Compliance as Code
Lessons Learned from Regulated Organizations

#ossuommit  Sergiu Bodiu
2018 November  CloudNativeCon China
Agenda

- About
- DevOps keeps eating the world
- Compliance as Code
- Infrastructure as code
- Continuous Compliance
About Speakers

Architect. Building Communities. Developer. Speaker

Architect @Standard Chartered
Alumni: Pivotal, JP Morgan, Bank of America Merrill Lynch, Adobe

Founder of Spring User Group Singapore
Organiser for DevOpsDays Singapore

https://www.devopsdays.org/events/2018-singapore

@Sergiu_Bodiu
https://www.linkedin.com/in/sergiubodiu/
What is DevOps

“What is DevOps
It means faster and smaller releases
It’s automation
It’s a job title
It’s Development and Operations collaboration
It means faster and smaller releases

7 Habits of Successful DevOps

“DevOps continues to evolve in response to the state of software development”
- Matt Ray
@matray
## Agile Roles & Responsibilities

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
</table>
| **Tech. & Investment Governance**         | - Secures funds and manages budgets  
- Manage collective activities, issues, and risks  
- Country level implementation and rollout |
| **Solution Architect**                    | - Overall architecture governance  
- Work collaborative with the team in the solution design  
- Define high level architecture design and principles |
| **Stakeholders**                          | - Are sponsors and impacted-teams  
- Have significant decision making authority  
- Ensure project alignment with business and technology strategy |
| **Specialists**                           | - Deep understanding of specific disciplines  
- Bridge gaps in business and technical knowledge  
- Part of the agile team on need basis |
| **Release Team**                          | - Govern releases  
- Perform quality checks and provide approvals  
- Deploy to production |
| **Agile Coach**                           | - Helps teams to adopt and improve on Agile methods and practice  
- Help teams to adopt DevOps tools and practices including CI/CD |
Governance Manual

• IT Security Policy Program Management
• IT Controls Assurance
• Third Party Catalog
• Issue Management
What security and compliance risks or obligations need to be addressed?
The following sections provide considerations for FIs as they assess their responsibilities with regards to the following guidelines:

- MAS Guidelines on Outsourcing
- MAS Technology Risk Management (TRM) Guidelines
- Association of Banks in Singapore (ABS) Cloud Computing Implementation Guide
What are the challenges to migrate to cloud

• What applications are suitable for migration to cloud?
• Is there sufficient business justification for migrating?
• What is the best technical approach for migrating?
• What integration solutions are needed to support an application on the cloud platform?
• What security and compliance risks or obligations need to be addressed?
Customer responsibility “Security in the Cloud”

CUSTOMER
RESPONSIBILITY FOR SECURITY ‘IN’ THE CLOUD

AWS
RESPONSIBILITY FOR SECURITY ‘OF’ THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

SOFTWARE

COMPUTE
STORAGE
DATABASE
NETWORKING

@sergiu_bodiu
AWS Config - Overview

AWS Config

• Monitors and records your AWS resource configurations. It also keeps track of relationships between resources

AWS Config Rules

• Managed (pre-defined) or Custom-created rules that AWS periodically runs to evaluate your configuration to see if configuration is in compliance and provides action.

TLDR; Configuration management “lens” on your AWS resources that can be helpful in your control objectives.

https://github.com/awslabs/aws-config-rules
Compliance Account

Lambda functions (Custom Rules)

One Rule is dedicated to report regularly the compliance status of all AWS resources.

Record compliance results of all resources over time

Keep updated the latest results of all Rules

Send notification in case of a non-compliant resource

Application Account(s)

AWS Config records configurations. Every change triggers appropriate Rule(s) to verify the compliance of the new configuration.

AWS IAM provides short-lived credentials to the lambda functions with the permissions to read the configuration, and react if necessary.

Various AWS resources and services are verified on the defined baseline and can be modified if authorized in the lambda.

