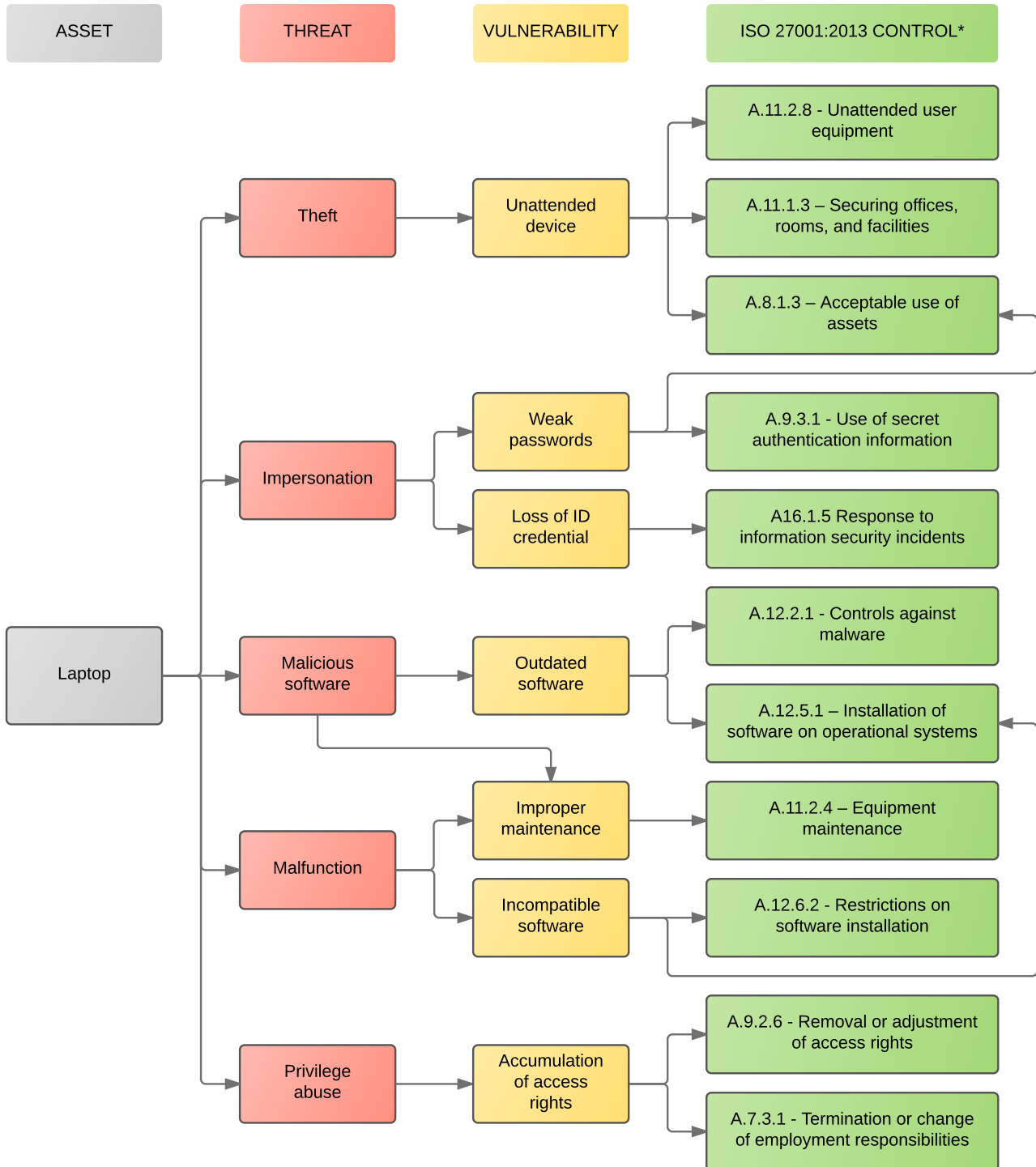# Diagram of ISO 27001 Risk Assessment and Treatment Process

Note: This diagram is based on the Asset-Threath-Vulnerability approach. To learn more about this approach, click here

ASSET	THREAT	VULNERABILITY	ISO 27001:2013 CONTROL*
Laptop	Theft	Unattended device	A.11.2.8 - Unattended user equipment
			A.11.1.3 – Securing offices, rooms, and facilities
			A.8.1.3 – Acceptable use of assets
	Impersonation	Weak passwords	A.9.3.1 - Use of secret authentication information
		Loss of ID credential	A16.1.5 Response to information security incidents
	Malicious software	Outdated software	A.12.2.1 - Controls against malware
			A.12.5.1 – Installation of software on operational systems
	Malfunction	Improper maintenance	A.11.2.4 – Equipment maintenance
		Incompatible software	A.12.6.2 - Restrictions on software installation
	Privilege abuse	Accumulation of access rights	A.9.2.6 - Removal or adjustment of access rights
			A.7.3.1 - Termination or change of employment responsibilities

* 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).