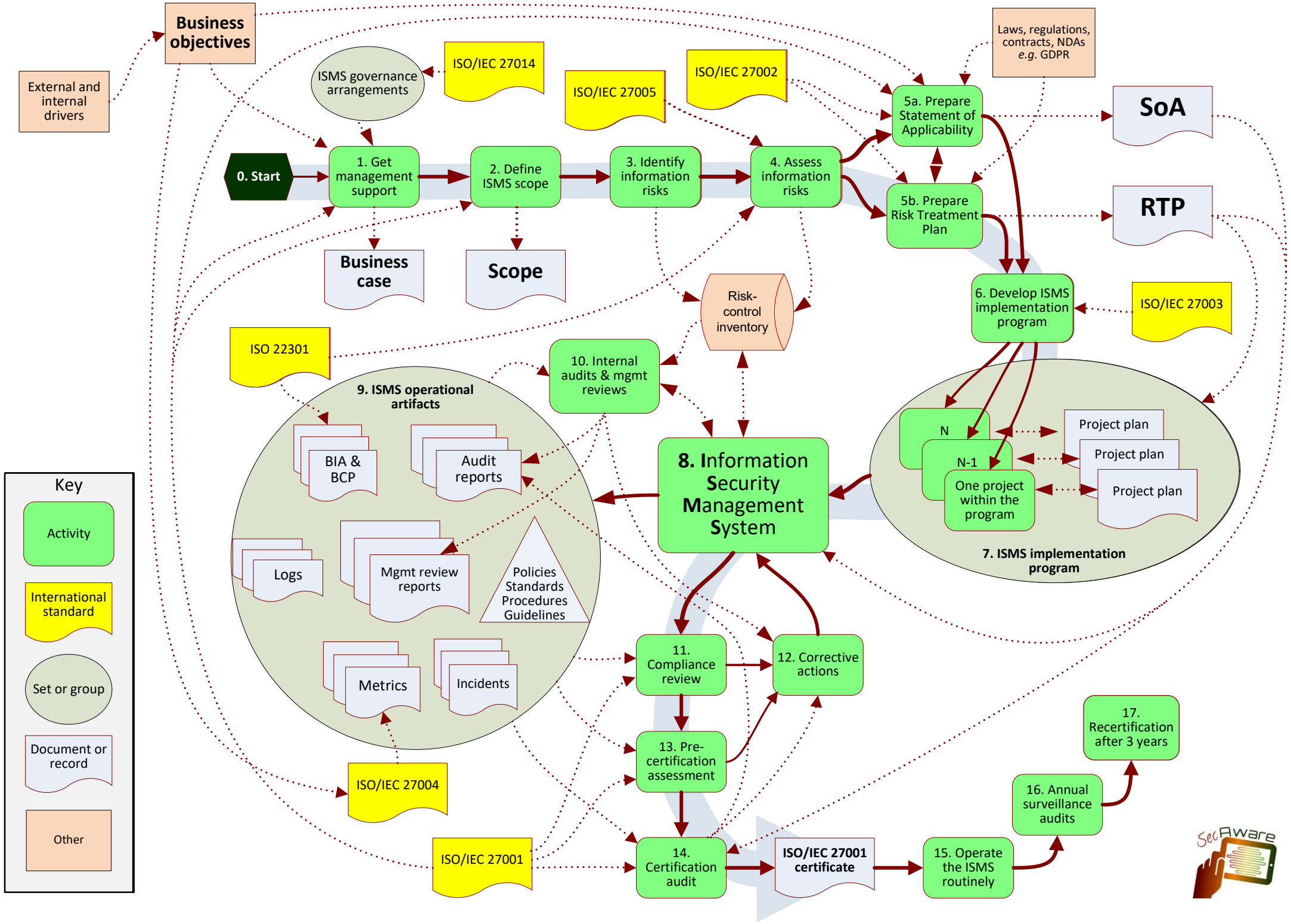
Business objectives
External and internal drivers
ISMS governance arrangements
ISO/IEC 27014
ISO/IEC 27005
ISO/IEC 27002
Laws, regulations, contracts, NDAs e.g. GDPR
5a. Prepare Statement of Applicability
SoA
0. Start
1. Get management support
2. Define ISMS scope
3. Identify information risks
4. Assess information risks
5b. Prepare Risk Treatment Plan
RTP
Business case
Scope
Risk-control inventory
6. Develop ISMS implementation program
ISO/IEC 27003
ISO 22301
10. Internal audits & mgmt reviews
9. ISMS operational artifacts
BIA & BCP
Audit reports
Logs
Mgmt review reports
Policies Standards Procedures Guidelines
Metrics
Incidents
8. Information Security Management System
N
N-1
One project within the program
Project plan
Project plan
Project plan
7. ISMS implementation program
11. Compliance review
12. Corrective actions
13. Pre-certification assessment
14. Certification audit
ISO/IEC 27001 certificate
15. Operate the ISMS routinely
16. Annual surveillance audits
17. Recertification after 3 years
ISO/IEC 27004
ISO/IEC 27001
Key
Activity
International standard
Set or group
Document or record
Other
SecAware