KafkaGuard

TEAM EDITION

Kafka Security & Compliance Assessment Report

88.4%

COMPLIANCE SCORE

NEEDS ATTENTION

CLUSTER

unknown-cluster-id

KAFKA CLUSTER

2 brokers

1 topics

CONTROLS

55

POLICY

finance-iso

v1.0

FINDINGS

48 / 55

PASS RATE

48 passed

7 failed

Scan Date:	April 27, 2026 at 7:37 PM
Policy:	finance-iso v1.0
KafkaGuard:	dev

KafkaGuard Compliance Report

Cluster Information

Cluster Name:	unknown-cluster-id
Brokers:	2
Topics:	1
ZK Nodes:	3
Scan Date:	April 27, 2026 at 7:37 PM

Policy Information

Policy:	finance-iso v1.0
Total Controls:	55

Compliance Score

88.4%

Summary Statistics

Controls	Total	Passed	Failed	N/A
Scan Result	**55**	**48**	**7**	**0**

Findings by Severity

Compliance Summary Dashboard

Pass rates per compliance framework based on mapped controls in this scan.

PCI-DSS 4.0 — 77%

26 controls mapped — 20 passed — 6 failed

SOC 2 Type II — 86%

51 controls mapped — 44 passed — 7 failed

ISO 27001 — 87%

53 controls mapped — 46 passed — 7 failed

Things to Address Before Your Audit

KG-022	[HIGH]	ZK quorum healthy (>=3 nodes)
KG-008	[MEDIUM]	ZooKeeper authentication enabled
KG-009	[MEDIUM]	ZooKeeper ACLs enabled
KG-013	[MEDIUM]	SSL endpoint identification enabled
KG-015	[MEDIUM]	Monitoring endpoint security
KG-042	[MEDIUM]	Log retention >=90 days
KG-040	[LOW]	GC logging enabled

Controls Evaluation Results

PASS = green FAIL = red bold Sorted by Control ID

Control ID	Title	Status	Severity	Category
KG-001	SASL authentication enabled	PASS	HIGH	security
KG-002	SSL/TLS encryption enabled	PASS	HIGH	security
KG-003	ACL authorization enabled	PASS	HIGH	security
KG-005	TLS certificate expiry >30 days	PASS	HIGH	security
KG-006	TLS protocol >=1.2	PASS	HIGH	security
KG-007	Inter-broker encryption enabled	PASS	HIGH	security
KG-010	No default passwords	PASS	CRITICAL	security
KG-011	SASL mechanism secure	PASS	HIGH	security
KG-012	Client authentication required	PASS	HIGH	security
KG-014	Security protocol valid	PASS	HIGH	security
KG-016	Replication factor >=3	PASS	HIGH	reliability
KG-017	Min ISR >=2	PASS	HIGH	reliability
KG-018	No under-replicated partitions	PASS	HIGH	reliability
KG-019	No offline partitions	PASS	CRITICAL	reliability
KG-022	**ZK quorum healthy (>=3 nodes)**	FAIL	HIGH	reliability
KG-024	Disk usage <90%	PASS	HIGH	reliability
KG-025	Heap usage <85%	PASS	HIGH	reliability
KG-029	Log directories not in /tmp	PASS	HIGH	operational
KG-041	Audit logging enabled	PASS	HIGH	security
KG-043	Encryption at rest configured	PASS	HIGH	security
KG-044	Broker-to-broker mutual TLS	PASS	HIGH	security
KG-045	No deprecated TLS protocols	PASS	HIGH	security
KG-046	Strong cipher suites only	PASS	HIGH	security
KG-048	Admin access restricted	PASS	HIGH	security
KG-053	All KRaft controller voters healthy	PASS	HIGH	reliability
KG-054	Metadata log replication not lagging	PASS	HIGH	reliability
KG-056	KRaft authorizer compatible with controller listener	PASS	HIGH	security
KG-004	No wildcard ACLs	PASS	MEDIUM	security
KG-008	**ZooKeeper authentication enabled**	FAIL	MEDIUM	security
KG-009	**ZooKeeper ACLs enabled**	FAIL	MEDIUM	security
KG-013	**SSL endpoint identification enabled**	FAIL	MEDIUM	security
KG-015	**Monitoring endpoint security**	FAIL	MEDIUM	security
KG-020	Unclean leader election disabled	PASS	MEDIUM	reliability
KG-021	Log retention configured	PASS	MEDIUM	reliability
KG-023	Broker version consistent	PASS	MEDIUM	reliability

