Policy

Policy

把（法律、條例）編集成典

- Cyber security policy can be considered the **codification of cyber security objectives** to support desired behaviour to achieve said objectives.

- Objectives do not **easily translate** into specific behaviours. Policies provide the blueprint for the overall cyber security approach for your organisation.

- Policies present security goals, rather than specifications. Policies may require the documentation of implementation, but implementation should not form part of policy.

History of policies

- Several enterprises collapsed within the United Kingdom in the 1980s. State questioned the approach to management and governance of many organisations.
- For example: Bank of Credit and Commerce International (BCCI) was forced to closed due to poor management.
- 1992 Cadbury Report made several recommendations to minimise the threats to assets through poor management.

Governance

- Policy aims will alter inline with the governing body. Policy is governed by a given group and applies to a specific realm.
- Policy producing process will also be influenced by the governing body. Many policies may be governed by different units within an organisation, potentially creating conflicts and overlaps.

Power of Policies

Policy process

What are policies?

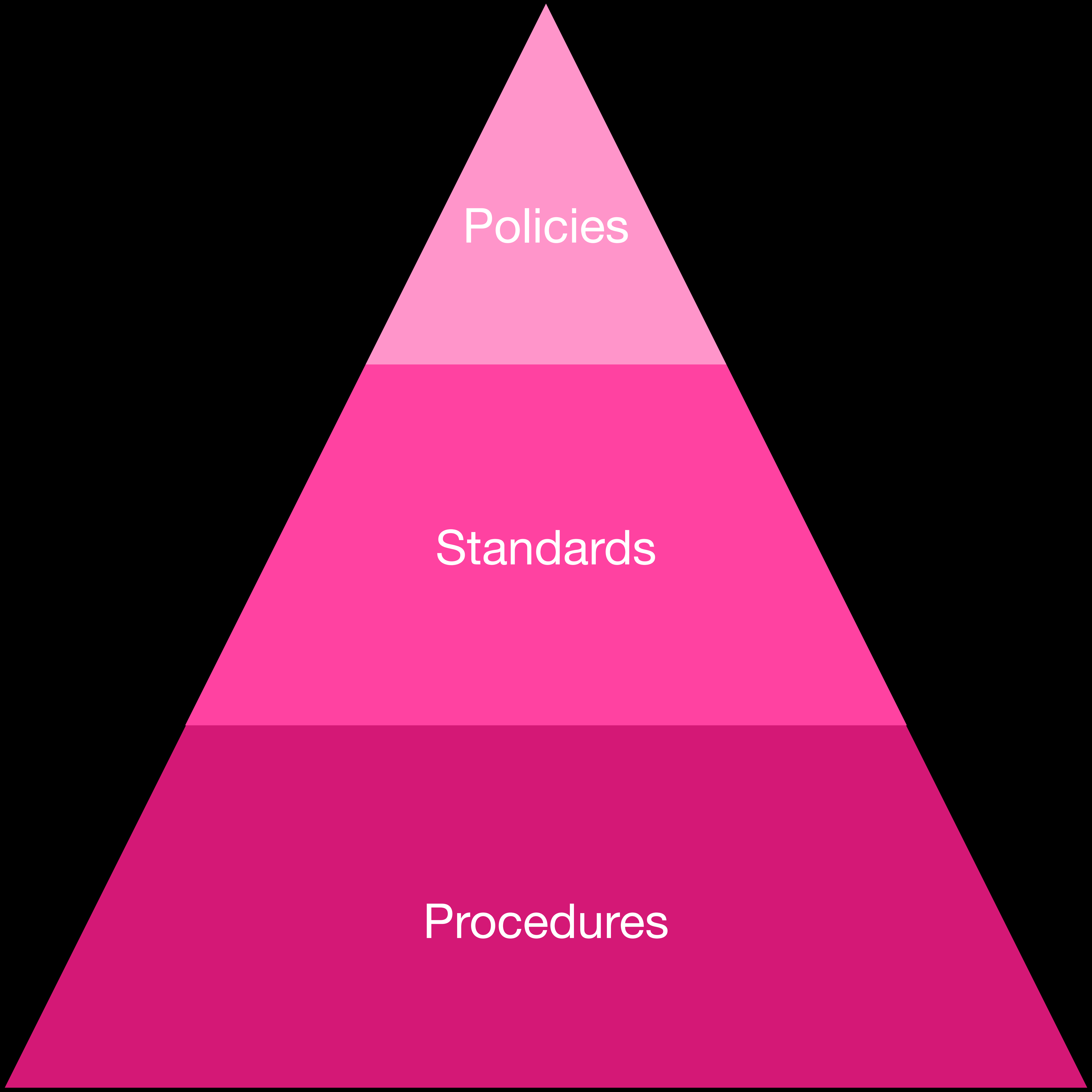
What are policies?

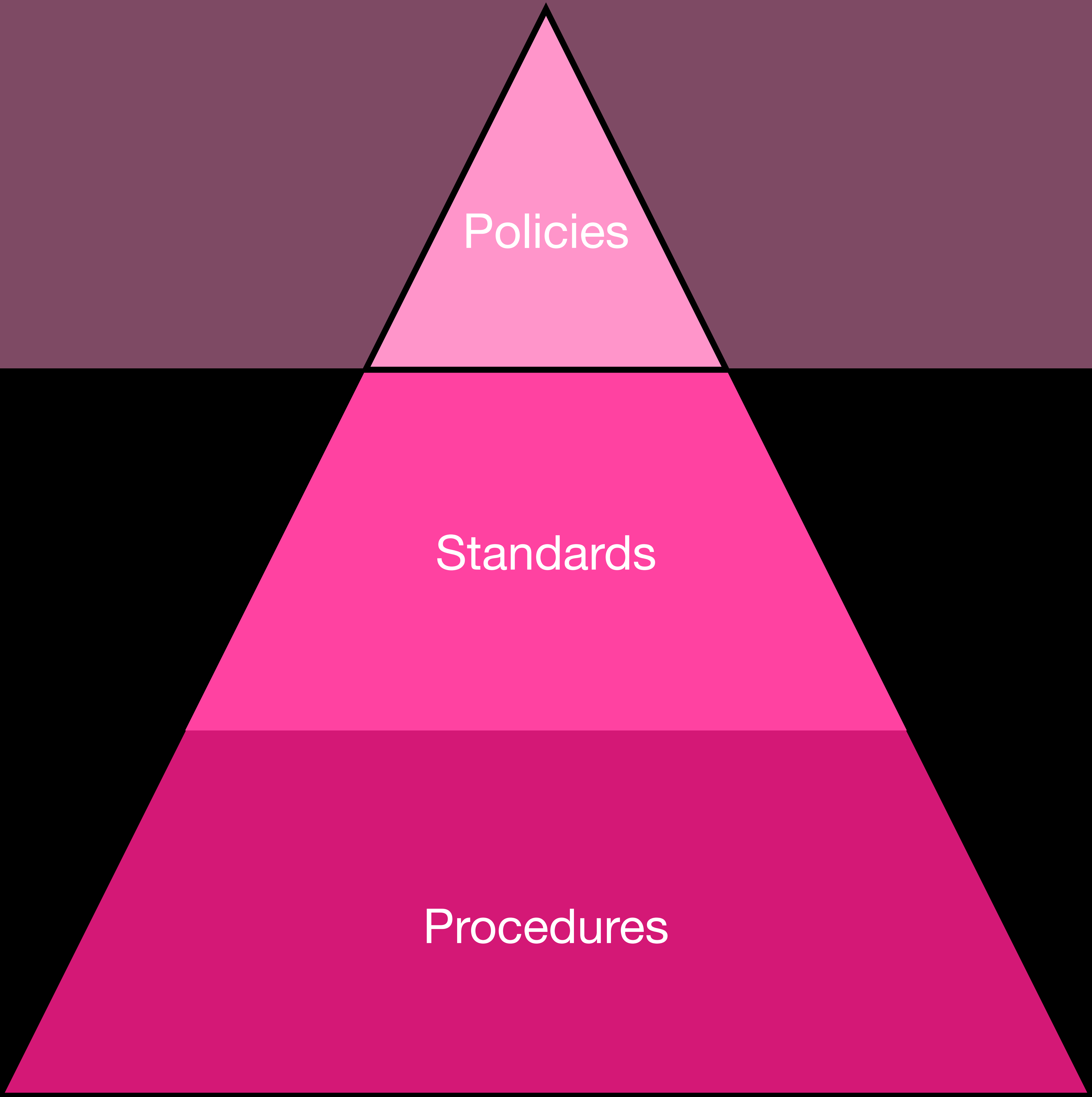
- Instructions from management that **indicate the expected governance** of that organisation.
- Comprises **not only of general directives**, but can also contain goals, objectives, beliefs and responsibilities.
- Policies may be complimented with instructions, guidelines or procedures to support attainting the general instructions they communicate.
- Policies themselves are not standards or procedures, policies are expected to endure for several years, they do not outline implementation details or mention specific technology.

