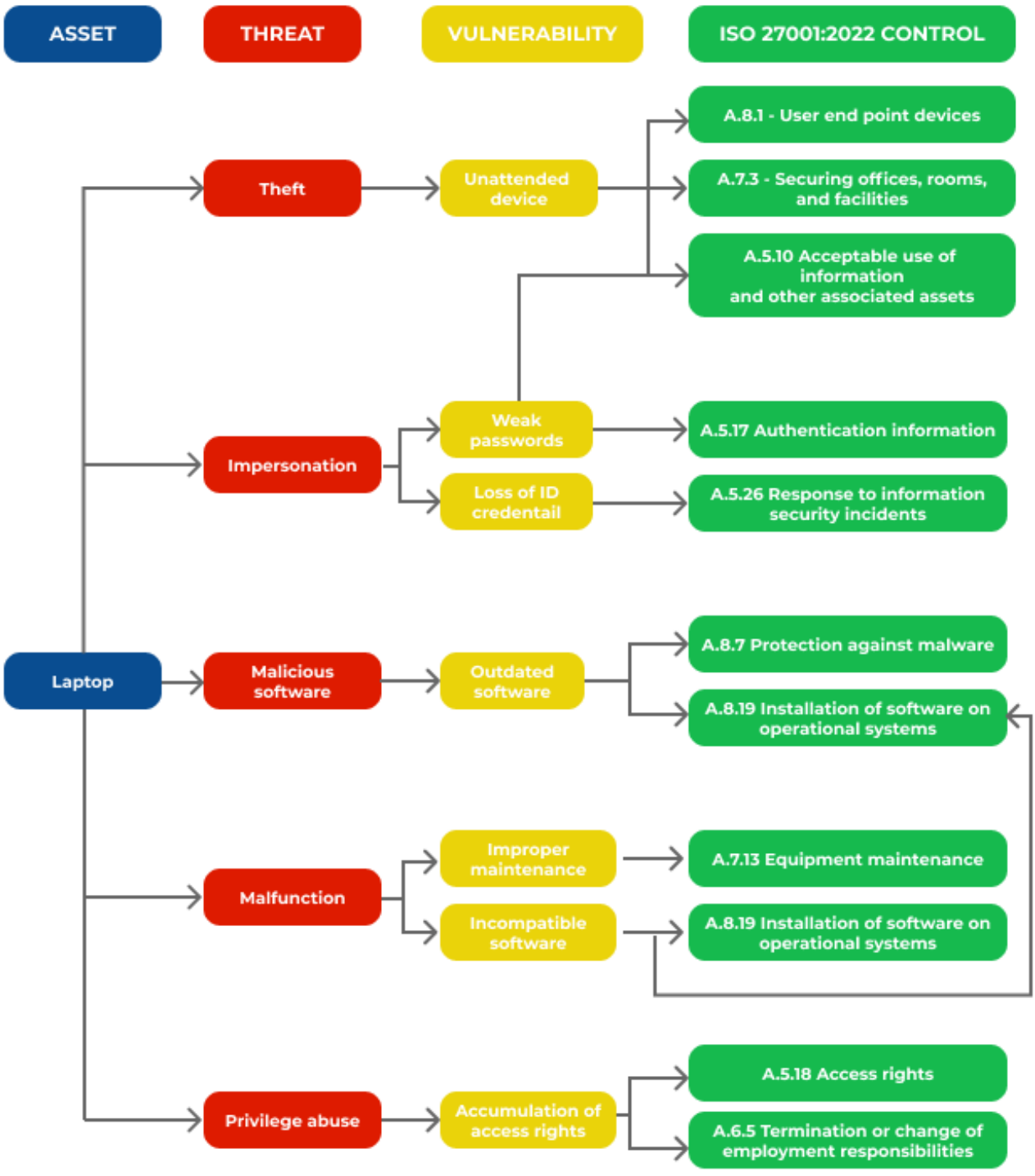
Diagram of the ISO 27001 Risk Assessment and Treatment Process



* These are only examples. The applicability of a control should be supported by the results of risk assessments, legal requirements, or organizational decisions.

Regardless of the applied approach, you should note that:

1 – One threat can exploit multiple vulnerabilities.
2 – One vulnerability can be related to multiple threats (e.g., improper maintenance).
3 – One control can be used to treat multiple risks (e.g., acceptable use of assets and installation of SW on operational systems).

Note: This diagram is based on the Asset-Threat-Vulnerability approach. To see how to use the ISO 27001 risk register with catalogs of assets, threats, and vulnerabilities, and to get automated suggestions on how they are related, sign up for a free trial of Conformio, the leading ISO 27001 compliance software.

Copyright © 2023 Advisera Expert Solutions Ltd.