KG-027	Leader election timeout configured	PASS	MEDIUM	reliability
KG-028	Auto-create topics disabled	PASS	MEDIUM	operational
KG-030	Delete topic disabled	PASS	MEDIUM	operational
KG-033	Log retention hours configured	PASS	MEDIUM	operational
KG-042	Log retention >=90 days	FAIL	MEDIUM	security
KG-047	ACL deny rules configured	PASS	MEDIUM	security
KG-049	Data retention policies enforced	PASS	MEDIUM	security
KG-052	KRaft controller quorum size >= 3	PASS	MEDIUM	reliability
KG-026	Network threads configured	PASS	LOW	reliability
KG-031	Compression configured	PASS	LOW	operational
KG-032	Log segment bytes appropriate	PASS	LOW	operational
KG-034	Network threads appropriate	PASS	LOW	operational
KG-035	IO threads appropriate	PASS	LOW	operational
KG-036	Send buffer bytes configured	PASS	LOW	operational
KG-037	Receive buffer bytes configured	PASS	LOW	operational
KG-038	Replica fetch max bytes configured	PASS	LOW	operational
KG-039	Message max bytes configured	PASS	LOW	operational
KG-040	GC logging enabled	FAIL	LOW	operational
KG-050	Compliance metadata configured	PASS	LOW	security
KG-055	Confluent version matches Kafka version	PASS	LOW	reliability

Detailed Findings

KG-022: ZK quorum healthy (>=3 nodes)

Status: FAIL

Severity: HIGH

Category: reliability

Description:

ZooKeeper cluster must have at least 3 nodes and healthy quorum

Remediation Steps:

```
Add ZooKeeper nodes to reach quorum of 3 or more
```

Evidence:


```
{ "acl_count": 4, "actual_values": [ "brokers: 2", "topics: 5", "acls: 4" ],
"broker_count": 2, "control_id": "KG-022", "expected_value": "See control description
for expected configuration", "expression": "cluster_mode == \"kraft\" ||
(zookeeper.quorum_size \u003e= 3 \u0026\u0026 zookeeper.quorum_healthy)",
"failure_reason": "Control KG-022 failed: Control failed", "iso27001_controls": [
"A.12.3.1", "A.17.1.1", "A.17.2.1" ], "result": false, "s...
```


KG-008: ZooKeeper authentication enabled

Status: FAIL

Severity: MEDIUM

Category: security

Description:

ZooKeeper authentication must be enabled

Remediation Steps:

```
Enable ZooKeeper authentication
```

Evidence:


```
{ "acl_count": 4, "actual_values": [ "brokers: 2", "topics: 5", "acls: 4" ],
"broker_count": 2, "control_id": "KG-008", "expected_value": "See control description
for expected configuration", "expression": "cluster_mode == \"kraft\" ||
zookeeper.auth_enabled == true", "failure_reason": "Control KG-008 failed: Control
failed", "iso27001_controls": [ "A.9.2.1", "A.9.2.2" ], "pci_dss_controls": [ "8.1"
], "result": false, "soc2_controls": [ ...
```

KG-009: ZooKeeper ACLs enabled

Status: FAIL

Severity: MEDIUM

Category: security

Description:

ZooKeeper ACLs must be enabled

Remediation Steps:

```
Enable ZooKeeper ACLs
```

Evidence:


```
{ "acl_count": 4, "actual_values": [ "brokers: 2", "topics: 5", "acls: 4" ],
"broker_count": 2, "control_id": "KG-009", "expected_value": "See control description
for expected configuration", "expression": "cluster_mode == \"kraft\" ||
zookeeper.acl_enabled == true", "failure_reason": "Control KG-009 failed: Control
failed", "iso27001_controls": [ "A.9.1.1", "A.9.2.5" ], "pci_dss_controls": [ "7.1"
], "result": false, "soc2_controls": [ ...
```