Policies are not procedures

- Policies are **not specific implementation instructions or specific procedures**, for example to duplicate a data repository.
- Policies are not controls, but can controls can be used to meet policy directives and objectives.
  - A policy directive prohibiting conflicts of interest could be obtained with a control that requires employees to complete a declaration.
  - … though policies may state controls that are required.
- Generally, policy represent the areas of interest and focus for management.

Hierarchy of Governance

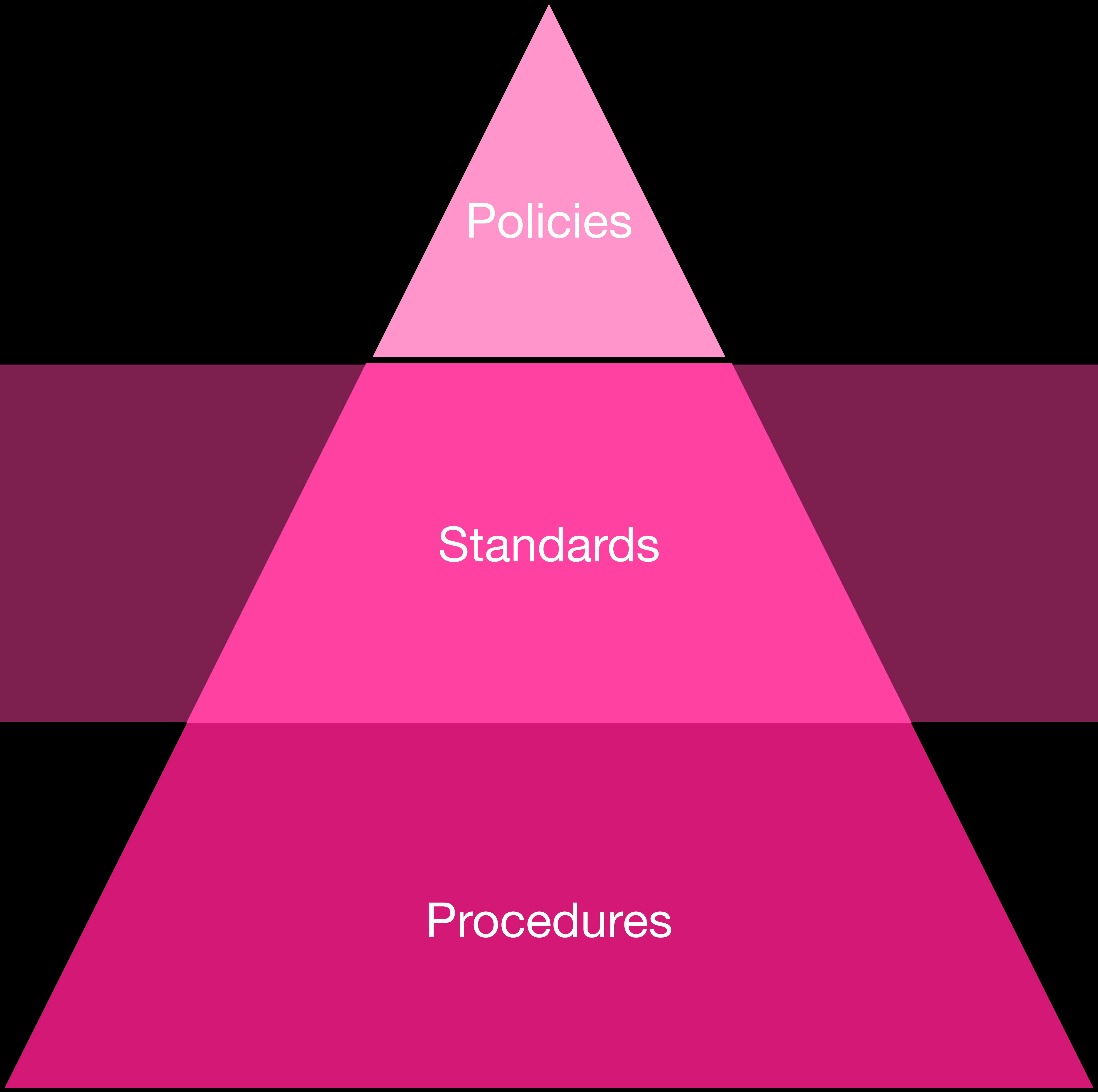

Policies
Standards
Procedures



The high-level objectives of the organisation and directives to mitigate and minimise risks.

Specific standards that can be employed to meet the objectives and directives of the policy.

Detailed instructions that employees follow to complete process.



Policies

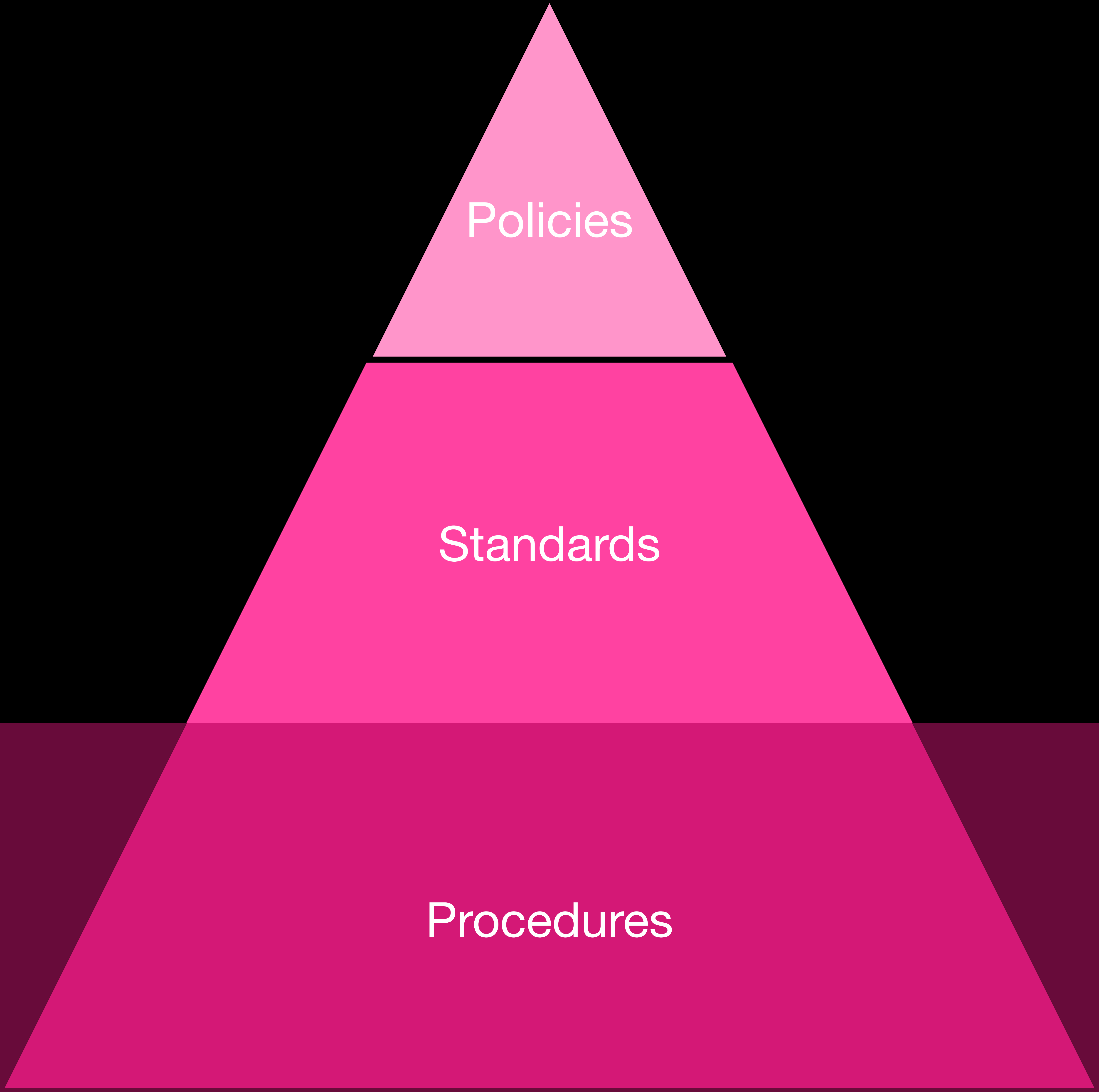
The high-level objectives of the organisation and directives to mitigate and minimise risks.

