A security policy criteria decision tree example

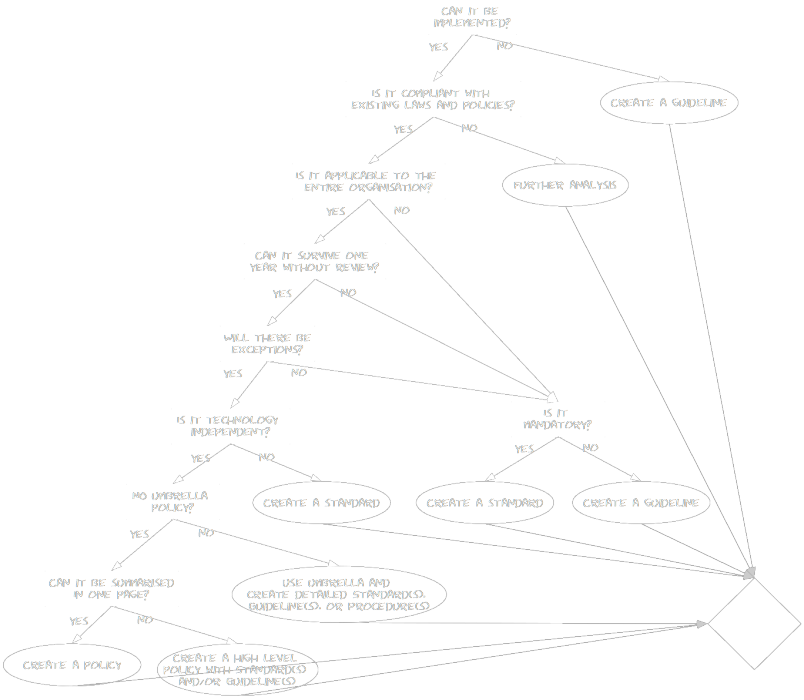
Possible questions

For an example tree supporting policy-making decisions, suppose the following questions:

Is there a compelling need for this guidance and, if yes, what type of guidance (policy, standard, guideline) needs to be created?

1. What are the consequences/risks of not having documented guidance covering this security topic?
    - Is there is a legal requirement to have it documented?
    - Are there operational issues that require direction?
    - Is there new technology that requires organisation-wide guidance?
    - Will documenting (and implementing) this guidance mitigate risks?
2. What are the consequences/risks of having documented guidance covering this security topic?
    - Can it be implemented?
    - Does it represent a strategy we want to plan for?
    - Does a policy already exist?
    - Does a new policy contradict existing policies or other laws and/or regulations?
3. Will the documented guidance use “must” and “should” (is it to be mandatory)? Does it require technology? *If it is mandatory, implementable, applicable across the organisation, and technology-independent, state it as a policy. If it is mandatory, implementable, and applicable, but specific to a particular technology, state it as a standard.*
    - Is there a law requiring the organisation to follow this?
    - Is there a contractual obligation to do so?
    - Is there another reason to make it mandatory?
    - Is this guideline likely to change when new technology becomes available? What part of it is technology dependent, and what part is general policy?
4. Can it be summarized in one page? *More detailed documentation can be provided as standards, guidelines, or procedures.*
5. How often do policies and related standards, guidelines, or procedures need to be reviewed in order to stay current?
6. Are exemptions or exceptions allowed?
7. Is it organisation-wide?
8. Is it IT specific? What other domains are involved and who should be included in its drafting and the decision-making process?

Possible tree



security, test-driven-development, security-improvements, policies