNOWLEDGE (CBK)

- **collection of knowledge**, informations, taxonomies and terms - that experts are meant to know.

- common body of knowledge can be used to **debate, discuss, argue and transfer knowledge**.

- CBK can be used to **inform training as well as educational materials** as areas of interest.

- CBK is base for training **Certified Information Systems Security Professionals** (CISSP).

(ISC)² COMMON BODY OF KNOWLEDGE (CBK)

1	ACCESS CONTROL	6	ARCHITECTURE
2	COMMUNICATION	7	OPERATIONS
3	GOVERNANCE	8	BUSINESS CONTINUITY
4	SOFTWARE DEVELOPMENT	9	REGULATORY
5	CRYPTOGRAPHY	10	PHYSICAL

CONCERNS

(ISC)² COMMON BODY OF KNOWLEDGE (CBK) CONCERNS

- concerns about the **relevancy** of material contained with the common body of knowledge.

- **evolution** of material is also challenging, may find little difference between the common body of knowledge from now and a decade prior.

- **criticism** that the common body of knowledge is not valid, that it does not reflect the concerns of practitioners.

BENEFITS

(ISC)² COMMON BODY OF KNOWLEDGE (CBK) BENEFITS

- ethics.
- affords professionals to become experts in security.
- accepted body of knowledge.
- continuing professional development.

CENTRE FOR INTERNET SECURITY

CRITICAL SECURITY CONTROLS (CSC)

CRITICAL SECURITY CONTROLS (CSC)

- original developed by SANS institute, private for-profit organisation specialising in cyber security training.
- managed and developed by the Centre for Internet Security since 2015.
- designed to appeal to IT professionals - simple language to promote automated controls.
- created through consultation with several organisations in many different domains.

CRITICAL SECURITY CONTROLS (CSC) BENEFITS

- **areas of focus** for an enterprise to extract maximum benefit for investment.

- simple language aimed at IT professionals to implement **automated controls**.

- controls are developed from regular **consultation** with contributors from many domains.

- provides an **ecosystem** of products and systems for enterprise to utilise.

- Centre for the Protection of National Infrastructure (CPNI) promote CSC controls to cut through the **‘fog of more’**.

CRITICAL SECURITY CONTROLS (CSC) CONCERNS

- **product** or ecosystem focused, rather than being driven by actual threats.

- **review** is difficult as its not clear what are the metrics for success.

- **consultation** is advocated, but the specification controls is not organic.

- unclear how the controls fits within the wider landscape of frameworks and standards.

COMMON CRITERIA

COMMON CRITERIA

- internationally recognised criteria for information security products.

- support enterprises in purchasing products that meet their security functional requirements (SFRs) and security assurance requirements (SARs)

- governments and sophisticated enterprises can demand products that meet the criteria.

COMMON CRITERIA

- Protection Profile (PP), implementation-independent document, set of security requirements for a class of Targets of Evaluation (TOEs).

- Security Target (ST), documented, claimed security properties of TOE.

- ST can claim that it meets specific PPs.

- Common Criteria can indicate potential SFRs and their dependencies.

COMMON CRITERIA

- organisations can purchase equipment independently verified meeting security requirements.
- common criteria can be applied to operating systems as smart cards.
- protection profile (PP) is specified for each of these products.
- think of these are generic security requirements for any product in that class.

APPLE MAC OS X 10.6

APPLE MAC OS X 10.6

1 Executive Summary

The Target of Evaluation (TOE) is the operating system Apple Mac OS X 10.6, delivered in two different types: Apple Mac OS X Server 10.6 and Apple Mac OS X 10.6.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Controlled Access Protection Profile, Version 1.d as of 1999-10-08; providing demonstrable conformance.

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL3 augmented by ALC_FLR.3.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The TOE Security Functional Requirements are implemented by the following TOE Security Functions:

TOE Security Function	Addressed issue
Audit	The TOE has the ability to audit user actions and store the records in an audit trail that is protected from unauthorized access. The administrator has the ability to select which events get audited.
User Data Protection	The TOE provides a discretionary access control mechanism to

COMMON CRITERIA BENEFITS

COMMON CRITERIA BENEFITS

- support many individuals that simply lack specialist knowledge to make decisions.
- strong at identifying problems and lack of clarity in documentation.
- can be included and form part of service contracts with external subsystems.
- accessible to smaller subsystems supporting disruption in different domains.

COMMON CRITERIA CONCERNS

COMMON CRITERIA CONCERNS

- **expense** in the evaluation process of products means the economics may not work for many vendors.

- **disruptive** products from startups are at a disadvantage as they may not be able to justify the expense.