KG-013: SSL endpoint identification enabled

Status: FAIL

Severity: MEDIUM

Category: security

Description:

SSL endpoint identification must be enabled

Remediation Steps:

```
Enable SSL endpoint identification
```

Evidence:


```
{ "acl_count": 4, "actual_values": [ "brokers: 2", "topics: 5", "acls: 4" ],
"broker_count": 2, "control_id": "KG-013", "expected_value": "See control description
for expected configuration", "expression": "brokers.all(b, !b.ssl_enabled ||
b.configs['ssl.endpoint.identification.algorithm'] != '')", "failure_reason":
"Control KG-013 failed: Control failed", "iso27001_controls": [ "A.10.1.1",
"A.13.1.1" ], "pci_dss_controls": [ "4.1" ], "result"...
```

KG-015: Monitoring endpoint security

Status: FAIL

Severity: MEDIUM

Category: security

Description:

JMX or metrics endpoints must be properly secured (Prometheus, JMX, Jolokia)

Remediation Steps:

```
For Prometheus JMX Exporter: Bind to localhost (127.0.0.1:PORT) or add authentication
via reverse proxy For Traditional JMX: Enable authentication and SSL For Jolokia:
Enable authentication Example fix (Prometheus):
Environment="KAFKA_OPTS=-javaagent:/opt/jmx_exporter/jmx_prometheus_javaagent.jar=127.0.0.1:9999:/opt/
```

Evidence:


```
{ "acl_count": 4, "actual_values": [ "brokers: 2", "topics: 5", "acls: 4" ],
"broker_count": 2, "control_id": "KG-015", "expected_value": "See control description
for expected configuration", "expression": "monitoring.size() \u003e 0 \u0026\u0026
monitoring.all(m, m.type != 'none' \u0026\u0026 ((m.type == 'prometheus_exporter'
\u0026\u0026 (m.bind_address == '127.0.0.1' || m.bind_address == 'localhost' ||
m.requires_auth == true)) || (m.type == 'traditional_jmx' \u00...
```


KG-042: Log retention >=90 days

Status: FAIL

Severity: MEDIUM

Category: security

Description:

Brokers must retain logs for at least 90 days for compliance audit trails

Remediation Steps:

```
Set log.retention.hours=2160 (90 days) or higher in server.properties
```

Evidence:


```
{ "acl_count": 4, "actual_values": [ "brokers: 2", "topics: 5", "acls: 4" ],
"broker_count": 2, "control_id": "KG-042", "expected_value": "See control description
for expected configuration", "expression": "brokers.all(b, b.log_retention_hours
\u003e= 2160)", "failure_reason": "Control KG-042 failed: Control failed",
"iso27001_controls": [ "A.12.4.1" ], "pci_dss_controls": [ "10.7" ], "result": false,
"soc2_controls": [ "CC7.3" ], "topic...
```

KG-040: GC logging enabled

Status: FAIL

Severity: LOW

Category: operational

Description:

Brokers must have GC logging enabled for JVM monitoring

Remediation Steps:

```
Enable GC logging in JVM startup parameters
```

Evidence:


```
{ "acl_count": 4, "actual_values": [ "brokers: 2", "topics: 5", "acls: 4" ],
"broker_count": 2, "control_id": "KG-040", "expected_value": "See control description
for expected configuration", "expression": "brokers.all(b, b.gc_logging_enabled ==
true)", "failure_reason": "Control KG-040 failed: Control failed",
"iso27001_controls": [ "A.12.4.1", "A.12.4.2", "A.12.4.3" ], "pci_dss_controls": [
"10.1" ], "result": false, "soc2_controls": [...
```