Standards

Specific standards that can be employed to meet the objectives and directives of the policy.

Procedures

Detailed instructions that employees follow to complete process.



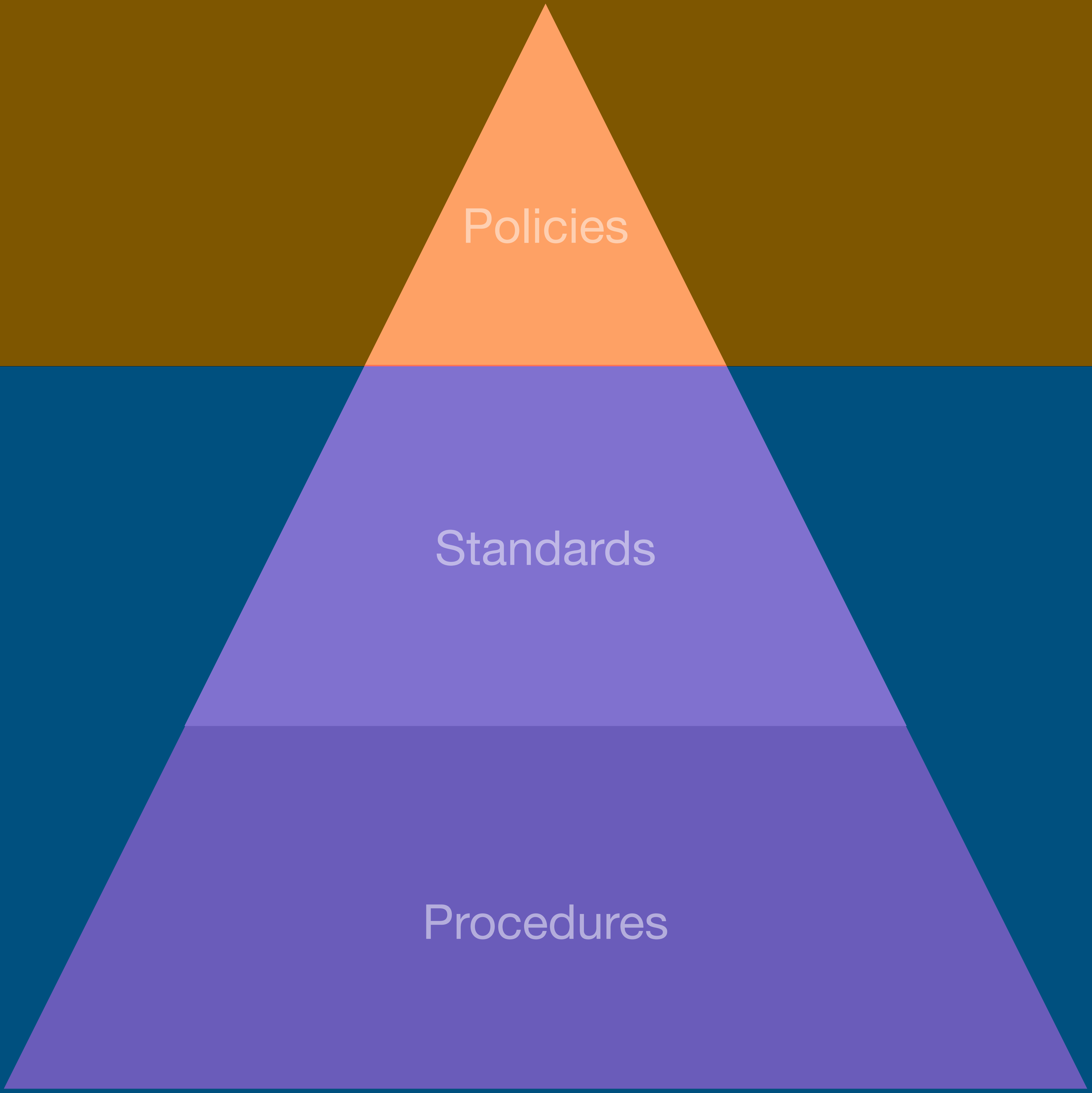
The high-level objectives of the organisation and directives to mitigate and minimise risks.

Specific standards that can be employed to meet the objectives and directives of the policy.

Detailed instructions that employees follow to complete process.

WHAT

HOW



Policies

Standards

Procedures

Motivation for Policies

Motivation for Policies

- Consistency
- Controls and Products
- Distribution of Knowledge
- Expectations
- Compliance and Audit
- Avoiding Liability
- Tone
- Management Endorsement

Consistency

Motivation for Policies

- Policies can reduce **inconsistent behaviours** between employees and partners and can contribute to consistent responses to problems.
- Policies can reduce autonomy for individuals and leaders and ensure **consistent application of the rules**.
- **Exert caution**, reducing autonomy can improve security in one direction, but can also impact negatively on the enterprise or other aspects of security.

Controls and Products

Motivation for Policies

- Enterprises may assume that security can be attained only with the purchase of a security software and hardware product, The product has to be deployed in **adherence with the context**, policy is crucial in achieving such objectives.

- Enterprise often do not have the competencies or the ability to create specific technical controls, they purchase them or select them from a library of options. **Policy is valuable in supporting enterprises to make selections** or purchase products, even commission them.

Distribution of Knowledge

Motivation for Policies

- Policies provide an **effective communication channel** to distrubite knowledge throughout an organisation.

- Policies provide **information for employees to consume**, there is little benefit in security experts within the enterprise knowing not to share passwords, if the rest of the organisation is unaware.

Expectations

Motivation for Policies

- Policies in powerful in **setting boundaries and rules for employees** when it comes to using systems.
- **Establish foundation for disciplinary actions** as enterprises can use policy to clarify **what is permitted and what is not permitted with systems.**

Compliance and Audit

Motivation for Policies

- The process involved in creating policy can be effective in the organisation **considering legal and regulatory concerns.**
- Many regulators will **expect policies to exist**, especially from the perspective that their existence likely points to a process that considers various aspects of the business.

Avoiding Liability

Motivation for Policies

- The process to creating policies at the very least allows enterprises to demonstrate that they have **at least thought about the security of their organisation.**
- Management will want to ensure they **avoid accusations** of not performing due diligence or not attaining the standard expected of the industry or peers.

Avoiding Liability

Tone

Motivation for Policies

- Policy valuable in setting the tone for security within the organisation, that employees will project.

Management Endorsement

Motivation for Policies

- Policy is an effective tool for management to demonstrate to employees and partners that **security is important** and that employees **should pay attention to security** in their role.
- Policies that are **not supported by management are unlikely to succeed** within an organisation.

Motivation for Policies

- Consistency
- Controls and Products
- Distribution of Knowledge
- Expectations
- Compliance and Audit
- Avoiding Liability
- Tone
- Management Endorsement

Language

Language

- Policy only outlines the **general solution** for addressing a problem it is not implementation, it does not give specific steps.

- Directives should be **short** and **simple** as if it is too long people may ignore it and communicate **what** an organisation is seeking to achieve.

  - Clear language such as “must”, “do” or “will” and not contain ambiguous and vague language as “try” and “should” as policies are not optional.

- Policy is meant to be read and followed, not overly complex or prose-like, limited sentences and/or bullet-point format will suffice.

- Policy language **must be clear and not vague**, for example: “consider security when reading emails”.

Realistic expectations

Language

- Policy directives should be **realistic in the expectation** of what they want in terms of desired behaviours.

- Policy directives **should not prohibit that they can not enforce**, otherwise it is likely employees will not adhere to policy.