- **evaluation** of the process can mean that version 2.0 is ready, once version 1.0 is approved.

COMMON CRITERIA CONCERNS

- **influence** over the evaluation process itself and relevancy to the wider industry, including software development.

- **clarity** in terms of the focus of the evaluation, considerable focus can be on what the system claims to do, rather than what is actually does.

- **confidence** in that the product performs in the way expected and as it crosses into different territories.

INTERNATIONAL ORGANISATION FOR STANDARDISATION (ISO) 27001/27002

ISO 27001/27002

- **International Organisation for Standardisation**, independent, no-one government, supporting 162 countries.
- **English, French and Russian** - referred to as ISO rather than IOS.
- standards and best practice apply to **many different domains**.
- support global trade as well as disruption of existing economies and markets.
- Common Criteria is an ISO standard (ISO 15408)

ISO 27001/27002

1	POLICIES	8	OPERATIONAL SECURITY
2	ORGANISATION	9	COMMUNICATIONS
3	HR SECURITY	10	SYSTEM DEVELOPMENT
4	ASSETS	11	SUPPLIER RELATIONSHIPS
5	ACCESS CONTROL	12	INCIDENT MANAGEMENT
6	CRYPTOGRAPHY	13	BUSINESS CONTINUITY
7	PHYSICAL SECURITY	14	COMPLIANCE

