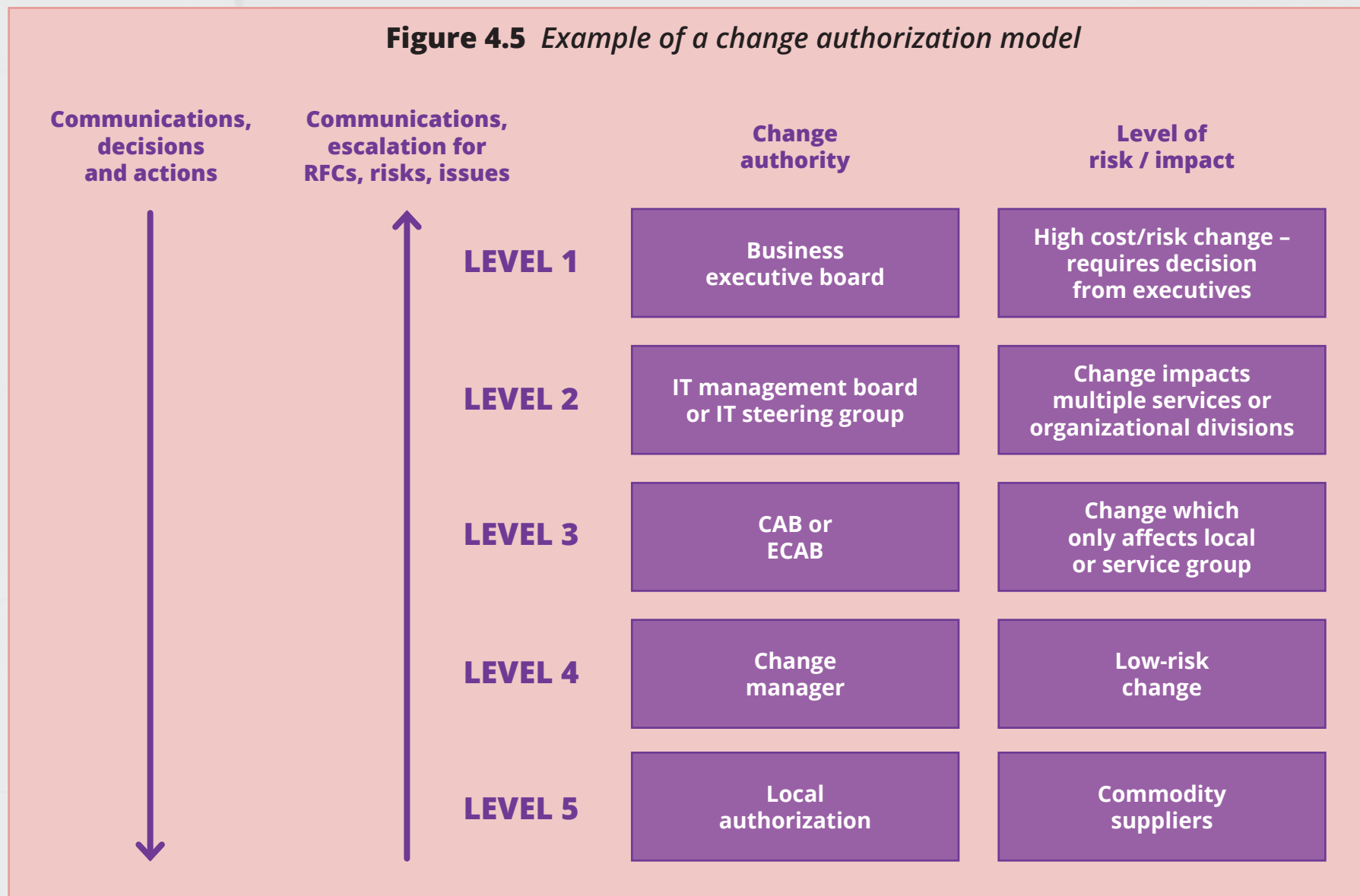# ITIL® Poster Series #45
Change Authorisation Model

Good e-Learning

Introduction

Successful change management replies on effective and efficient process particularly when authorizing a change. In order to fulfil the requirements of authorization for change management, it is necessary to develop a pragmatic approach to authorization that does not become overly bureaucratic or introduce delays to successful change process adoption. If the process of authorization is perceived to be a blocker, then this will encourage people to by-pass the process and implement unauthorized changes, which will most likely be detrimental in the long term. In this presentation, we provide an example of a change authorization model, but this will of course, need to be adapted to suit your individual business needs.

Figure 4.5 *Example of a change authorization model*

	Communications, decisions and actions	Communications, escalation for RFCs, risks, issues	Change authority	Level of risk / impact
LEVEL 1			Business executive board	High cost/risk change – requires decision from executives
LEVEL 2			IT management board or IT steering group	Change impacts multiple services or organizational divisions
LEVEL 3			CAB or ECAB	Change which only affects local or service group
LEVEL 4			Change manager	Low-risk change
LEVEL 5			Local authorization	Commodity suppliers

Formal authorization is obtained for each change from a change authority that may be a role, person or a group of people. The levels of authorization for a particular type of change should be judged by the type, size, risk and potential business impact of the change, e.g. changes in a large enterprise that affect several distributed sites may need to be authorized by a higher-level change authority such as a global CAB or the board of directors.

The culture of the organization dictates, to a large extent, the manner in which changes are authorized. Hierarchical structures may well impose many levels of change authorization, while flatter structures could allow a more streamlined approach.

A degree of delegated authority may exist within an authorization level, e.g. delegating authority to a change manager according to preset parameters relating to:

- **Anticipated business risk**
- **Financial implications**
- **Scope of the change**
  (e.g. internal effects only, within the finance service, specific outsourced services).

An example of a change authorization hierarchy is shown in Figure 4.5. Each organization should formally document its own change authorization hierarchy, which may be very different to the example shown here. All change authorities should be documented in the CMS.

The level at which change is authorized should rest where accountability for accepting risk and remediation exist.

Should disputes arise over change authorization or rejection, there should be a right of appeal to the higher level. Changes that have been rejected should be formally reviewed and closed.

Does this hierarchic model reflect your own organizational experience? Can you see the benefit of capturing this approach in a formal process document? What skill sets are required to enable this to take place in your organization? Is the culture of your organization able to designate authority to the appropriate management levels to support this approach?