- Policy directives must not be designed in such a way that makes them **difficult or unrealistic to follow.**

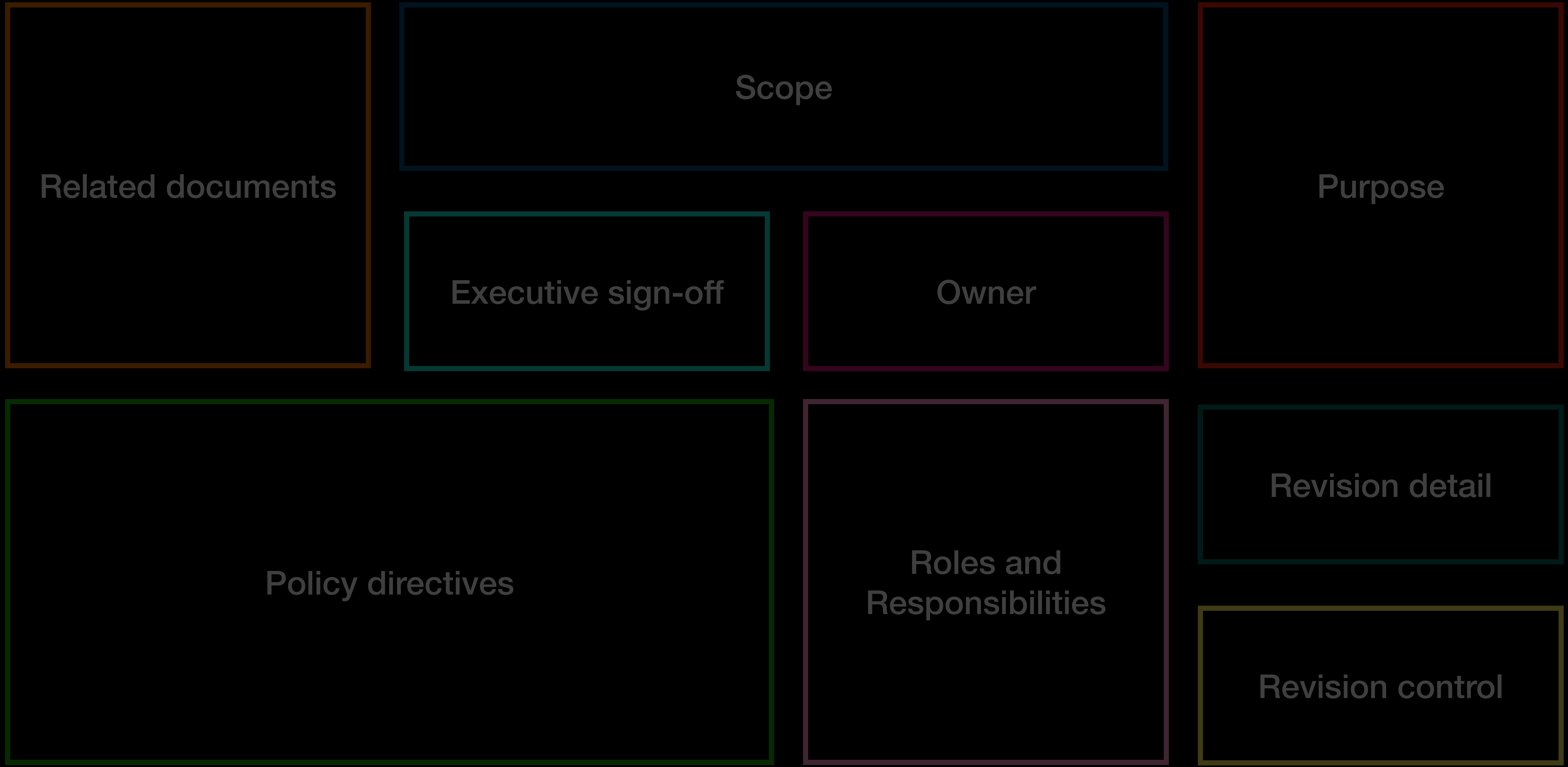
- Policy directives must **operate within the legal and regulatory environment.**

Inclusive vs Exclusive

Language

- Policies may be inclusive or exclusive, decisions need to be taken to determine the best option.
- Inclusive policies indicate what is **permitted**, while exclusive policies state what is **prohibited**.
  - Inclusive policies essentially prohibit unknown or new applications and services, but then they need to be updated when application because known.