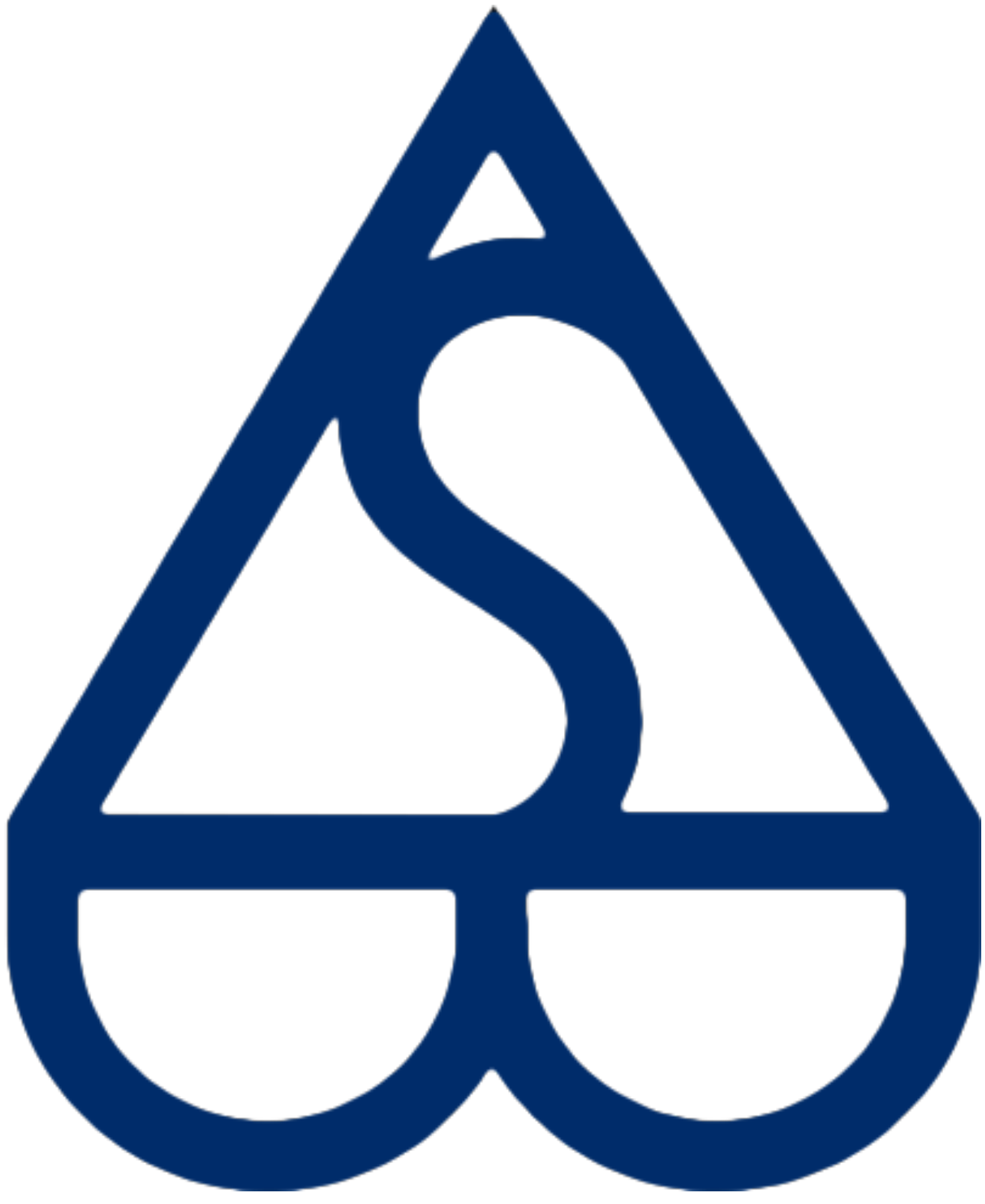
ISO 27001/27002

- **ISO 27001** best practice framework for Information Security Management System (ISMS) in enterprises.

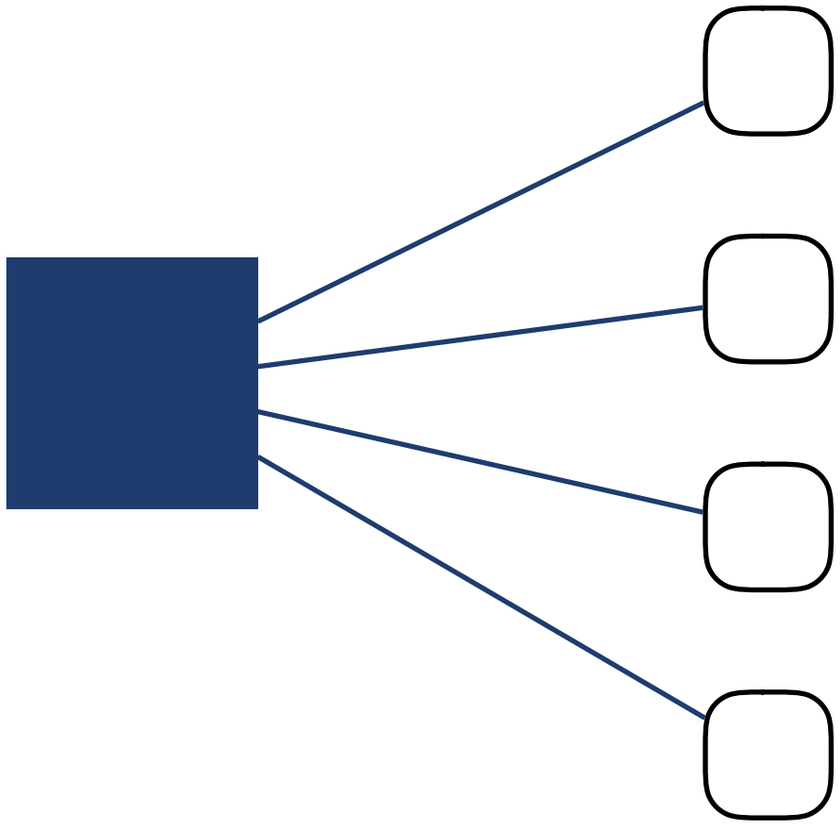
- **ISO 27002** set of practice for specific controls.

- organisations can be **independently** assessed and audited by external organisation.

- ISO 27001/27002 2013 is 114 controls over 14 families.



MAINFRAME ERA (1950S-70S)



BSI 7799

- British Standards Institute guidance on best practice and guidance on Information Security Management.
- foundations of the standard came from Shell, they donated research and efforts to the organisation.
- guidance and concepts circled around the idea of legacy-era systems and mainframe architecture.
- standard was originally released in 1995 and simply did not consider cyber space.

PDCA

- proposed by Edwards Deming as an approach to improve effectiveness of business processes.
- understand the problem by collecting and analysing data, devise a plan to address it.
- develop a solution to the problem and deploy it, collect measurements to understand effectiveness.
- check that solution actually addresses the perceived problem.
- produce report, communicate changes and identify the next set of problems.

ISO 27001/27002 BENEFITS

ISO 27001/27002 BENEFITS

- affords interoperability between different enterprises.
- smaller subsystems can demonstrate compliance with an agreed standard.
- support competitive controls and training programs as there is an agreed international standard.
- scalable between small and large organisations.

ISO 27001/27002 CONCERNS

ISO 27001/27002 CONCERNS

- legacy mainframes influence the release and update of standards compared to the threats that emerge everyday.
- trade focused rather than consumer focused.
- independence.
- difference in adoption between countries.
- scope can be challenging and can be misleading.

STANDARDS AND SOCIETY

SMALL GROUP DISCUSSION

ENTERPRISE CYBER SECURITY

REFLECTION AND REVISION

University of Glasgow