AWS CERTIFIED

# SCS-C02 Security Specialty Quick Reference

65 Qs 170 Min 750 Pass No Penalty

D1 Threat Detection 14% | D2 Logging 18% | D3 Infrastructure 20% | D4 IAM 16% | D5 Data Protection 18% | D6 Governance 14%

## D1 THREAT DETECTION & INCIDENT RESPONSE 14%

| Service | Function | Key Fact |
|---|---|---|
| **GuardDuty** | ML threat detection | CT+VPC+DNS+S3 sources; org via delegated admin; suppression rules for known-good |
| **Detective** | Investigate findings | Behavior graphs from history — NOT detection; used after GuardDuty fires |
| **Inspector** | CVE scanning | EC2 (SSM Agent req)+Lambda+ECR; continuous; CVSS scores; v2 only |
| **Macie** | S3 data classify | Finds PII/PHI/financial in S3; SensitiveData + Policy findings; no auto-action |
| **Security Hub** | Aggregate findings | ASFF format; CIS/FSBP/PCI/NIST; compliance % score; org delegated admin |

| GuardDuty Finding | Meaning |
|---|---|
| **CryptoCurrency:EC2/BitcoinTool** | EC2 querying crypto-mining C&C; domains |
| **UnauthorizedAccess:IAMUser/MaliciousIPCaller** | IAM creds used from a known-bad IP |
| **Policy:S3/BucketPublicAccessGranted** | S3 bucket made publicly accessible |
| **Exfiltration:S3/AnomalousBehavior** | Unusual large data transfer from S3 |
| **Recon:EC2/PortProbeUnprotectedPort** | Port scan detected on EC2 instance |
| **UnauthorizedAccess:EC2/TorClient** | EC2 communicating via a Tor exit-node |

**IR Automation Pattern:**

`GuardDuty → EventBridge → Lambda (deny-all SG + EBS snapshot + revoke IAM + SNS)`

***Compromised key: DISABLE not delete + inline Deny aws:TokenIssueTime < now***
***Inspector needs SSM Agent + AmazonSSMManagedInstanceCore instance profile***
***GD Suppression Rules: auto-archive known-good findings; archived not deleted***

## D2 SECURITY LOGGING & MONITORING 18%

| Log Source | Captures | Use Case |
|---|---|---|
| **CloudTrail Mgmt** | API calls: who/when/what | Audit, compliance, insider threat — free |
| **CloudTrail Data** | S3/Lambda object ops | Who accessed which S3 object — paid |
| **CT Insights** | Unusual API volumes | Spike in CreateUser; anomalous patterns |
| **VPC Flow Logs** | IP meta (no payload) | Network anomalies; ACCEPT/REJECT |
| **R53 Query Logs** | DNS queries from VPC | DNS tunneling; C&C; domain comms |
| **AWS Config** | Resource config state | WHAT changed — CT shows WHO changed |
| **CloudWatch Logs** | App/OS logs + metrics | Metric Filters for ongoing alarms |

**Alert pattern:**

`CloudTrail → CW Logs → Metric Filter → CW Alarm → SNS → team`

**Real-time SIEM:**

`CloudTrail → CW Logs → Subscription Filter → Kinesis → SIEM`

| Config Managed Rule | Checks |
|---|---|
| **restricted-ssh** | SG with 0.0.0.0/0 inbound on port 22 |
| **s3-bucket-public-access-prohibited** | S3 bucket with any public access |
| **iam-password-policy** | Account password complexity settings |
| **cloud-trail-enabled** | CloudTrail active in the account |
| **encrypted-volumes** | EBS volumes encrypted at rest |
| **vpc-flow-logs-enabled** | VPC Flow Logs active on VPC |
| **access-keys-rotated** | IAM access keys not rotated in N days |

| CloudTrail Key Facts |
|---|
| Log integrity: SHA-256 digest files + RSA signature; validate-logs detects tampering |
| Org trail: covers all accounts + all regions; delivers to central S3 in security account |
| CloudTrail Lake: managed SQL lake; no S3/Athena setup needed; 7-year retention |
| Prevent disable (SCP): deny StopLogging + DeleteTrail + UpdateTrail org-wide |
| Config = WHAT changed; CloudTrail = WHO — need BOTH for a complete audit trail |