Contents



Related documents

Scope

Purpose

Executive sign-off

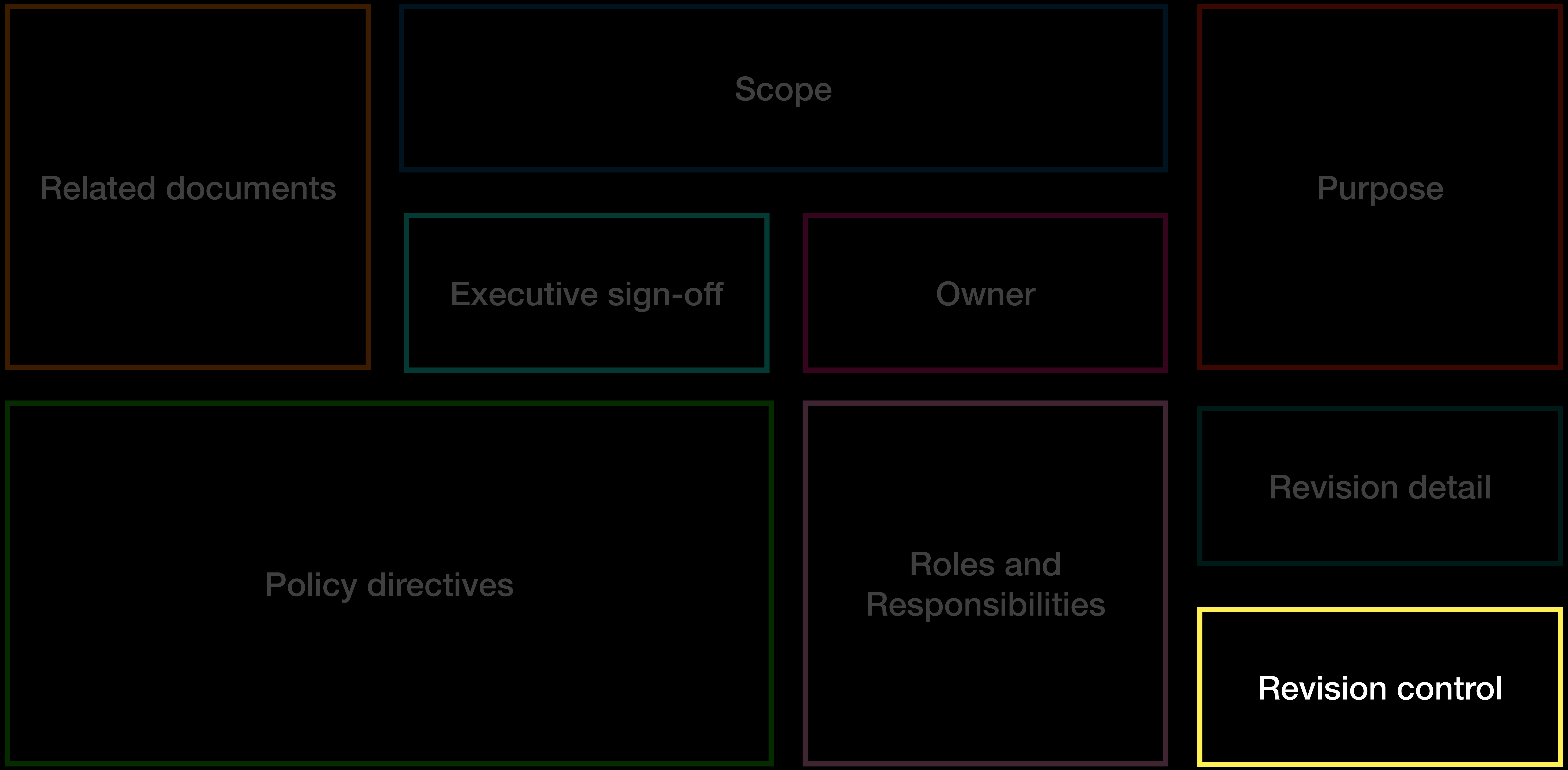
Owner

Policy directives

Roles and Responsibilities

Revision detail

Revision control



Related documents

Scope

Purpose

Executive sign-off

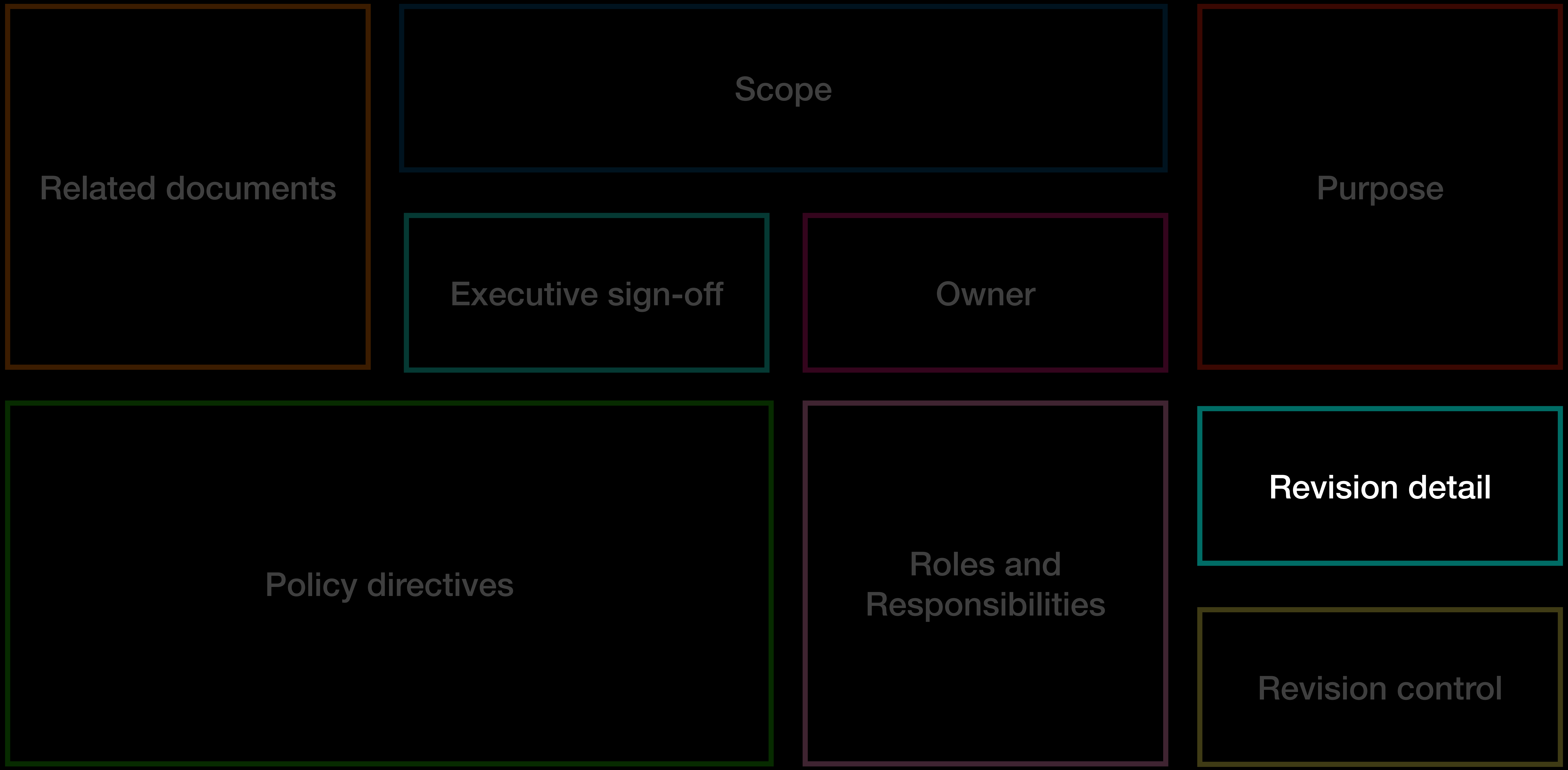
Owner

Policy directives

Roles and Responsibilities

Revision detail

Revision control



Related documents

Scope

Executive sign-off

Owner

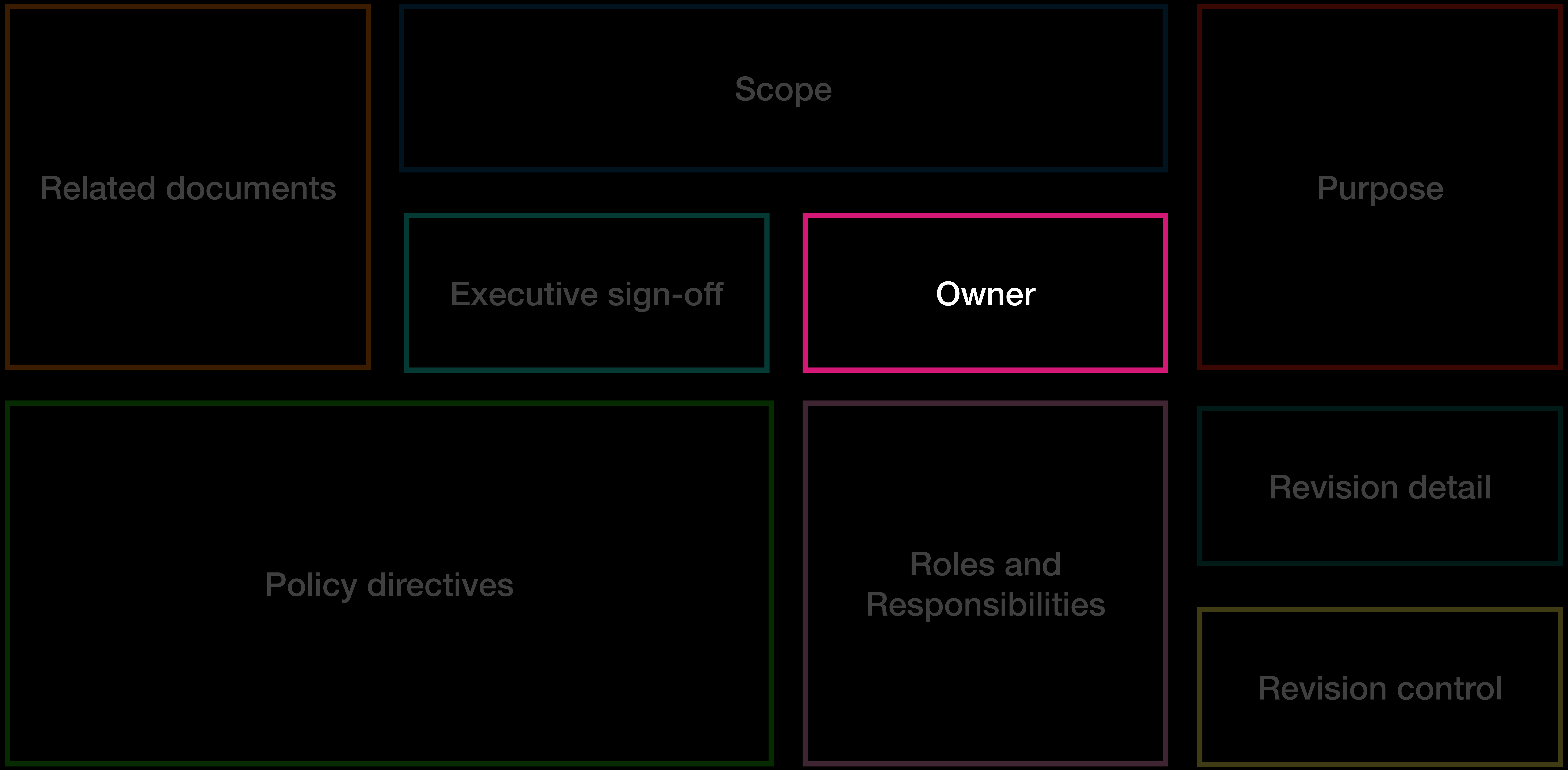
Purpose

Policy directives

Roles and Responsibilities

Revision detail

Revision control



Related documents

Scope

Purpose

Executive sign-off

Owner

Policy directives

Roles and Responsibilities

Revision detail

Revision control

Related documents

Scope

Purpose

Executive sign-off

Owner

Policy directives

Roles and Responsibilities

Revision detail

Revision control

Related documents

Scope

Purpose

Executive sign-off

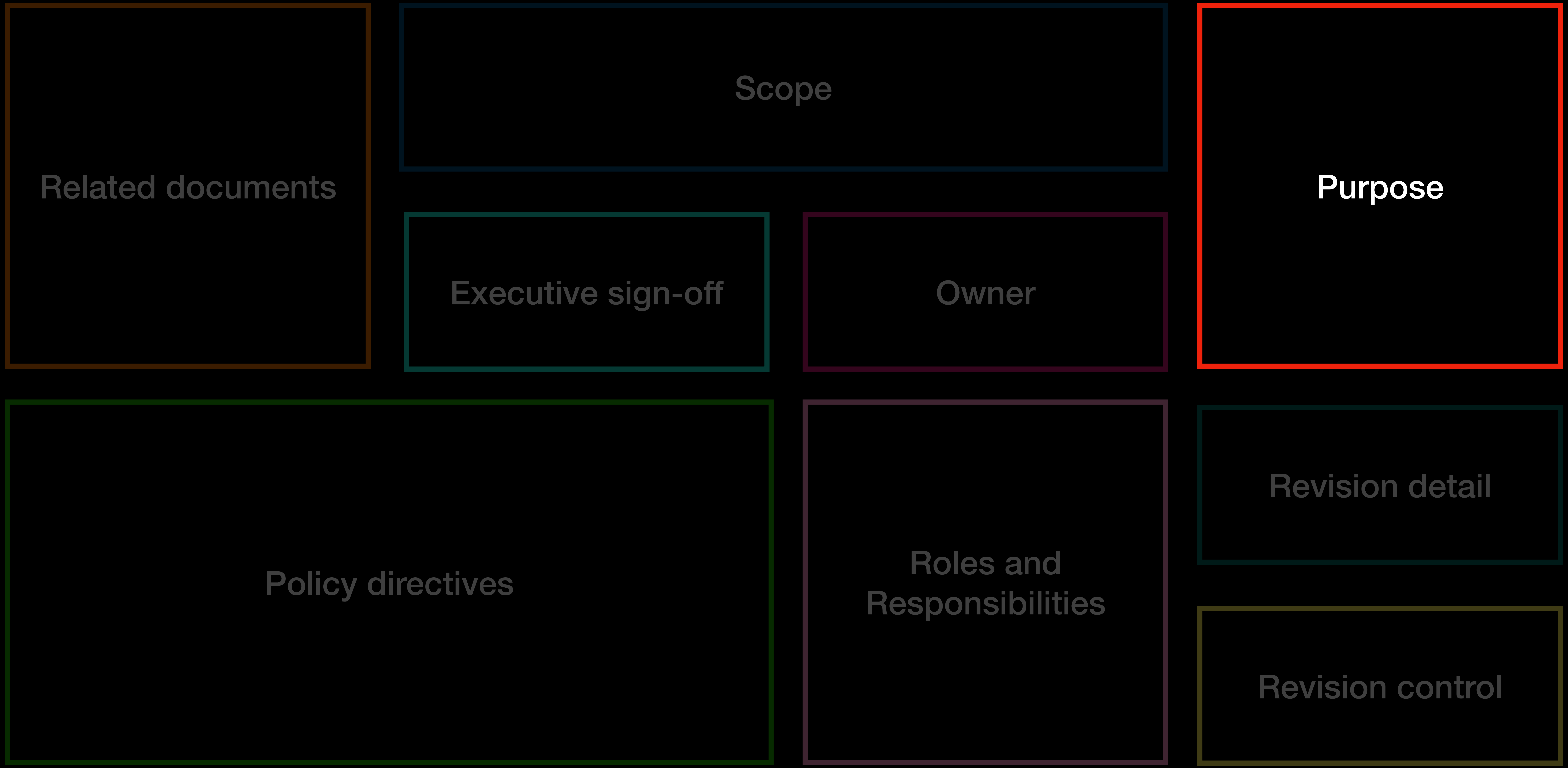
Owner

Policy directives

Roles and Responsibilities

Revision detail

Revision control



Related documents

Scope

Executive sign-off

Owner

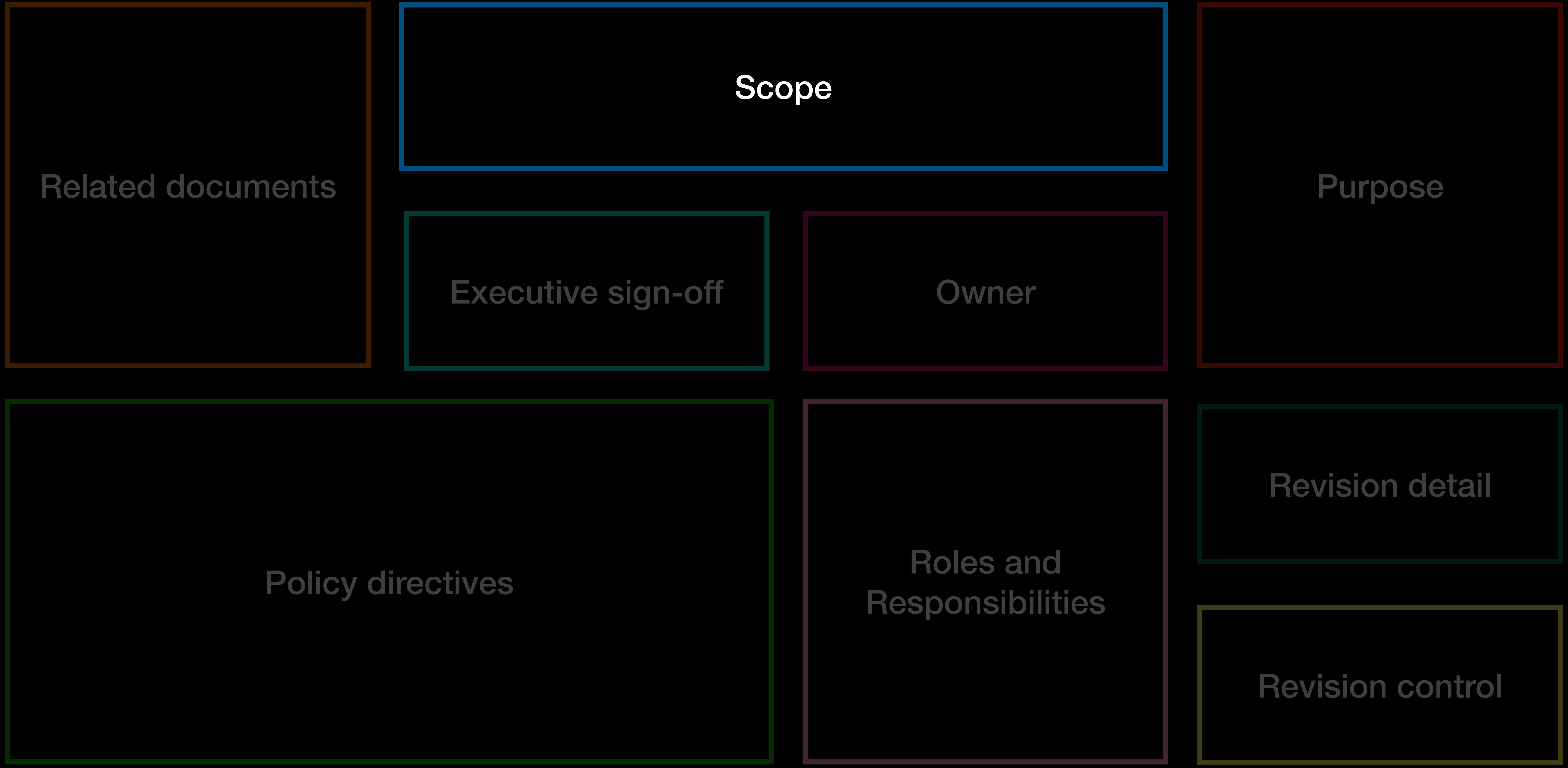
Purpose

Policy directives

Roles and Responsibilities

Revision detail

Revision control



Related documents

Scope

Executive sign-off

Owner

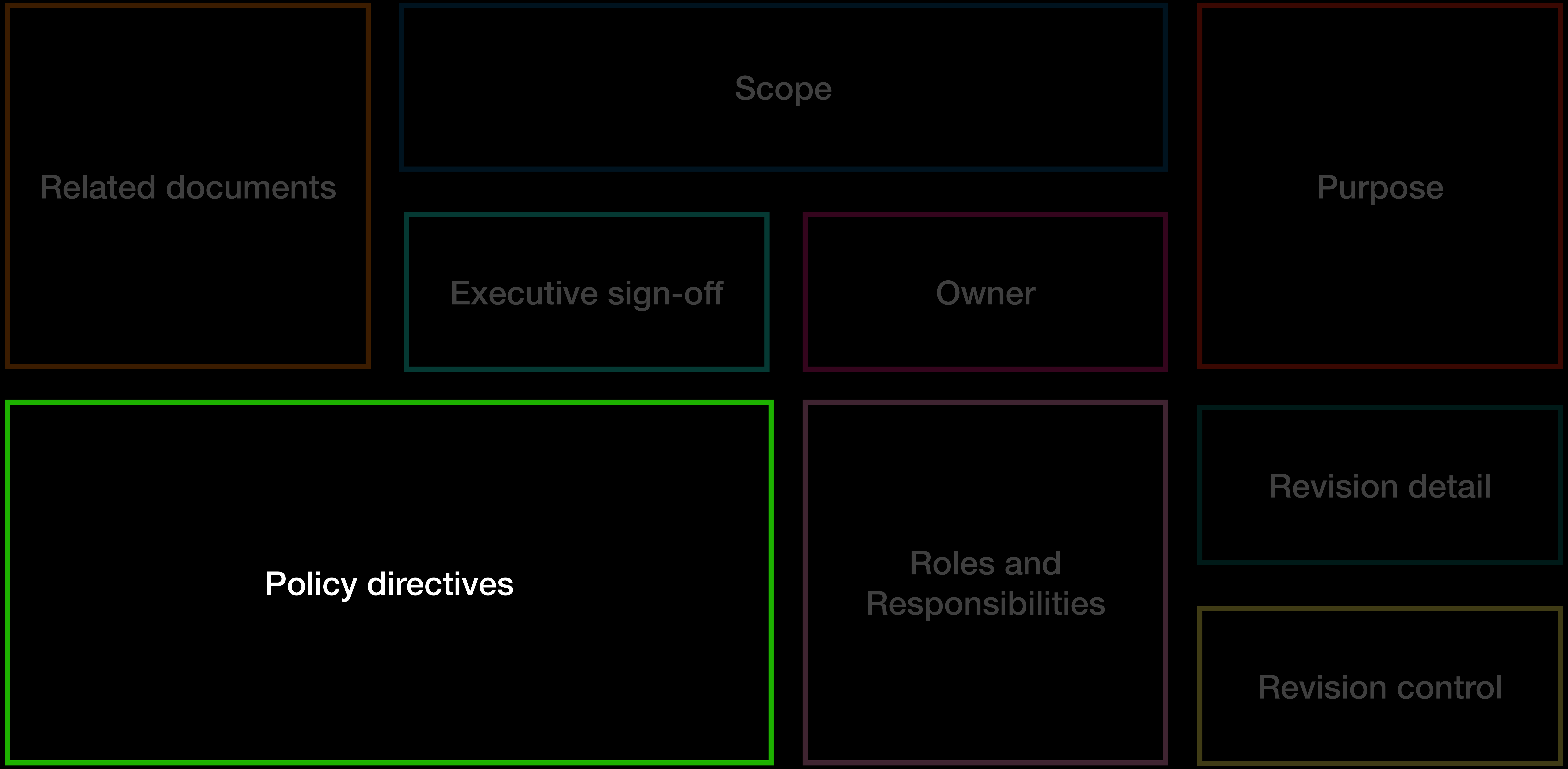
Purpose

Policy directives

Roles and Responsibilities

Revision detail

Revision control



Related documents

Scope

Purpose

Executive sign-off

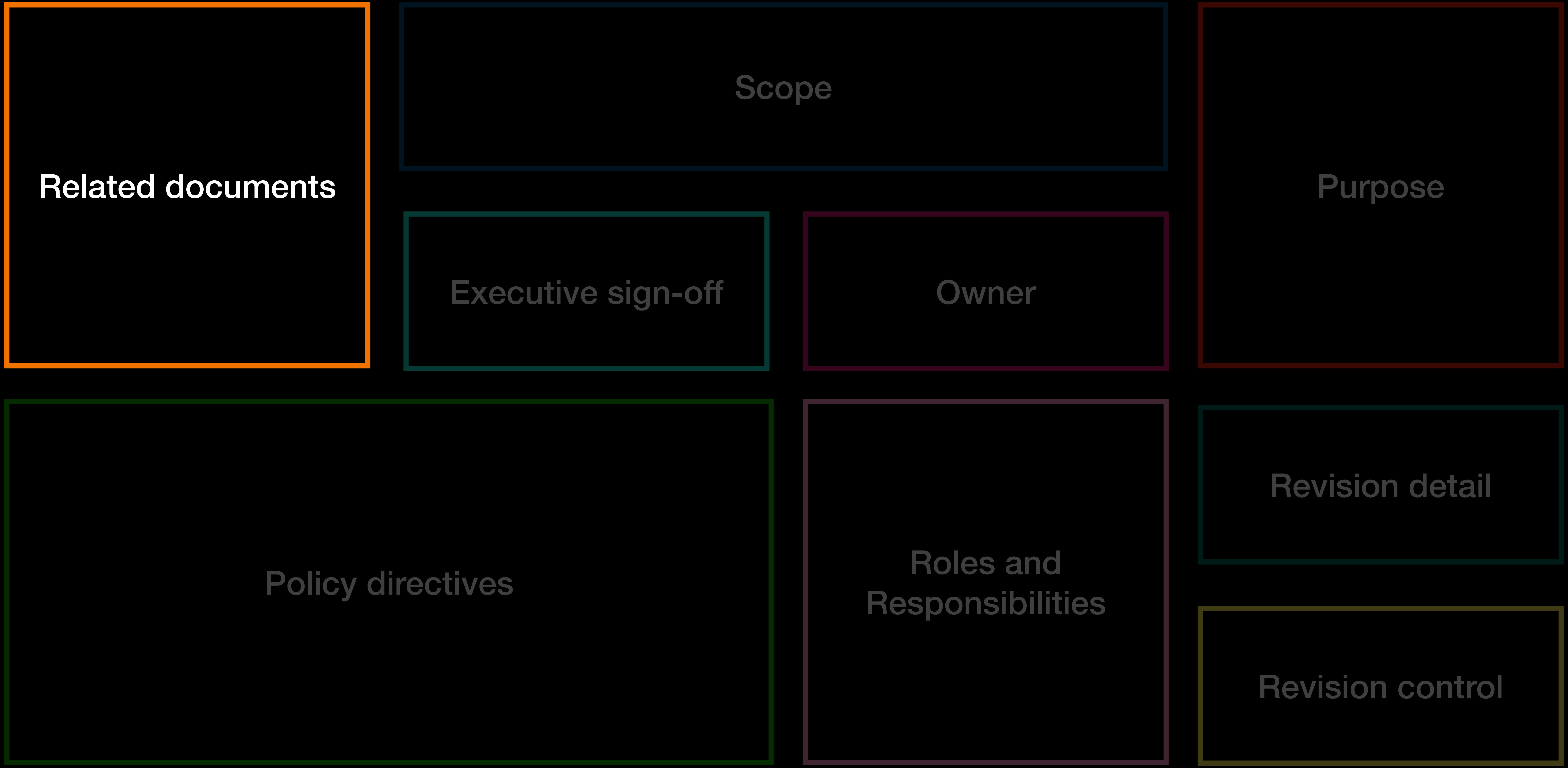
Owner

Policy directives

Roles and Responsibilities

Revision detail

Revision control



Related documents

Scope

Purpose

Executive sign-off

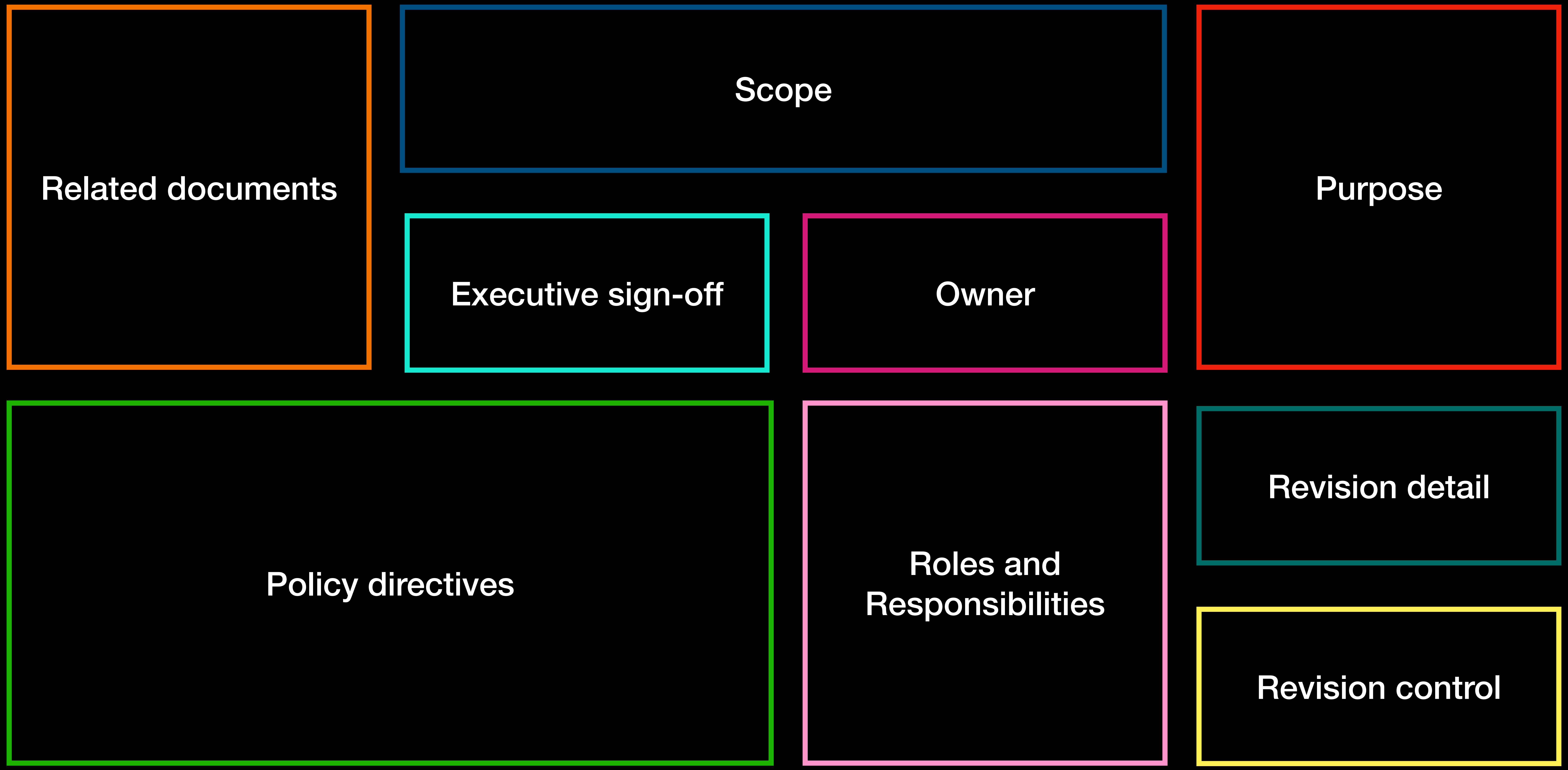
Owner

Policy directives

Roles and Responsibilities

Revision detail

Revision control



Related documents

Scope

Executive sign-off

Owner

Purpose

Policy directives

Roles and Responsibilities

Revision detail

Revision control

Policy Topics

sign-off

Mobile Device Encryption Policy

Mobile Employee Endpoint Responsibility Policy

Pandemic Response Planning Policy

Password Construction Guidelines

Pers
Commu
Devices an

Lab Security Policy

DMZ Lab Security Policy

Email Retention Policy

Email Policy

Server Audit Policy

ner

Internet Usage Policy

Data Breach Response Policy

Acceptable Encryption Policy

