Patch management policy exceptions clause

Annex A Patch exceptions

A.1 Definition. An exception is an approved departure from a window in section 4 of this policy for named assets, for a stated period.

A.2 Who may request. A system owner, group owner or the patch coordinator.

A.3 Grounds. A request is accepted for consideration only on one of these grounds: (a) no patch is available; (b) the only available patch would adversely affect the confidentiality, integrity or availability of the system or its data; (c) the vendor no longer supports the software; (d) the disadvantages of applying the patch outweigh the security benefit and the reasons can be substantiated in writing; (e) a legal or contractual restriction prevents patching in the window.

A.4 The request records:

1. The assets (inventory IDs), their owner and maintenance group.
2. The vulnerability or patch (identifier, vendor advisory, class, original deadline).
3. The ground under A.3 and the evidence for it.
4. The measures applied meanwhile, who operates them and how their working is checked.
5. The requested end date.
6. The plan to remove the exception, with a named owner.
7. The requester and the date.

A.5 Signers. The group owner and the policy owner sign every exception. An exception on a class 1 or class 2 vulnerability also requires [executive sponsor].

A.6 Maximum duration. [90] calendar days. A longer period needs the executive sponsor's signature and a fresh request, not an extension.

A.7 Re-check. The patch coordinator reviews every open exception at least every [30] days to determine whether the window can be met now, and records the result.

A.8 Expiry. An exception ends on its end date. The asset then falls under the standard window; an expired exception is reported as a missed window in the next monthly report.

A.9 Register. The patch coordinator keeps a register of open and closed exceptions with every field in A.4; the register is part of the monthly report.

A.10 Escalation. A window that is going to be missed without an approved exception is escalated to the executive sponsor before it expires.