Standard Based Cyber Security Management

Build your Cyber Security based on reputable industry standards (ISO 27001/NIST/HITRUST)

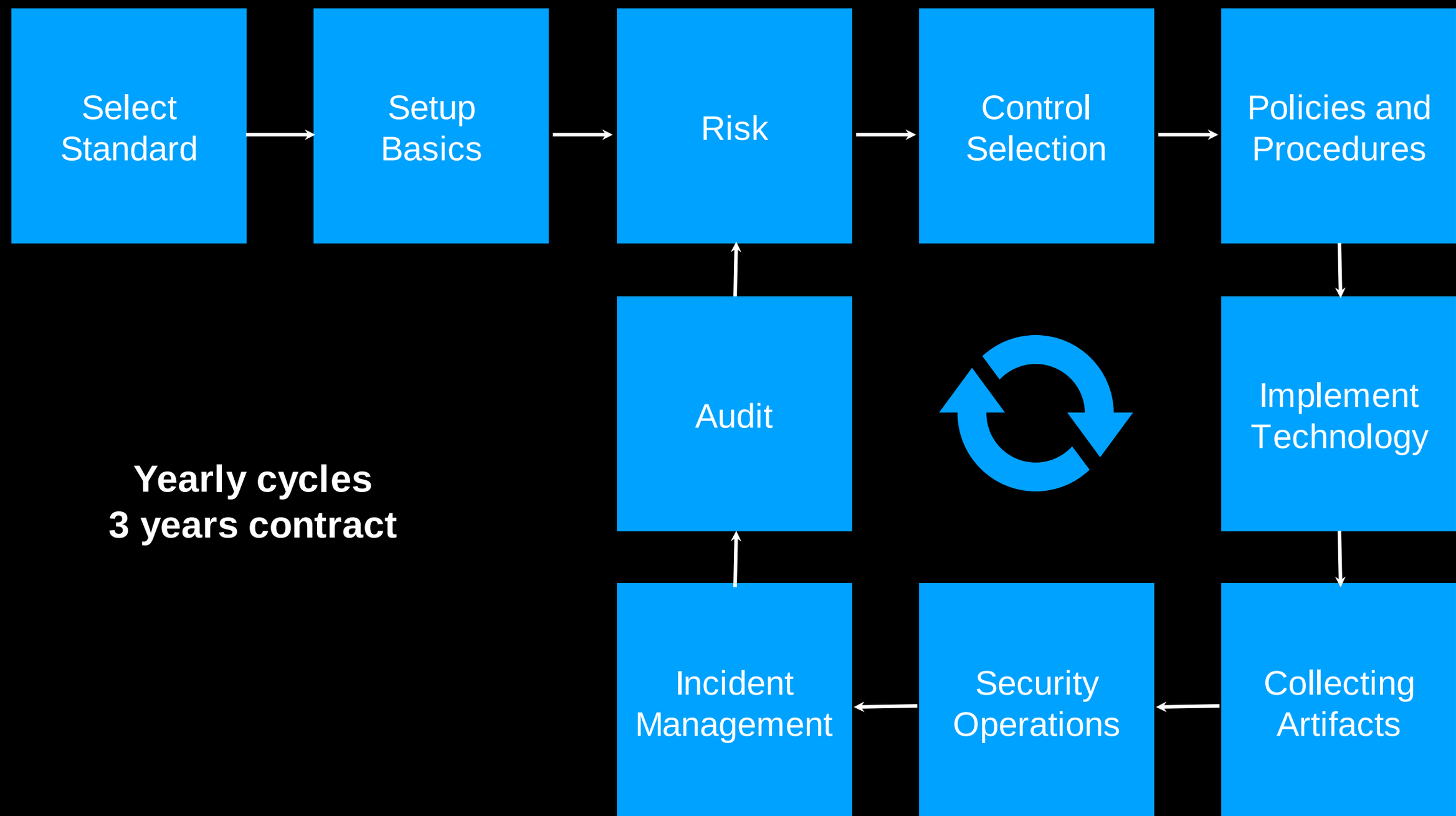
Standard Based Cyber Security Management

There is only one way to be sure that your cyber security is done right is to follow a standard.