Security Response Plan Policy

Remote A
Po

Social Engineering Awareness Policy

Employee Internet Use Monitoring and Filtering Policy

Acquisition Assessment Policy

Automatically Forwarded Email Policy

Server Security Policy

off

End User Encryption Key Protection Plan

Communications Equipment Policy

Bluetooth Baseline Requirements Policy

Workstation Security (For HIPAA) Policy

Technology
Equipment Disp
Policy

Information Logging Standard

Remote Access Mobile Computing

Server Malware Protection Policy

Software Installation Policy

Wireless Communication Policy

sign-off

Mobile Device Encryption Policy

Mobile Employee Endpoint Responsibility Policy

Pandemic Response Planning Policy

Password Construction Guidelines

Pers
Commu
Devices an

Lab Security Policy

DMZ Lab Security Policy

Email Retention Policy

Email Policy

Server Audit Policy

ner

Internet Usage Policy

Data Breach Response Policy

Acceptable Encryption Policy

Security Response Plan Policy

Remote A
Po

Social Engineering Awareness Policy

Employee Internet Use Monitoring and Filtering Policy

Acquisition Assessment Policy

Automatically Forwarded Email Policy

Server Security Policy

off

End User Encryption Key Protection Plan

Communications Equipment Policy

Bluetooth Baseline Requirements Policy

Workstation Security (For HIPAA) Policy

Technolog
Equipment Disp
Policy

Information Logging Standard

Remote Access Mobile Computing

Server Malware Protection Policy

Software Installation Policy

Wireless Communication Policy

sign-off

Mobile Device Encryption Policy

Mobile Employee Endpoint Responsibility Policy

Pandemic Response Planning Policy

Password Construction Guidelines

Pers
Commu
Devices an

Lab Security Policy

DMZ Lab Security Policy

Email Retention Policy

Email Policy

Server Audit Policy

ner

Internet Usage Policy

Data Breach Response Policy

Acceptable Encryption Policy

Security Response Plan Policy

Remote A
Po

Social Engineering Awareness Policy

Employee Internet Use Monitoring and Filtering Policy

Acquisition Assessment Policy

Automatically Forwarded Email Policy

Server Security Policy

off

End User Encryption Key Protection Plan

Communications Equipment Policy

Bluetooth Baseline Requirements Policy

Workstation Security (For HIPAA) Policy

Technology
Equipment Disp