***CW Alarms: ONE notification per OK→ALARM transition — not per threshold breach***
***Data events must be explicitly enabled; charged and high-volume — enable selectively***

AWS CERTIFIED

# SCS-C02 Security Specialty Quick Reference

65 Qs 170 Min 750 Pass No Penalty

D1 Threat Detection 14% | D2 Logging 18% | D3 Infrastructure 20% | D4 IAM 16% | D5 Data Protection 18% | D6 Governance 14%

## D3 INFRASTRUCTURE SECURITY 20%

| Control | Layer | Key Behavior |
|---|---|---|
| **Security Group** | L4 stateful ENI | Allow-only; SG-to-SG refs; return traffic auto-allowed |
| **NACL** | L3/4 stateless subnet | Allow+Deny; lowest rule# wins; allow ephemeral 1024-65535 out |
| **Network Firewall** | L3-7 VPC | Suricata IPS; SNI domain filter (no decrypt); TLS inspect w/ ACM CA |
| **AWS WAF** | L7 HTTP/HTTPS | ALB/CF/API GW; managed rules; rate-based; geo; bot control |
| **Shield Advanced** | L3-7 org-wide | $3K/mo; L7 needs WAF ACL; DRT 24/7; DDoS cost protection |
| **Firewall Manager** | All org-wide | WAF+Shield+SG+NF+DNS Firewall; auto-applies to new accts/VPCs |

| NACL Critical Rules |
|---|
| NACL evaluated FIRST at subnet — if NACL denies, SG is never reached |
| Lowest rule# wins: rule 100 allow-all beats rule 200 deny-SSH (first match stops) |
| Stateless: MUST allow ephemeral return ports 1024-65535 outbound for TCP/UDP |
| Default NACL: allow all. Custom NACL: deny all — add rules explicitly |

| Session Manager (No-SSH) |
|---|
| No port 22/3389 — eliminates bastion hosts and SSH key management |
| IAM-based via AmazonSSMManagedInstanceCore instance profile on EC2 |
| Commands + output logged to CloudWatch Logs and/or S3 — full audit |
| VPC Interface Endpoints required: ssm + ssmmessages + ec2messages |

| Pattern | Detail |
|---|---|
| **WAF rule priority** | Lower priority# = first evaluated; ALLOW rule before managed group fixes false positives |
| **Shield Adv L7** | Associate WAF Web ACL + enable auto app-layer DDoS mitigation on resource |
| **NF domain filter** | Reads TLS SNI in ClientHello — blocks by domain WITHOUT decrypting HTTPS |
| **WAF rate-based** | Auto-blocks IP > threshold/5 min (min 100 req); auto-unblocks when rate drops |
| **Firewall Mgr prereqs** | Organizations enabled + FMS admin account + Config enabled in ALL accounts |
| **VPC Endpoint Policy** | aws:ResourceOrgID condition blocks S3 exfil to accounts outside your org |

***Shield Advanced L7: WAF Web ACL must be associated — not automatic***
***NF SNI domain blocking needs no decryption; TLS Inspect needs ACM Private CA***

## D4 IDENTITY & ACCESS MANAGEMENT 16%

| Policy Type | Applied To | Behavior |
|---|---|---|
| **Identity-based** | User/Group/Role | Grants permissions; combined with resource policy |
| **Resource-based** | S3/KMS/Lambda etc | Grants cross-account; evaluated with identity policy |
| **Permission Boundary** | User or Role | MAX cap — does NOT grant; effective = identity AND boundary |
| **SCP** | Account or OU | Org MAX ceiling — does NOT grant; mgmt account exempt |
| **Session Policy** | STS session | Further restricts session; cannot exceed role perms |

| IAM Pattern | Implementation |
|---|---|
| **Enforce MFA** | Deny: StringEquals aws:MultiFactorAuthPresent: false |
| **ABAC scoping** | StringEquals: aws:ResourceTag/X: ${aws:PrincipalTag/X} |
| **Confused deputy** | ExternalId condition in cross-account role trust policy |
| **Least-priv policy** | Access Analyzer: Generate Policy from 90-day CloudTrail |
| **Block root API** | SCP deny *:* with condition aws:PrincipalType = Root |
| **Cross-acct DDB** | Role chain: Account A AssumeRole into Account B role |
| **Revoke sessions** | Inline Deny: aws:TokenIssueTime < current timestamp |
| **Region restrict** | SCP deny *:* when aws:RequestedRegion not in approved list |