ISO 27001 is the international standard that describes best practice for an information security management system (ISMS) and is the only internationally-accepted, universal standard for information security governance.

Digital Edge is a cybersecurity provider implementing Information Security practices, processes, procedures and technology based on internationally accepted standards

Standard Based Cyber Security Management



Yearly cycles
3 years contract

Step 1: SELECT A STANDARD

- NIST
- ISO
- PCI
- SOC 2
- Need privacy compliance?

Step 2: SETUP BASICS

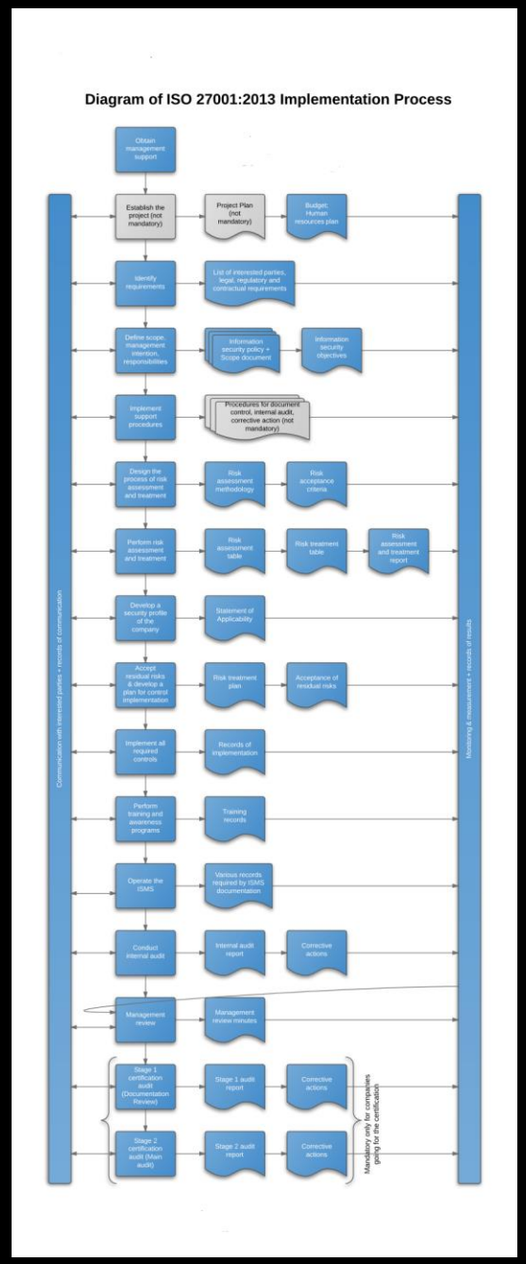
- Governance
- Information and system classification
- Required laws and compliance
- Scope

Step 3: RISK

- Identification
- Classification
- Management
- Policies and procedures

Step 4: CONTROL SELECTION

- Select applicable controls from the standard
- Review sufficiency
- Applicability statement



Step 5: POLICIES & PROCEDURES

- Documentation
- Awareness
- Management approval

Step 6: IMPLEMENT TECHNOLOGY

- Review controls and required artifacts
- Additional implementations and compensations
- Monitoring and review