Policy

Information Logging Standard

Remote Access Mobile Computing

Server Malware Protection Policy

Software Installation Policy

Wireless Communication Policy

sign-off

Mobile Device Encryption Policy

Mobile Employee Endpoint Responsibility Policy

Pandemic Response Planning Policy

Password Construction Guidelines

Pers
Commu
Devices an

Lab Security Policy

DMZ Lab Security Policy

Email Retention Policy

Email Policy

Server Audit Policy

ner

Internet Usage Policy

Data Breach Response Policy

Acceptable Encryption Policy

Security Response Plan Policy

Remote A
Po

Social Engineering Awareness Policy

Employee Internet Use Monitoring and Filtering Policy

Acquisition Assessment Policy

Automatically Forwarded Email Policy

Server Security Policy

off

End User Encryption Key Protection Plan

Communications Equipment Policy

Bluetooth Baseline Requirements Policy

Workstation Security (For HIPAA) Policy

Technology
Equipment Disp
Policy

Information Logging Standard

Remote Access Mobile Computing

Server Malware Protection Policy

Software Installation Policy

Wireless Communication Policy

sign-off

Mobile Device Encryption Policy

Mobile Employee Endpoint Responsibility Policy

Pandemic Response Planning Policy

Password Construction Guidelines

Pers
Commu
Devices an

Lab Security Policy

DMZ Lab Security Policy

Email Retention Policy

Email Policy

Server Audit Policy

ner

Internet Usage Policy

Data Breach Response Policy

Acceptable Encryption Policy

Security Response Plan Policy

Remote A
Po

Social Engineering Awareness Policy

Employee Internet Use Monitoring and Filtering Policy

Acquisition Assessment Policy

Automatically Forwarded Email Policy

Server Security Policy

off

End User Encryption Key Protection Plan

Communications Equipment Policy

Bluetooth Baseline Requirements Policy

Workstation Security (For HIPAA) Policy

Technology
Equipment Disp
Policy

Information Logging Standard

Remote Access Mobile Computing

Server Malware Protection Policy

Software Installation Policy

Wireless Communication Policy

Communication

Communication

- Policies are crucial to communication within the organisation, they **should be easily accessible.**
    - Policies should be easily accessible by employees, may want to consider physical copies.