PCI-DSS Compliance Mapping

Framework: Payment Card Industry Data Security Standard

Requirement ID	Control ID	Control Title	Status	Severity
8.1, 8.2	KG-001	SASL authentication enabled	PASS	HIGH
4.1	KG-002	SSL/TLS encryption enabled	PASS	HIGH
7.1, 7.2	KG-003	ACL authorization enabled	PASS	HIGH
4.1	KG-005	TLS certificate expiry >30 days	PASS	HIGH
4.1	KG-006	TLS protocol >=1.2	PASS	HIGH
4.1	KG-007	Inter-broker encryption enabled	PASS	HIGH
8.2	KG-010	No default passwords	PASS	CRITICAL
8.2	KG-011	SASL mechanism secure	PASS	HIGH
8.1, 8.2	KG-012	Client authentication required	PASS	HIGH
4.1	KG-014	Security protocol valid	PASS	HIGH
10.1, 10.2	KG-041	Audit logging enabled	PASS	HIGH
3.4, 3.5	KG-043	Encryption at rest configured	PASS	HIGH
4.1	KG-044	Broker-to-broker mutual TLS	PASS	HIGH
4.1	KG-045	No deprecated TLS protocols	PASS	HIGH
4.1	KG-046	Strong cipher suites only	PASS	HIGH
2.2, 10.1	KG-056	KRaft authorizer compatible with controller liste	PASS	HIGH
7.1	KG-004	No wildcard ACLs	PASS	MEDIUM
8.1	KG-008	ZooKeeper authentication enabled	FAIL	MEDIUM
7.1	KG-009	ZooKeeper ACLs enabled	FAIL	MEDIUM
4.1	KG-013	SSL endpoint identification enabled	FAIL	MEDIUM
8.1, 8.2	KG-015	Monitoring endpoint security	FAIL	MEDIUM
2.2	KG-028	Auto-create topics disabled	PASS	MEDIUM
10.7	KG-033	Log retention hours configured	PASS	MEDIUM
10.7	KG-042	Log retention >=90 days	FAIL	MEDIUM
3.1	KG-049	Data retention policies enforced	PASS	MEDIUM
10.1	KG-040	GC logging enabled	FAIL	LOW

SOC 2 Type II Compliance Mapping

Framework: System and Organization Controls 2

Requirement ID	Control ID	Control Title	Status	Severity
CC6.1, CC6.2, CC9.2, CC10.	KG-001	SASL authentication enabled	PASS	HIGH
CC6.5, CC6.6, CC9.1, CC10.	KG-002	SSL/TLS encryption enabled	PASS	HIGH
CC6.1, CC6.2, CC6.3, CC6.4	KG-003	ACL authorization enabled	PASS	HIGH
CC6.5, CC6.6	KG-005	TLS certificate expiry >30 days	PASS	HIGH
CC6.5, CC6.6	KG-006	TLS protocol >=1.2	PASS	HIGH
CC6.5, CC6.6	KG-007	Inter-broker encryption enabled	PASS	HIGH
CC6.2	KG-010	No default passwords	PASS	CRITICAL
CC6.2	KG-011	SASL mechanism secure	PASS	HIGH
CC6.1, CC6.2	KG-012	Client authentication required	PASS	HIGH
CC6.5, CC6.6	KG-014	Security protocol valid	PASS	HIGH
CC7.1	KG-016	Replication factor >=3	PASS	HIGH
CC7.1	KG-017	Min ISR >=2	PASS	HIGH
CC7.1	KG-018	No under-replicated partitions	PASS	HIGH
CC7.1	KG-019	No offline partitions	PASS	CRITICAL
CC7.1	KG-022	ZK quorum healthy (>=3 nodes)	FAIL	HIGH
CC7.1	KG-024	Disk usage <90%	PASS	HIGH
CC7.1	KG-025	Heap usage <85%	PASS	HIGH
CC7.1	KG-029	Log directories not in /tmp	PASS	HIGH
CC7.2, CC7.3	KG-041	Audit logging enabled	PASS	HIGH
CC6.1	KG-043	Encryption at rest configured	PASS	HIGH
CC6.2, CC6.3	KG-048	Admin access restricted	PASS	HIGH
CC7.1	KG-053	All KRaft controller voters healthy	PASS	HIGH
CC7.1	KG-054	Metadata log replication not lagging	PASS	HIGH
CC6.1, CC6.6	KG-056	KRaft authorizer compatible with controller liste	PASS	HIGH
CC6.2, CC6.4	KG-004	No wildcard ACLs	PASS	MEDIUM
CC6.1, CC6.2	KG-008	ZooKeeper authentication enabled	FAIL	MEDIUM
CC6.1, CC6.2, CC6.4	KG-009	ZooKeeper ACLs enabled	FAIL	MEDIUM
CC6.5, CC6.6	KG-013	SSL endpoint identification enabled	FAIL	MEDIUM
CC6.1, CC6.2, CC6.6	KG-015	Monitoring endpoint security	FAIL	MEDIUM
CC8.1	KG-020	Unclean leader election disabled	PASS	MEDIUM
CC7.2	KG-021	Log retention configured	PASS	MEDIUM
CC7.1	KG-023	Broker version consistent	PASS	MEDIUM
CC7.1	KG-027	Leader election timeout configured	PASS	MEDIUM