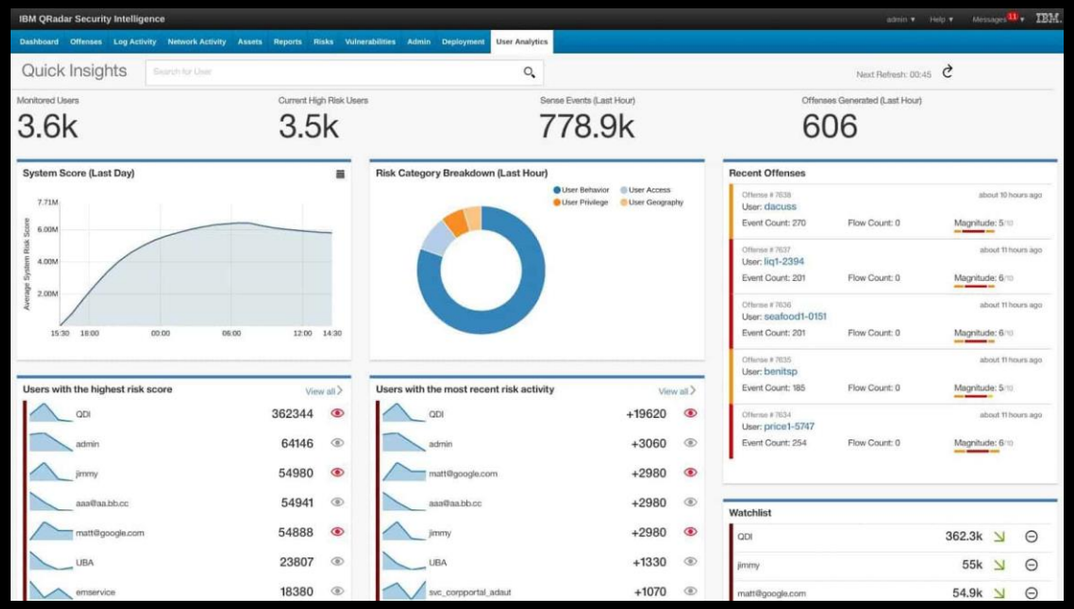
Step 7: COLLECT ARTIFACTS

- Review controls and required artifacts
- Additional implementations and compensations
- Monitoring and review

```
bash-3.2# pwd
/var/db/diagnostics
bash-3.2# ls -l
total 192584
drwxr-xr-x   2 root  wheel       68 Sep 27 19:03 Events
drwxr-xr-x  31 root  wheel     1054 Nov 13 19:44 FaultsAndErrors
drwxr-xr-x   2 root  wheel       68 Sep 27 19:03 Oversize
drwxr-xr-x   2 root  wheel       68 Sep 27 19:03 SpecialHandling
drwxr-xr-x   2 root  wheel       68 Sep 27 19:03 StateDumps
drwxr-xr-x  16 root  wheel      544 Nov 13 19:44 TTL
-rw-r-----   1 root  wheel  10586976 Nov  6 06:08 logdata.Persistent.20161106T045449.tracev3
-rw-r-----   1 root  wheel  10549904 Nov  6 17:03 logdata.Persistent.20161106T112151.tracev3
-rw-r-----   1 root  wheel   2331488 Nov  6 19:17 logdata.Persistent.20161106T221230.tracev3
-rw-r-----   1 root  wheel   6667976 Nov  7 19:18 logdata.Persistent.20161107T002825.tracev3
-rw-r-----   1 root  wheel   3605360 Nov  7 21:56 logdata.Persistent.20161108T003223.tracev3
-rw-r-----   1 root  wheel  10506760 Nov  9 23:11 logdata.Persistent.20161109T001242.tracev3
-rw-r-----   1 root  wheel   3068952 Nov 10 20:57 logdata.Persistent.20161110T051134.tracev3
-rw-r-----   1 root  wheel  10587272 Nov 11 17:55 logdata.Persistent.20161111T023347.tracev3
-rw-r-----   1 root  wheel   3177928 Nov 11 20:21 logdata.Persistent.20161111T230548.tracev3
-rw-r-----   1 root  wheel  10573896 Nov 12 12:10 logdata.Persistent.20161112T012527.tracev3
-rw-r-----   1 root  wheel   5564952 Nov 12 19:32 logdata.Persistent.20161112T185153.tracev3
-rw-r-----   1 root  wheel  10602712 Nov 13 11:58 logdata.Persistent.20161113T003205.tracev3
-rw-r-----   1 root  wheel   9023072 Nov 13 19:37 logdata.Persistent.20161113T170327.tracev3
-rw-r-----   1 root  wheel    520040 Nov 13 19:59 logdata.Persistent.20161114T004307.tracev3
-rw-r-----   1 root  wheel   1212268 Nov 13 19:43 logdata.statistics.0.txt
```