Results for compliance and non-compliance are displayed on the Config Dashboard
def IAM_1_2_root_mfa_enabled()
    iam = STS_SESSION.client("iam")
    response = iam.get_account_summary()
    if response['SummaryMap']['AccountMFAEnabled'] != 1:
        status = 'NON_COMPLIANT'
    else:
        status = 'COMPLIANT'

    config = STS_SESSION.client("config")
    config.put_evaluations(
        Evaluations=[
            {
                "ComplianceResourceType": "AWS::IAM::User",
                "ComplianceResourceId": "Root MFA enabled",
                "ComplianceType": status,
                "OrderingTimestamp": str(datetime.now())
            },
        ],
        ResultToken=result_token
    )

https://github.com/awslabs/aws-config-engine-for-compliance-as-code
@sergiu_bodiu

<table>
<thead>
<tr>
<th>Benchmark</th>
<th>Security Control Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 Avoid the use of the &quot;root&quot; account</td>
<td>IAMRootActivityCloudWatchMetric</td>
</tr>
<tr>
<td>1.2 Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password</td>
<td>UsersMustHaveMfaEnabled</td>
</tr>
<tr>
<td>1.3 Ensure credentials unused for 90 days or greater are disabled</td>
<td>DisableUnusedCredentials</td>
</tr>
<tr>
<td>1.4 Ensure access keys are rotated every 90 days or less</td>
<td>DisableUnusedCredentials</td>
</tr>
<tr>
<td>1.5 Ensure IAM password policy requires at least one uppercase letter</td>
<td>IamPasswordPolicyMustMeetRequirements</td>
</tr>
<tr>
<td>1.6 Ensure IAM password policy require at least one lowercase letter</td>
<td>IamPasswordPolicyMustMeetRequirements</td>
</tr>
<tr>
<td>1.7 Ensure IAM password policy require at least one symbol</td>
<td>IamPasswordPolicyMustMeetRequirements</td>
</tr>
<tr>
<td>1.8 Ensure IAM password policy require at least one number</td>
<td>IamPasswordPolicyMustMeetRequirements</td>
</tr>
<tr>
<td>1.9 Ensure IAM password policy requires minimum length of 14 or greater</td>
<td>IamPasswordPolicyMustMeetRequirements</td>
</tr>
<tr>
<td>1.10 Ensure IAM password policy prevents password reuse</td>
<td>IamPasswordPolicyMustMeetRequirements</td>
</tr>
<tr>
<td>1.11 Ensure IAM password policy expires passwords within 90 days or less</td>
<td>IamPasswordPolicyMustMeetRequirements</td>
</tr>
<tr>
<td>1.12 Ensure no root account access key exists</td>
<td>RootAccountMustHaveMfaEnabled</td>
</tr>
<tr>
<td>1.13 Ensure MFA is enabled for the &quot;root&quot; account</td>
<td>RootAccountMustHaveMfaEnabled</td>
</tr>
<tr>
<td>1.14 Ensure hardware MFA is enabled for the &quot;root&quot; account</td>
<td>RootAccountMustHaveMfaEnabled</td>
</tr>
<tr>
<td>1.15 Ensure security questions are registered in the AWS account</td>
<td></td>
</tr>
<tr>
<td>1.16 Ensure IAM policies are attached only to groups or roles</td>
<td>UsersMustNotHaveAssociatedPolicies</td>
</tr>
<tr>
<td>1.17 Enable detailed billing</td>
<td></td>
</tr>
<tr>
<td>1.18 Ensure IAM Master and IAM Manager roles are active</td>
<td></td>
</tr>
<tr>
<td>1.19 Maintain current contact details</td>
<td></td>
</tr>
<tr>
<td>1.20 Ensure security contact information is registered</td>
<td></td>
</tr>
<tr>
<td>1.21 Ensure IAM instance roles are used for AWS resource access from instances</td>
<td>InstancesMustUseIamRoles</td>
</tr>
<tr>
<td>1.22 Ensure a support role has been created to manage incidents with AWS Support</td>
<td></td>
</tr>
<tr>
<td>1.23 Do not setup access keys during initial user setup for all IAM users that have a console password</td>
<td></td>
</tr>
<tr>
<td>1.24 Ensure IAM policies that allow full &quot;<em>:</em>&quot; administrative privileges are not created</td>
<td>IamPoliciesMustNotContainStarStar</td>
</tr>
<tr>
<td>2.1 Ensure CloudTrail is enabled in all regions</td>
<td>CloudTrailMustBeActive</td>
</tr>
<tr>
<td>2.2 Ensure CloudTrail log file validation is enabled</td>
<td>CloudTrailLogFilesMustBeValidated</td>
</tr>
<tr>
<td>2.3 Ensure the S3 bucket CloudTrail logs to is not publicly accessible</td>
<td>CloudTrailBucketMustBeSecure</td>
</tr>
<tr>
<td>2.4 Ensure CloudTrail trails are integrated with CloudWatch Logs</td>
<td>CloudTrailMustBeActive</td>
</tr>
<tr>
<td>2.5 Ensure AWS Config is enabled in all regions</td>
<td>ConfigMustBeEnabledInAllRegions</td>
</tr>
<tr>
<td>2.6 Ensure S3 bucket access logging is enabled on the CloudTrail S3 bucket</td>
<td>CloudTrailBucketMustBeSecure</td>
</tr>
<tr>
<td>2.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs</td>
<td>CloudTrailLogsMustBeValidated</td>
</tr>
<tr>
<td>2.8 Ensure rotation for customer created CMKs is enabled</td>
<td>KmsCustomerKeysMustBeRotated</td>
</tr>
</tbody>
</table>
## PCI DSS compliance and Shared Responsibility