Requirement ID	Control ID	Control Title	Status	Severity
CC6.6	KG-028	Auto-create topics disabled	PASS	MEDIUM
CC7.1	KG-030	Delete topic disabled	PASS	MEDIUM
CC7.2	KG-033	Log retention hours configured	PASS	MEDIUM
CC7.3	KG-042	Log retention >=90 days	FAIL	MEDIUM
CC6.1	KG-047	ACL deny rules configured	PASS	MEDIUM
CC7.1	KG-052	KRaft controller quorum size >= 3	PASS	MEDIUM
CC7.1	KG-026	Network threads configured	PASS	LOW
CC7.1	KG-031	Compression configured	PASS	LOW
CC7.1	KG-032	Log segment bytes appropriate	PASS	LOW
CC7.1	KG-034	Network threads appropriate	PASS	LOW
CC7.1	KG-035	IO threads appropriate	PASS	LOW
CC7.1	KG-036	Send buffer bytes configured	PASS	LOW
CC7.1	KG-037	Receive buffer bytes configured	PASS	LOW
CC7.1	KG-038	Replica fetch max bytes configured	PASS	LOW
CC7.1	KG-039	Message max bytes configured	PASS	LOW
CC7.2	KG-040	GC logging enabled	FAIL	LOW
CC7.1	KG-050	Compliance metadata configured	PASS	LOW
CC8.1	KG-055	Confluent version matches Kafka versi	PASS	LOW

