ISO/IEC 27001:2013 Information security management systems
-Control of operational software-

RiG
CERT

Security category – 12.5. Control of operational software

Control – 12.5.1. Installation of software on operational systems
The organization should have procedures for the installation of software on operational systems.

Systems can be affected by the installation of unauthorized software and by unauthorized changes to software.

Procedures should be implemented to control the installation of software on operational systems.

ISO/IEC 27001:2013 Information security management systems
-Control of operational software-

Guidelines for the installation of software, according to ISO/IEC 27002:

a) updating of the operational software, applications and program libraries should only be performed by trained personnel and with authorization;
b) operational systems should only hold approved executable code and not development code or compilers;
c) applications and operating system software should be implemented only after successful testing;
d) there has to be a strategy for situations where changes to software go wrong;
e) previous versions of application software should be retained as for contingency purposes;
f) old versions of software should be archived.

Physical or logical access to suppliers for software support should only be given for specific activities, under approval from management and be it should be monitored.