**Policy Evaluation Order:**
`Explicit Deny > SCP > Resource policy > Identity policy > Boundary > Session`

| IAM Identity Center vs Manual SAML |
|---|
| Identity Center RECOMMENDED for enterprise multi-account SSO |
| Permission sets: one definition deployable to many accounts at once |
| SCIM: auto-provision/de-provision from Azure AD or Okta |
| Manual per-account SAML does not scale for 50+ account environments |

| Access Analyzer Feature | Purpose |
|---|---|
| **External Access findings** | Resources accessible outside org zone of trust — different account or public |
| **Unused Access analyzer** | Roles/keys/permissions unused in 90-180 d lookback — over-provisioned IAM |
| **Policy Validation** | Errors and warnings before a policy is applied — catches mistakes early |
| **Generate Policy** | Minimal least-privilege policy from actual 90-day CloudTrail API usage |
| **Archive Rules** | Suppress known-good findings without deleting; retained for audit history |

***SCP Deny overrides AdministratorAccess — no IAM policy can override it in member accounts***
***Permission Boundary caps one user/role; SCP caps the whole account/OU — neither grants perms***
***Cross-account S3: BOTH bucket policy (Account B) AND IAM policy (Account A) required***

AWS CERTIFIED

# SCS-C02 Security Specialty Quick Reference

65 Qs 170 Min 750 Pass No Penalty

D1 Threat Detection 14% | D2 Logging 18% | D3 Infrastructure 20% | D4 IAM 16% | D5 Data Protection 18% | D6 Governance 14%

## D5 DATA PROTECTION 18%

| S3 Encryption | Key Owner | Audit | Notes |
|---|---|---|---|
| **SSE-S3** | AWS — free default | None | AES-256; default since Jan 2023 |
| **SSE-KMS** | Customer CMK | Full CT | $0.003/10K ops; key policy required |
| **DSSE-KMS** | Customer CMK | 2x KMS | Dual-layer; two KMS calls per object |
| **SSE-C** | Customer (external) | None | Key in HTTPS header; AWS never stores |

| S3 Security Control | Protects Against / Key Fact |
|---|---|
| **Block Public Access (account)** | Overrides ALL bucket policies + ACLs absolutely; applies to existing + new buckets |
| **Object Lock — Compliance mode** | Truly immutable WORM; nobody incl root can delete/shorten retention |
| **Object Lock — Governance mode** | Bypassable with s3:BypassGovernanceRetention — less strict |
| **Bucket policy: aws:SecureTransport false → Deny** | Enforces HTTPS-only; all HTTP requests are rejected |
| **VPC Endpoint + aws:ResourceOrgID** | Blocks exfil to any S3 bucket outside your AWS organization |
| **MFA Delete** | Extra MFA step required to delete any object version |

| KMS Concept | Key Fact |
|---|---|
| **Envelope encryption** | GenerateDataKey: DEK encrypts data locally; CMK encrypts DEK; data never in KMS (4 KB limit) |
| **Key policy required** | CMK access needs BOTH IAM policy (kms:Decrypt + kms:GenerateDataKey) AND key policy grant |
| **Deletion window** | 7-30 day pending period; cancel to recover; after expiry data is permanently irrecoverable |
| **Multi-Region keys** | Same key material in multiple regions; different ARNs; cross-region decrypt without API hop |
| **CloudHSM vs KMS** | CloudHSM: FIPS Level 3, sole control, PKCS#11; Custom Key Store: CloudHSM as KMS backend |

| Secrets Manager vs Parameter Store |
|---|
| Secrets Manager: built-in auto-rotation; native RDS/Redshift/DocumentDB; $0.40/secret/month |
| Parameter Store SecureString: no built-in rotation; lower cost; good for config values/flags |
| ACM public certs: free for ALB/CloudFront/API GW; private key cannot be exported from ACM |

***Encrypt existing RDS: snapshot → copy with KMS → restore new DB instance (immutable at creation)***
***Encrypt existing EBS: snapshot → copy with KMS encryption → create new volume from copy***
***SSE-KMS most auditable: CT logs kms:GenerateDataKey (upload) + kms:Decrypt (download) per object***