ISO 27001 Compliance Mapping

Framework: ISO/IEC 27001 Information Security Management

Requirement ID	Control ID	Control Title	Status	Severity
A.9.2.1, A.9.2.2, A.9.2.3, A.9.	KG-001	SASL authentication enabled	PASS	HIGH
A.10.1.1, A.10.1.2, A.13.1.1,	KG-002	SSL/TLS encryption enabled	PASS	HIGH
A.9.1.1, A.9.1.2, A.9.2.5, A.9.	KG-003	ACL authorization enabled	PASS	HIGH
A.10.1.1, A.10.1.2	KG-005	TLS certificate expiry >30 days	PASS	HIGH
A.10.1.1, A.13.1.1	KG-006	TLS protocol >=1.2	PASS	HIGH
A.10.1.1, A.13.1.1	KG-007	Inter-broker encryption enabled	PASS	HIGH
A.9.2.4	KG-010	No default passwords	PASS	CRITICAL
A.9.2.4, A.9.4.2	KG-011	SASL mechanism secure	PASS	HIGH
A.9.2.1, A.9.2.2	KG-012	Client authentication required	PASS	HIGH
A.10.1.1, A.13.1.1	KG-014	Security protocol valid	PASS	HIGH
A.12.3.1, A.12.3.2, A.17.1.1,	KG-016	Replication factor >=3	PASS	HIGH
A.12.3.1, A.17.1.1, A.17.2.1	KG-017	Min ISR >=2	PASS	HIGH
A.12.3.1, A.17.1.1	KG-018	No under-replicated partitions	PASS	HIGH
A.12.3.1, A.17.1.1	KG-019	No offline partitions	PASS	CRITICAL
A.12.3.1, A.17.1.1, A.17.2.1	KG-022	ZK quorum healthy (>=3 nodes)	FAIL	HIGH
A.12.3.1, A.17.1.1	KG-024	Disk usage <90%	PASS	HIGH
A.12.3.1, A.17.1.1	KG-025	Heap usage <85%	PASS	HIGH
A.12.3.1, A.12.4.2	KG-029	Log directories not in /tmp	PASS	HIGH
A.12.4.1, A.12.4.2	KG-041	Audit logging enabled	PASS	HIGH
A.10.1.1, A.10.1.2	KG-043	Encryption at rest configured	PASS	HIGH
A.13.1.1, A.13.1.2	KG-044	Broker-to-broker mutual TLS	PASS	HIGH
A.13.1.1	KG-045	No deprecated TLS protocols	PASS	HIGH
A.10.1.1	KG-046	Strong cipher suites only	PASS	HIGH
A.9.2.3, A.9.4.1	KG-048	Admin access restricted	PASS	HIGH
A.12.3.1, A.17.1.1	KG-053	All KRaft controller voters healthy	PASS	HIGH
A.12.3.1, A.17.1.1	KG-054	Metadata log replication not lagging	PASS	HIGH
A.9.4.1, A.13.1.1	KG-056	KRaft authorizer compatible with controller liste	PASS	HIGH
A.9.1.1, A.9.4.1	KG-004	No wildcard ACLs	PASS	MEDIUM
A.9.2.1, A.9.2.2	KG-008	ZooKeeper authentication enabled	FAIL	MEDIUM
A.9.1.1, A.9.2.5	KG-009	ZooKeeper ACLs enabled	FAIL	MEDIUM
A.10.1.1, A.13.1.1	KG-013	SSL endpoint identification enabled	FAIL	MEDIUM
A.9.2.1, A.9.2.2, A.9.4.1	KG-015	Monitoring endpoint security	FAIL	MEDIUM
A.12.3.1, A.12.3.2	KG-020	Unclean leader election disabled	PASS	MEDIUM

Requirement ID	Control ID	Control Title	Status	Severity
A.12.4.1, A.12.4.2, A.12.4	KG-021	Log retention configured	PASS	MEDIUM
A.12.5.1, A.12.6.1	KG-023	Broker version consistent	PASS	MEDIUM
A.12.3.1, A.17.1.1	KG-027	Leader election timeout configured	PASS	MEDIUM
A.12.1.1, A.12.1.2, A.12.1	KG-028	Auto-create topics disabled	PASS	MEDIUM
A.12.3.1, A.12.4.2	KG-030	Delete topic disabled	PASS	MEDIUM
A.12.4.1, A.12.4.2, A.12.4	KG-033	Log retention hours configured	PASS	MEDIUM
A.12.4.1	KG-042	Log retention >=90 days	FAIL	MEDIUM
A.9.4.1	KG-047	ACL deny rules configured	PASS	MEDIUM
A.12.3.1, A.17.1.1, A.17.2	KG-052	KRaft controller quorum size >= 3	PASS	MEDIUM
A.12.4.1, A.12.6.1	KG-026	Network threads configured	PASS	LOW
A.12.3.1	KG-031	Compression configured	PASS	LOW
A.12.3.1	KG-032	Log segment bytes appropriate	PASS	LOW
A.12.6.1	KG-034	Network threads appropriate	PASS	LOW
A.12.6.1	KG-035	IO threads appropriate	PASS	LOW
A.12.6.1	KG-036	Send buffer bytes configured	PASS	LOW
A.12.6.1	KG-037	Receive buffer bytes configured	PASS	LOW
A.12.3.1	KG-038	Replica fetch max bytes configured	PASS	LOW
A.12.3.1	KG-039	Message max bytes configured	PASS	LOW
A.12.4.1, A.12.4.2, A.12.4	KG-040	GC logging enabled	FAIL	LOW
A.12.5.1, A.12.6.1	KG-055	Confluent version matches Kafka versi	PASS	LOW