<table>
<thead>
<tr>
<th>PCI DSS Requirement</th>
<th>AWS</th>
<th>Cloud User</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Install and maintain a firewall configuration to protected cardholder data</td>
<td>Shared</td>
<td>Shared</td>
</tr>
<tr>
<td>2 Do not use vendor-supplied defaults for password or other security parameters</td>
<td>Shared</td>
<td>Shared</td>
</tr>
<tr>
<td>3 Protect stored cardholder data</td>
<td>Shared</td>
<td>Shared</td>
</tr>
<tr>
<td>4 Encrypt transmission of cardholder data across open, public networks</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>5 Protect all systems against malware and regularly update AV software/programs</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>6 Develop and maintain secure systems and applications</td>
<td>Shared</td>
<td>Shared</td>
</tr>
<tr>
<td>7 Restrict access to cardholder data by business need to know</td>
<td>Shared</td>
<td>Shared</td>
</tr>
<tr>
<td>8 Identify and authenticate access to system components</td>
<td>Shared</td>
<td>Shared</td>
</tr>
<tr>
<td>9 Restrict physical access to cardholder data</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>10 Track and monitor all access to network resources and cardholder data</td>
<td>Shared</td>
<td>Shared</td>
</tr>
<tr>
<td>11 Regularly test security systems and processes</td>
<td>Shared</td>
<td>Shared</td>
</tr>
<tr>
<td>12 Maintain a policy that addresses info security for all personnel</td>
<td>Shared</td>
<td>Shared</td>
</tr>
</tbody>
</table>
InSpec: Inspect Your Infrastructure

**InSpec** is a run-time framework and rule language used to specify compliance, security, and policy requirements. It includes a collection of resources that help you write auditing controls quickly and easily.

Turn your compliance, security, and other policy requirements into automated tests.
InSpec sample rules

describe aws_iam_user(name: ‘sergiubodiu’) do
    its(‘has_mfa_enabled?’) { should be false }
    its(‘has_console_password?’) { should be true }
end

describe aws_iam_access_key(username: ‘username’, id: ‘access-key id’) do
    it { should exist }
    it { should exist }
    its(‘created_date’) { should be > Time.now -365 * 86400 }
    its(‘last_used_date’) { should be > Time.now -365 * 86400 }
end

describe aws_iam_password_policy do
    its (‘requires_lowercase_letters?’) {should be true }
    its (‘requires_uppercase_letters?’) {should be true }
end

https://github.com/chef/inspec
Cloud Risk and Security Concerns

- Regulatory Obligations
- Statutory and Contractual Obligations
- Authorisation, Authentication and Entitlements
- Data Confidentiality and Privacy
- Data Residency
- Data Sovereignty
- Outsourcing Obligations
- The Right to Audit
Enable governance with pipelines

- Compliance Specifications
- Acceptance Tests
- Pipeline Definitions
- Controls Library

- Environment Definitions

Every change is logged and traceable
Code Testing History

- 1994: Kent Beck writes the SUnit testing framework for Smalltalk (source)
- 1998: article on Extreme Programming mentions that "we usually write the test first" (source)
- 1998 to 2002: "Test First" is elaborated into "Test Driven", in particular on the C2.com Wiki
- 2000: Mock Objects are among the novel techniques developed during that period (source)
- 2003: publication of "Test Driven Development: By Example" by Kent Beck
- 2003: agiledox, the ancestor of BDD, is a tool generating technical documentation automatically from JUnit tests, written by Chris Stevenson
- 2004: in order to test his hypotheses about de-emphasizing "test" terminology in favor of "behavior", Dan North releases JBehave
- 2006: in collaboration with Chris Matts, North proposes the given-when-then canvas to expand the scope of BDD to business analysis and documents the approach in "Introducing BDD"
- 2006-2009: several new tools are released confirming the community's investment in BDD, such as RSpec or more recently, Cucumber and GivWenZen

https://www.agilealliance.org/glossary/tdd
How acceptance TDD and developer TDD work
Flexible Infrastructure