## D6 MANAGEMENT & SECURITY GOVERNANCE 14%

| Service | Function | Key Fact |
|---|---|---|
| **Control Tower** | Multi-acct landing zone | Preventive=SCPs (block); Detective=Config rules (detect); Account Factory provisioning |
| **AWS Artifact** | Compliance reports | SOC1/2/3, PCI DSS AOC, ISO 27001, FedRAMP — free on-demand, no AWS Support needed |
| **Access Analyzer** | External access audit | External access; unused access (90-180d); policy validation; Generate Policy |
| **Trusted Advisor** | Best-practice checks | Core security checks free; full suite needs Business/Enterprise support |
| **Config Aggregator** | Multi-account Config | Centralizes compliance data across all accounts + regions org-wide |
| **Security Hub** | Findings + standards | CIS+FSBP+PCI+NIST; compliance % score; org delegated admin aggregates all |

| Control Tower Guardrail Types |
|---|
| PREVENTIVE: SCPs — block prohibited actions BEFORE they can happen |
| DETECTIVE: Config rules — detect non-compliant resources AFTER the fact |
| Account Factory: new accounts inherit all OU guardrails automatically |
| Audit + Log Archive accounts: org CloudTrail + Config centralized here |

| Governance Pattern | Solution |
|---|---|
| **Enable security services org-wide** | GD+SH+Macie+Inspector: delegated admin + auto-enable for new org members |
| **Prove PCI DSS compliance** | Artifact: PCI DSS Attestation of Compliance + AWS Responsibility Summary |
| **Service whitelist** | Remove FullAWSAccess SCP; attach Allow-only SCPs for approved services |
| **Find over-provisioned IAM** | Access Analyzer unused access analyzer (90-180 day lookback) |
| **2-year tamper-proof trail** | CloudTrail + Config in S3 with Object Lock Compliance mode + 2yr retention |
| **Detect external sharing** | Access Analyzer org zone of trust — surfaces all external access findings |
| **Auto-remediate Config** | Config rule NON_COMPLIANT → SSM Automation doc (manual or auto mode) |

***Fargate: AWS manages host OS + compute; customer manages container image + task IAM role***
***Config Conformance Packs: YAML bundle of rules + remediations; pre-built CIS/PCI/HIPAA/NIST***
***Security Hub score = (passing / total evaluated) x 100; below 80% = significant gaps***

AWS CERTIFIED

# SCS-C02 Security Specialty Quick Reference

65 Qs 170 Min 750 Pass No Penalty

| D1 Threat Detection 14% | D2 Logging 18% | D3 Infrastructure 20% | D4 IAM 16% | D5 Data Protection 18% | D6 Governance 14% |
|---|---|---|---|---|---|

