1.1 Incident Response:

https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/incident-response.html

https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/aws-security-incident-response-guide.html

https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/abuse-and-compromise.html

1.2 Detect security threats

https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/alert-sources.html

1.3 Respond to compromised resources

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_revoke-sessions.html

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/security-group-connection-tracking.html

https://docs.aws.amazon.com/secretsmanager/latest/userguide/rotating-secrets.html

https://repost.aws/knowledge-center/move-ec2-instance

2.1 Design and implement security monitoring and alerting

https://docs.aws.amazon.com/systems-manager/latest/userguide/patch-manager-security-hub-integration.html

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/AlarmThatSendsEmail.html

https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-cloudwatch-events.html

2.2 Troubleshoot security monitoring and alerting

https://docs.aws.amazon.com/solutions/latest/automated-security-response-on-aws/issues-and-resolutions.html

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/troubleshooting-CloudWatch-Agent.html

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/configuring-IMDS-new-instances.html

https://docs.aws.amazon.com/organizations/latest/userguide/services-that-can-integrate-inspector2.html

2.3 Design and implement a logging solution

https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/sec_detect_investigate_events_app_service_logging.html

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver-query-logs.html

2.4 Troubleshoot logging solutions

https://docs.aws.amazon.com/awscloudtrail/latest/userguide/default-kms-key-policy.html

https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-receive-logs-from-multiple-accounts.html

2.5 Design a log analysis solution

https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/sec_detect_investigate_events_analyze_all.html

https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/FilterAndPatternSyntax.html#metric-filters-extract-json

3.1 Design and implement security controls for edge services

https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/infrastructure-security.html

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/SecurityAndPrivateContent.html

https://docs.aws.amazon.com/whitepapers/latest/guidelines-for-implementing-aws-waf/guidelines-for-implementing-aws-waf.html?did=wp_card&trk=wp_card

3.2 Design and implement network security controls

https://docs.aws.amazon.com/directconnect/latest/UserGuide/MACsec.html

https://d1.awsstatic.com/architecture-diagrams/ArchitectureDiagrams/inspection-deployment-models-with-AWS-network-firewall-ra.pdf?did=wp_card&trk=wp_card

https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/sec_network_protection_layered.html

3.3 Design and implement security controls for compute workloads

https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/protecting-compute.html

https://docs.aws.amazon.com/accounts/latest/reference/credentials-access-keys-best-practices.html

https://docs.aws.amazon.com/IAM/latest/UserGuide/security-creds.html

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/configuring-IMDS-existing-instances.html

3.4 Troubleshoot network security

https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html

https://docs.aws.amazon.com/inspector/v1/userguide/inspector_network-reachability.html

4.1 Design, implement, and troubleshoot authentication for AWS resources

https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/identity-management.html

https://docs.aws.amazon.com/wellarchitected/latest/framework/sec_securely_operate_aws_account.html

https://docs.aws.amazon.com/rolesanywhere/latest/userguide/introduction.html

https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction_attribute-based-access-control.html

https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_attribute-based-access-control.html

https://aws.amazon.com/blogs/security/aws-federated-authentication-with-active-directory-federation-services-ad-fs/

4.2 Design, implement, and troubleshoot authorization for AWS resources

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html

https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/permissions-management.html

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_condition_operators.html

https://docs.aws.amazon.com/AmazonS3/latest/userguide/amazon-s3-policy-keys.html

https://aws.amazon.com/blogs/security/how-to-use-trust-policies-with-iam-roles/

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_integrate_services_list.html

5.1 Design and implement controls that provide confidentiality and integrity for data in transit

https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/protecting-data-in-transit.html

https://docs.aws.amazon.com/directconnect/latest/UserGuide/remote_regions.html

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.SSL.html

5.2 Design and implement controls that provide confidentiality and integrity for data at rest

https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/protecting-data-at-rest.html

https://docs.aws.amazon.com/kms/latest/cryptographic-details/key-hierarchy.html

https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#kms_keys

https://docs.aws.amazon.com/AmazonS3/latest/userguide/serv-side-encryption.html

5.3 Design and implement controls to manage the lifecycle of data at rest

https://docs.aws.amazon.com/whitepapers/latest/data-classification/data-classification.html

https://docs.aws.amazon.com/AmazonS3/latest/userguide/batch-ops-legal-hold.html

https://docs.aws.amazon.com/aws-backup/latest/devguide/legalhold.html

https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock-overview.html

5.4 Design and implement controls to protect credentials, secrets, and cryptographic key materials

https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/sec_identities_audit.html

https://docs.aws.amazon.com/kms/latest/developerguide/services-parameter-store.html

https://docs.aws.amazon.com/secretsmanager/latest/userguide/security-encryption.html

https://docs.aws.amazon.com/kms/latest/APIReference/API_GenerateDataKeyPair.html

6.1 Develop a strategy to centrally deploy and manage AWS accounts

https://docs.aws.amazon.com/prescriptive-guidance/latest/security-reference-architecture/welcome.html

https://docs.aws.amazon.com/controltower/latest/userguide/best-practices.html

https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/aws-account-management-and-separation.html

https://docs.aws.amazon.com/controltower/latest/userguide/controls.html

6.2 Implement a secure and consistent deployment strategy for cloud resources

https://docs.aws.amazon.com/controltower/latest/userguide/account-factory.html

https://docs.aws.amazon.com/ARG/latest/userguide/resource-groups.html

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_tag-policies.html
https://docs.aws.amazon.com/ram/latest/userguide/shareable.html
https://docs.aws.amazon.com/tag-editor/latest/userguide/tag-policies-orgs-evaluating-org-wide-compliance.html

6.3 Evaluate the compliance of AWS resources
https://docs.aws.amazon.com/macie/latest/user/discovery-asdd.html
https://docs.aws.amazon.com/macie/latest/user/data-classification.html
https://docs.aws.amazon.com/config/latest/developerguide/how-does-config-work.html
https://docs.aws.amazon.com/prescriptive-guidance/latest/aws-security-controls/detective-controls.html
https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/mask-sensitive-log-data.html
https://aws.amazon.com/audit-manager/faqs/
https://docs.aws.amazon.com/macie/latest/user/findings-monitor.html
https://docs.aws.amazon.com/macie/latest/user/findings-monitor-events-uno.html

6.4 Identify security gaps through architectural reviews and cost analysis
https://docs.aws.amazon.com/wellarchitected/latest/cost-optimization-pillar/monitor-cost-and-usage.html
https://aws.amazon.com/well-architected-tool/
https://aws.amazon.com/premiumsupport/technology/trusted-advisor/