- Developer sandboxing
- Cloud dev/test labs
- Containerization
- Microservices
- Autoscaling
- Failover
Infrastructure as Code is born

Infrastructure Automation: CFengine, Puppet, and Chef

The essence of **Infrastructure as Code** is to treat the configuration of systems the same way source code is treated. **Source code management** (SCM) systems, **TDD, CI, Refactoring**, and other XP practices are especially useful for making sure that changes to infrastructure are thoroughly tested, repeatable, and transparent.

**From the Iron Age to the Cloud Age**

*It uses techniques, practices, and tools from software development to ensure those actions are thoroughly tested before being applied to business critical systems.*

*(Infrastructure as Code - Kief Morris)*
Directed graph representing dependencies of several objects towards each other.
- Wikipedia
Each environment has its own stack instance. Use CD pipeline to promote a stack definition across environments.

Streamline & Centralise information required

• Eliminate duplicates entry of information and ensuring consistency
• Streamline approval process to ensure all regulatory requirements have been reviewed
• Transparency of information and approval process
• Centralised ITO know-how/expertise
• Centralised inventory of 3rd party to identify concentration risk
• Centralised information for Audit (internal, external, regulatory)
• Reduce time for renewal of engagements
Next generation Platforms

Continuous Compliance
Acceptance Test

GIVEN a code repository
  AND a set of approved design patterns
WHEN a new valid design specification file is committed
  AND the file is analyzed against the approved patterns
THEN the design is approved
  AND future releases can go to the "production-like" environment
“As an Application owner, I want to standardize the *NFR* for my applications running on the Cloud.

- Can rely upon solely steering in-flight Projects to Cloud
- Provide next generation software-driven facilities
- Requires detailed Portfolio and Architecture analysis
- Thorough understanding of dependencies and sequencing.
- Formal forecasting, commitments at a very senior level.
- And provision of funding for adoption (or elimination).
- Training new skills
<table>
<thead>
<tr>
<th>IaaS</th>
<th>CaaS</th>
<th>PaaS</th>
<th>FaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Application</td>
<td>Application</td>
<td>Functions</td>
</tr>
<tr>
<td>Data</td>
<td>Data</td>
<td>Data</td>
<td>Data + Application</td>
</tr>
<tr>
<td>Runtime</td>
<td>Runtime</td>
<td>Runtime</td>
<td>Runtime</td>
</tr>
<tr>
<td>Containers (Optional)</td>
<td>Containers</td>
<td>Containers (Optional)</td>
<td>Containers (Optional)</td>
</tr>
<tr>
<td>Operating System</td>
<td>Operating System</td>
<td>Operating System</td>
<td>Operating System</td>
</tr>
<tr>
<td>Virtualization</td>
<td>Virtualization</td>
<td>Virtualization</td>
<td>Virtualization</td>
</tr>
<tr>
<td>Hardware</td>
<td>Hardware</td>
<td>Hardware</td>
<td>Hardware</td>
</tr>
</tbody>
</table>

**Legend**

- Customer Managed
- Unit of Scale
- Delivered as a Service

Compliance as Code
Car as a Service Analogy

Car as a Service

On Premise
- Car
- Finance
- Depreciation
- Servicing
- Renewables
- Insurance
- Road Tax
- Garage
- Fuel
- Road Tolls
- Driver

Infrastructure as a Service (IaaS)
- Car
- Finance
- Depreciation
- Servicing
- Renewables
- Insurance
- Road Tax
- Garage
- Fuel
- Road Tolls
- Driver

Platform as a Service (PaaS)
- Car
- Finance
- Depreciation
- Servicing
- Renewables
- Insurance
- Road Tax
- Garage
- Fuel
- Road Tolls
- Driver

Software as a Service (SaaS)
- Car
- Finance
- Depreciation
- Servicing
- Renewables
- Insurance
- Road Tax
- Garage
- Fuel
- Road Tolls
- Driver