Step 8: SECURITY OPERATION

- Security Information and Event Management
- Reviews and SOPs
- Escalations

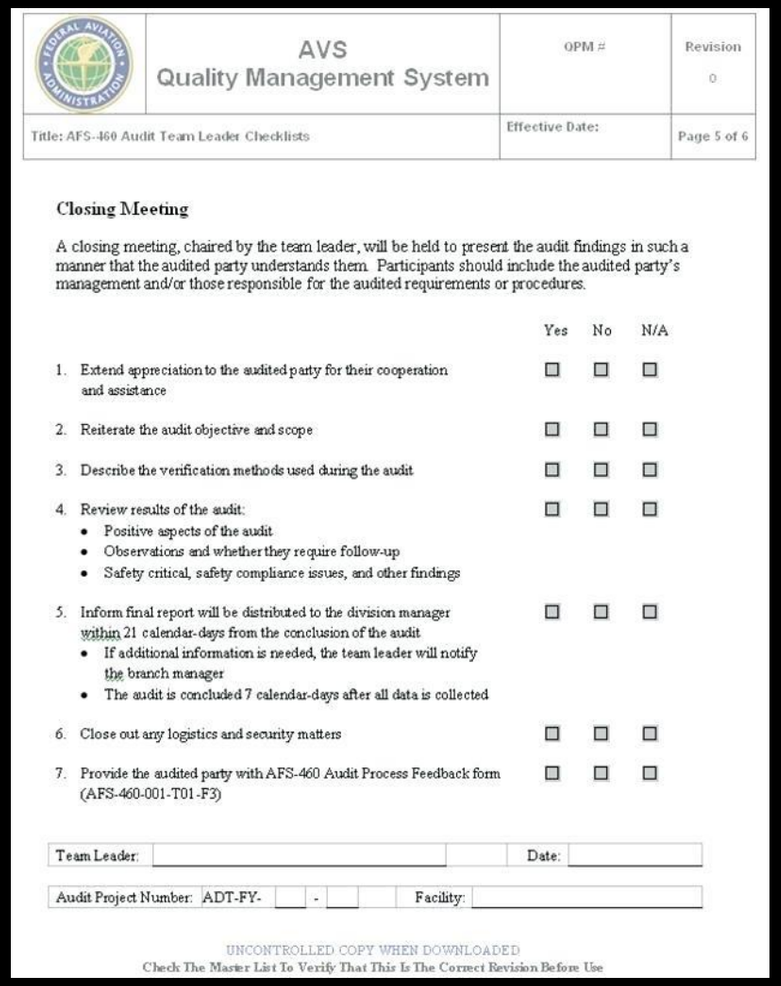


Step 9: INCIDENT MANAGEMENT

- CIRT operations
- Notification
- Documentation
- Risk correlation and measurements

Step 10: AUDIT

- Checkboxes vs self continues Due Diligence process
- Scheduled reviews
- Internal Audits
- Management reviews



AVS Quality Management System	OPM #	Revision 0
Title: AFS-460 Audit Team Leader Checklists	Effective Date:	Page 5 of 6

Closing Meeting

A closing meeting, chaired by the team leader, will be held to present the audit findings in such a manner that the audited party understands them. Participants should include the audited party's management and/or those responsible for the audited requirements or procedures.

	Yes	No	N/A
1. Extend appreciation to the audited party for their cooperation and assistance	☐	☐	☐
2. Reiterate the audit objective and scope	☐	☐	☐
3. Describe the verification methods used during the audit	☐	☐	☐
4. Review results of the audit: • Positive aspects of the audit • Observations and whether they require follow-up • Safety critical, safety compliance issues, and other findings	☐	☐	☐
5. Inform final report will be distributed to the division manager within 21 calendar-days from the conclusion of the audit • If additional information is needed, the team leader will notify the branch manager • The audit is concluded 7 calendar-days after all data is collected	☐	☐	☐
6. Close out any logistics and security matters	☐	☐	☐
7. Provide the audited party with AFS-460 Audit Process Feedback form (AFS-460-001-T01-F3)	☐	☐	☐

Team Leader: _____ Date: _____

Audit Project Number: ADT-FY- ___ - ___ Facility: _____

UNCONTROLLED COPY WHEN DOWNLOADED
Check The Master List To Verify That This Is The Correct Revision Before Use