- Management **top-down** communication focuses on cyber security direction and objectives to key-decision makers.
    - Communication of the cyber security objectives as well as the assets to the enterprise.

Standards

Standards

- In the context of policies, standards (and procedures) effectively support employees in **attaining the objectives and directives of the policy**.
- Standards are the “how” to the policy “what”, standards are technology-specific without the actual explicit instructions.
- For example, consider policy may have directives that are required authorised access to assets. Standards may outline detail around the password, such as storage requirements as well as rules around reuse or replacement.

Procedures

Procedures

- Procedures are specific instructions to achieve the expectations of standards at an implementation level.
- Procedures are not like in policies, in terms of what the organisation is trying to attain, procedures are instructions to attain standards.
- Standards are concrete specifics around attempt to meet the expectations of policy.
- Continuing the example of authorised access to assets at the policy-level, standards would outline password storage requirements, while procedures would outline specific implementation instructions. For example: passwords must be stored as cryptographic hash, SHA256 and above is acceptable … so on

Policy Verification and Validation

Policy verification and validation

- **Metrics** can be used to determine whether or not security objectives are being met.
- Security solutions can be put in place to tackle know threats. **Verification metrics** confirm that solutions are meeting known requirements.
- Evidence needs to be presented to **validate** that security objectives are being met. Need more than just the latest known attacks are being defended against.

Problem with Policies

Problem with policies

- Many policies could lead to confusion, lack of clarity and may end up causing more harm than good.
- Policies may curb autonomy that could result in disgruntled employees that may result in an increase of insider threat.
- Policies may curb and impact on business objectives, that could interfere with the success of the system.
- Focus of policies is often on risk rather than how people make decisions and what motivates them.

Policy