Car Owned
Car Leased
Car Hired
Taxi

Managed by Client
Managed by Service Provider
Governance, Risk & Compliance Approach

• Baseline Evaluation
• Gap analysis
• Minimal viable cloud service
• Ongoing assurance
• Regulatory compliance
AWS Provisioner that runs InSpec tests in the DevSec baselines.

```terraform
resource "aws_instance" "web" {
  connection {
    user = "ubuntu"
  }

  instance_type = "t2.micro"
  ami = "${lookup(var.aws_amis, var.aws_region)}"
  vpc_security_group_ids = ["${aws_security_group.default.id}"]
  subnet_id = "${aws_subnet.default.id}"
  key_name = "inspec"

  provisioner "inspec" {
    profiles = [
      "supermarket://dev-sec/linux-baseline",
      "supermarket://dev-sec/ssh-baseline",
    ]

    on_failure = "continue"
  }

  tags {
    Name = "HelloCompliance"
  }
}

https://github.com/inspec/terraform-provisioner-inspec
# installs inspec and executes the profiles
# allow pass if compliance errors happen
# compliance tags

# connects as user ubuntu
# ssh key
```

@sergiu_bodiu
Packer Workflow

Build → Provision → Post-Processes → Docker → VirtualBox → VMWare → AWS EC2 → Application Images
Immutable Images Flexibility vs Simplicity
Four Abstractions of Cloud Native Operations

- Service Brokers
- Containers
- Applications
- Functions

Operational Efficiency

Opinions
Why automate?

• Continuous monitoring
• Continuous assessment
• Audit and Compliance
• Change management
• Operational troubleshooting
Thank you

Questions?

@Sergiu_Bodiu
https://www.linkedin.com/in/sergiubodiu/
Improve Flow of Customer Value

Continuous Integration
Continuous Deployment
Release Management
Automated Testing
System Engineers and Software Engineers

WE ARE HIRING
Cost per mile

Charge Time

All Electric
When battery is fully charged, first 35 miles only.

93 MPGeq
36 kW-hrs per 100 miles

$601 cost per year if always run in All Electric

Gas Only
When electricity is used up, runs on gas for another 344 miles.

37 MPG
2.7 gallons per 100 miles

$1,302 cost per year if always run in Gas Only mode

Range (Miles)

All Electric Range (battery) - 35 miles

Extended Range (gas) - 379 miles

Examples: Charging Routines

Miles driven between full charge | Fuel Economy MPG | Electricity Consumed | Electricity + Fuel Energy Cost
--- | --- | --- | ---
30 | N/A | 10.9 kWh | 4¢/mi
45 | 168 | 12.9 kWh | 5¢/mi
60 | 89 | 12.9 kWh | 6¢/mi
75 | 69 | 12.9 kWh | 7¢/mi
Never Charge | 37 35 city / 40 hwy | N/A | 9¢/mi

Your actual mileage and costs will vary with fuel cost, temperature, driving conditions, and how you drive and maintain your vehicle. Costs estimates are based on 15,000 miles per year at $3.20 per gallon and 11 cents per kWh. MPGeq: 33.7 kW-hrs = 1 gallon gasoline energy.

Visit www.fueleconomy.gov to download the Fuel Economy Guide (also available at dealers).
## Common Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cloud (Computing)</strong></td>
<td>• On-demand delivery of IT resources via broad network access with rapid elasticity, resource pooling, and measured service.</td>
</tr>
<tr>
<td><strong>Container</strong></td>
<td>• An isolated user-space instance created by OS-level virtualization. Make it easier to package and deploy applications by treating the Container as a unit of software delivery</td>
</tr>
<tr>
<td><strong>IaaS</strong></td>
<td>• Self service model for provisioning and utilizing compute, storage and networking and resources in a pay-as-you-go model, on a service basis without any upfront commitment.</td>
</tr>
<tr>
<td><strong>PaaS</strong></td>
<td>• A platform for the development or running of applications by providing a development framework that abstracts much of the underlying infrastructure and operating system</td>
</tr>
<tr>
<td><strong>SaaS</strong></td>
<td>• Cloud service model where a vendor provided application is accessed remotely, usually over the internet, by the customer. The entire application-infrastructure stack and operations is managed by the vendor, usually in a multi-tenant configuration.</td>
</tr>
</tbody>
</table>
What is Governance and Compliance

• **Governance** is the oversight role and the process by which firms manage and mitigate risks.