## MASTER QUICK REFERENCE — KNOW THESE COLD

| Service / Concept | Dom | The Key Fact to Remember |
|---|---|---|
| **GuardDuty** | D1 | ML detect; CT+VPC+DNS+S3; org via delegated admin; suppression rules for noise |
| **Amazon Detective** | D1 | INVESTIGATES findings — NOT detection; behavior graphs; starts where GuardDuty ends |
| **Amazon Inspector** | D1 | CVE scan EC2(SSM Agent req)+Lambda+ECR; continuous; CVSS scores |
| **Amazon Macie** | D1 | S3 PII/PHI/financial via ML; SensitiveData + Policy findings; no auto-action |
| **Security Hub** | D1 | ASFF; CIS/FSBP/PCI/NIST; compliance % score; org delegated admin aggregates all |
| **IR: compromised key** | D1 | DISABLE not delete + inline Deny aws:TokenIssueTime < now + investigate blast radius |
| **CloudTrail data events** | D2 | Explicitly enable for S3/Lambda; records GetObject/PutObject/Invoke; paid |
| **CloudTrail Insights** | D2 | Detects unusual management API VOLUMES vs baseline — not data events or network |
| **Config vs CloudTrail** | D2 | Config = WHAT changed (state); CloudTrail = WHO changed + when + credentials |
| **Prevent CT disable** | D2 | SCP deny StopLogging + DeleteTrail + UpdateTrail in all member account OUs |
| **R53 query logs** | D2 | Detect DNS tunneling: data encoded in subdomain queries to C&C; DNS server |
| **CW metric filter** | D2 | Filter → metric → CW Alarm → SNS; ONE notification per OK→ALARM transition |
| **Security Group** | D3 | Stateful; ENI-level; allow-only; return traffic auto-allowed; SG-to-SG refs |
| **NACL** | D3 | Stateless; subnet-level; lowest rule# wins; allow ephemeral 1024-65535 out |
| **AWS WAF** | D3 | L7 ALB/CF/API GW; managed rule groups; rate-based per IP/5 min |
| **Shield Advanced** | D3 | $3K/mo org; L7 needs WAF ACL + auto L7 mitigation enabled; DRT 24/7 |
| **Network Firewall** | D3 | VPC Suricata IPS; SNI domain filter (no decrypt); TLS inspect w/ ACM CA |
| **Firewall Manager** | D3 | WAF+Shield+SG+NF+DNS Firewall org-wide; auto-applies new accts/VPCs |
| **Session Manager** | D3 | No port 22/3389; IAM-based; log to CW/S3; VPC endpoints: ssm+ssmmessages+ec2messages |
| **SCP basics** | D4 | MAX ceiling — does NOT grant; AdministratorAccess cannot override SCP Deny |
| **Permission boundary** | D4 | Caps MAX for specific user/role; effective = identity policy AND boundary |
| **IAM eval order** | D4 | Explicit Deny > SCP > Resource-based > Identity-based > Boundary > Session |
| **ExternalId** | D4 | Prevents confused deputy; shared secret required in trust policy condition |
| **ABAC in IAM** | D4 | Tag principal + resource; condition: aws:ResourceTag/X = ${aws:PrincipalTag/X} |
| **MFA enforcement** | D4 | Deny when StringEquals aws:MultiFactorAuthPresent: false |
| **IAM Identity Center** | D4 | Preferred enterprise SSO; permission sets; SCIM auto-provision; Orgs integration |
| **IAM Access Analyzer** | D4 | External access + unused access (90d) + Generate Policy from CloudTrail |
| **SSE-KMS requirement** | D5 | Need BOTH: IAM policy (kms:Decrypt + kms:GenerateDataKey) AND KMS key policy grant |
| **S3 Object Lock Compliance** | D5 | Truly immutable WORM; nobody incl root can delete/shorten; for SEC 17a-4/FINRA |
| **S3 Block Public Access** | D5 | Account-level overrides ALL bucket policies + ACLs; existing + new buckets |
| **Envelope encryption** | D5 | GenerateDataKey: DEK encrypts data; CMK encrypts DEK; data never flows through KMS |
| **KMS deletion window** | D5 | 7-30 day pending period; cancel to recover; after expiry = permanently irrecoverable |
| **CloudHSM vs KMS** | D5 | CloudHSM: FIPS Level 3, sole control, PKCS#11; Custom Key Store: HSM as KMS backend |
| **RDS/EBS encrypt existing** | D5 | Snapshot → copy with KMS → restore new instance/volume; no in-place encryption |
| **Secrets Manager** | D5 | Auto-rotation; native RDS/Redshift; VPC endpoint if DB in private VPC; $0.40/secret |
| **VPC Endpoint Policy** | D5 | aws:ResourceOrgID condition blocks S3 exfil to buckets outside your org |
| **Control Tower guardrails** | D6 | Preventive=SCP (blocks); Detective=Config rule (detects); Account Factory governs |
| **AWS Artifact** | D6 | Free on-demand: SOC1/2/3, PCI DSS AOC, ISO 27001, FedRAMP; BAA/GDPR DPA agreements |
| **Security Hub standards** | D6 | CIS + FSBP + PCI DSS + NIST SP 800-53; compliance % score per standard/account |
| **AWS-internal encryption** | D5 | All EC2 traffic encrypted at L2 NIC hardware within same Region; no action needed |

**EXAM TIPS:** 750/1000 pass | 65 Qs | 170 min | No penalty — answer all | Mark and review scenario questions
**HOT TOPICS:** GuardDuty vs Detective vs Inspector vs Macie | KMS: key policy + IAM policy BOTH required | SCP vs Permission Boundary | NACL stateless ephemeral ports | CloudTrail + Config for complete audit
**ALWAYS CHOOSE:** Secrets Manager for rotation | IAM Identity Center for enterprise SSO | Shield Advanced + WAF ACL for L7 DDoS | Session Manager over SSH | Access Analyzer Generate Policy for least privilege | SCP Deny for org-wide preventive controls