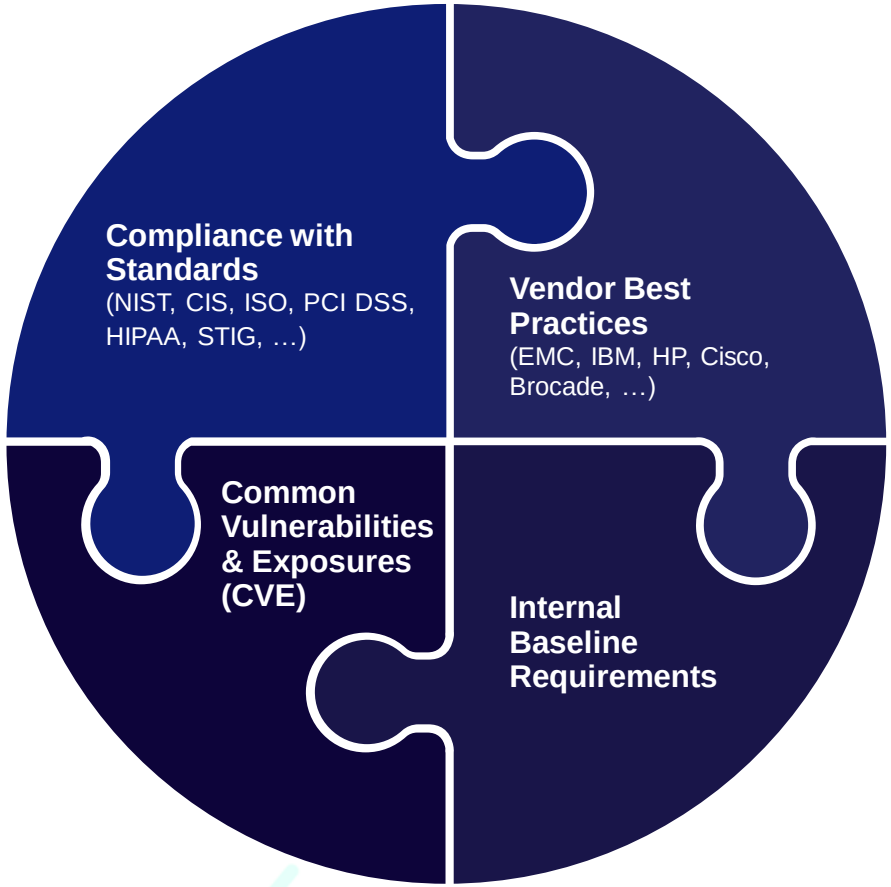
# THE RISK KNOWLEDGEBASE SOURCES




**Four main sources, including:**

- Automatic checks based on standard, interpreted for each device type
- Automatic checks for comprehensive and ongoingly updated vendor best practices
- Automatic checks for storage system vulnerabilities
- Automatic checks for community-driven security baseline configurations

# THE RISK KNOWLEDGEBASE CATEGORIES

### Authentication

- AD / LDAP, Vaulting, Radius
- Kerberos, MFA
- Login & passwd requirements

### Authorization

- Role configuration
- Restricted Admin access
- Default accounts / passwords

### SAN / NAS

- Zoning and masking
- CIFS and NFS access
- Port config

### Vendor best practices

- Dell EMC, IBM, HP, Hitachi
- Cisco, Brocade, NetApp
- Infinidat, Amazon, more.

### Administrative access

- Management systems / Apps
- CLI /API/SMI-S servers
- Automatic logoff, sessions

### Encryption

- At rest / In transit
- Encryption level, FIPS, Hashes
- Admin / User access, SSL/TLS

### Vulnerabilities

- Storage CVE detection
- Approved versions

### Leading standards

- ISO 27001, NIST, CIS SANS
- NYDFS, SEC, FFIEC, HIPAA
- FIPS, PCI DSS and more.

### Audit log

- Central Logging
- Log Retention
- Log Config and Immutability

### Services / Protocols

- Telnet, FTP, RSH, SSH, Rlogin
- NFS, CIFS (SMB)
- SNMP, NDMP, SMTP

### Ransomware protection

- Vendor / industry best practices
- Protection policies

### And more…

- Antivirus settings
- Time synchronization
- And more…

### COVERAGE

- Block Storage Arrays
- Storage Network Switches
- Storage Management Applications / Servers
- Storage Virtualization Systems
- Data Protection Appliances
- Object Storage
- Storage Area Network (SAN)
- Server-based SAN (Virtual SAN)
- Network Attached Storage (NAS)
- Backup Systems
- Cloud storage*
- Converged / Blade / Hypervisor*