• **IT Governance** is defined as the processes that ensure the effective and efficient use of IT in enabling an organization to achieve its goals.

• **Compliance** ensures that an organization has the process and internal controls to meet the requirements imposed by the governance body.
## Common Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Re-architect</strong></td>
<td>• Major changes to the application and/or infrastructure architecture leveraging the capabilities and services offered by the target platform</td>
</tr>
<tr>
<td>Benchmark</td>
<td>Profile Level</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------</td>
</tr>
<tr>
<td>1.1 Avoid the use of the &quot;root&quot; account</td>
<td>1</td>
</tr>
<tr>
<td>1.2 Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password</td>
<td>1</td>
</tr>
<tr>
<td>1.3 Ensure credentials unused for 90 days or greater are disabled</td>
<td>1</td>
</tr>
<tr>
<td>1.4 Ensure access keys are rotated every 90 days or less</td>
<td>1</td>
</tr>
<tr>
<td>1.5 Ensure IAM password policy requires at least one uppercase letter</td>
<td>1</td>
</tr>
<tr>
<td>1.6 Ensure IAM password policy require at least one lowercase letter</td>
<td>1</td>
</tr>
<tr>
<td>1.7 Ensure IAM password policy require at least one symbol</td>
<td>1</td>
</tr>
<tr>
<td>1.8 Ensure IAM password policy require at least one number</td>
<td>1</td>
</tr>
<tr>
<td>1.9 Ensure IAM password policy requires minimum length of 14 or greater</td>
<td>1</td>
</tr>
<tr>
<td>1.10 Ensure IAM password policy prevents password reuse</td>
<td>1</td>
</tr>
<tr>
<td>1.11 Ensure IAM password policy expires passwords within 90 days or less</td>
<td>1</td>
</tr>
<tr>
<td>1.12 Ensure no root account access key exists</td>
<td>1</td>
</tr>
<tr>
<td>1.13 Ensure MFA is enabled for the &quot;root&quot; account</td>
<td>2</td>
</tr>
<tr>
<td>1.14 Ensure hardware MFA is enabled for the &quot;root&quot; account</td>
<td>2</td>
</tr>
<tr>
<td>1.15 Ensure security questions are registered in the AWS account</td>
<td>1</td>
</tr>
<tr>
<td>1.16 Ensure IAM policies are attached only to groups or roles</td>
<td>1</td>
</tr>
<tr>
<td>1.17 Enable detailed billing</td>
<td>1</td>
</tr>
<tr>
<td>1.18 Ensure IAM Master and IAM Manager roles are active</td>
<td>1</td>
</tr>
<tr>
<td>1.19 Maintain current contact details</td>
<td>1</td>
</tr>
<tr>
<td>1.20 Ensure security contact information is registered</td>
<td>1</td>
</tr>
<tr>
<td>1.21 Ensure IAM instance roles are used for AWS resource access from instances</td>
<td>2</td>
</tr>
<tr>
<td>1.22 Ensure a support role has been created to manage incidents with AWS Support</td>
<td>1</td>
</tr>
<tr>
<td>1.23 Do not setup access keys during initial user setup for all IAM users that have a console password</td>
<td>1</td>
</tr>
<tr>
<td>1.24 Ensure IAM policies that allow full &quot;&quot;*/&quot;&quot; administrative privileges are not created</td>
<td>1</td>
</tr>
<tr>
<td>2. Logging</td>
<td></td>
</tr>
<tr>
<td>2.1 Ensure CloudTrail is enabled in all regions</td>
<td>1</td>
</tr>
<tr>
<td>2.2 Ensure CloudTrail log file validation is enabled</td>
<td>2</td>
</tr>
<tr>
<td>2.3 Ensure the S3 bucket CloudTrail logs to is not publicly accessible</td>
<td>1</td>
</tr>
<tr>
<td>2.4 Ensure CloudTrail trails are integrated with CloudWatch Logs</td>
<td>1</td>
</tr>
<tr>
<td>2.5 Ensure AWS Config is enabled in all regions</td>
<td>1</td>
</tr>
<tr>
<td>2.6 Ensure S3 bucket access logging is enabled on the CloudTrail S3 bucket</td>
<td>1</td>
</tr>
<tr>
<td>2.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs</td>
<td>2</td>
</tr>
<tr>
<td>2.8 Ensure rotation for customer created CMKs is enabled</td>
<td>2</td>
</tr>
</tbody>
</table>