

An aerial photograph of a tropical beach and high-rise buildings. The beach is on the left, with people and umbrellas. The ocean is a vibrant turquoise. On the right, several modern high-rise buildings with glass facades and balconies are visible. A large teal graphic overlay, consisting of a grid of lines, is positioned over the buildings and extends towards the beach. In the center, there is a white box with a black border containing the event information.

# GRC

SUMMIT 2023

MIAMI, JUNE 14 & 15

Hosted by **MetricStream**

EXPERIENCE  
**the Power of Connection**



The logo for GRC Summit 2023, featuring the letters 'GRC' in a large, bold, teal font.

SUMMIT 2023

MIAMI, JUNE 14 & 15

Hosted by MetricStream

A panoramic view of a city skyline with several tall skyscrapers. Overlaid on the image are numerous thin, teal-colored lines that connect different buildings, symbolizing a network or digital connectivity. The sky is blue with scattered white clouds.

EXPERIENCE  
the Power of Connection

# Unlocking Cloud Compliance: Optimizing Audit With Automation

Anil Kumar GK- Senior Director (IT & Cyber Security- MetricStream)

Neha Singh Rajpurohit-Senior Product Manager (AWS Audit Manager)

# Agenda

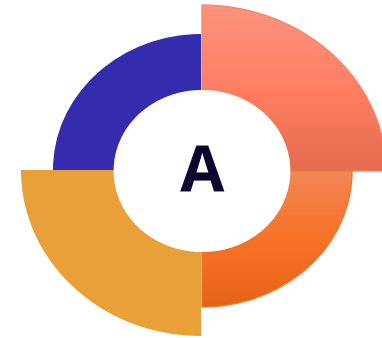
1. Traditional audit experience
2. Challenges faced by customer
3. Compliance at cloud scale
4. Enabling compliance through automation
5. About AWS Audit Manager
6. Example walkthrough
7. Leveraging GRC to optimize audits



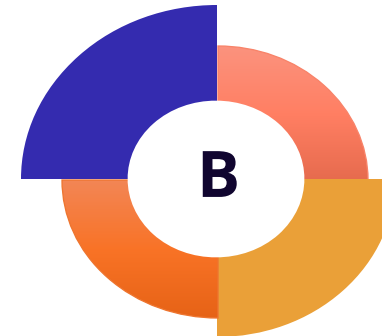
# How do you see your organization towards **automating evidence extraction** for audits and compliance requirements.

**Spectators** – We extract evidence manually as this is the easiest solution for us now and are waiting to see what others are doing  
**Explorers** – We are evaluating opportunities for automation, and we are still new to this area

**Innovators** – We have taken steps to automate our controls and will look to do so as much as possible  
**Visionary** – our goal is to develop a path to automate everything



Spectators & Explorers



Innovators & Visionary

# Typical Audit Experience

**Tedious**

**Time-Consuming**

**Redundant**





# What makes audits inefficient?



**Manual collection  
of Evidence**



**Difficulty in  
searching & reuse  
of Evidence**



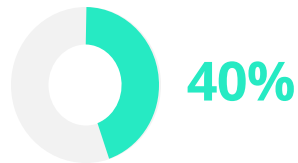
**Incorrect or  
Incomplete  
Evidence**



**Redaction and  
sharing of  
Evidence**

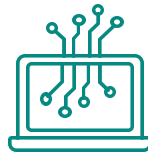
# Broad classification of controls

## Area of applicability



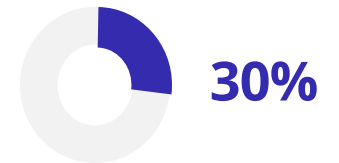
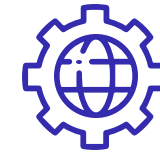
### Infrastructure

- They help to protect the organizations infrastructure from a variety of threats, including unauthorized access, data breaches, and malware attacks.



### Applications

- They are designed to protect specific applications from a variety of threats, including unauthorized access, data breaches, and malware attacks.

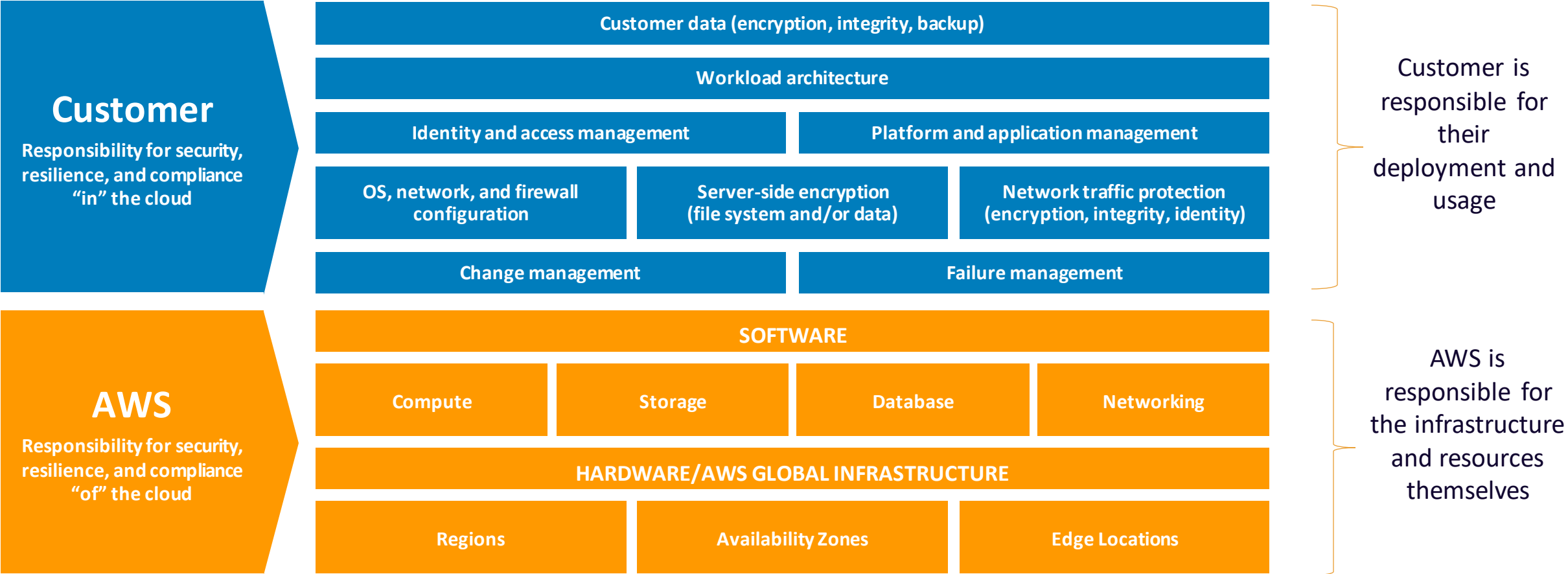


### Policies and Procedures

- Policy and procedural controls are an important part of an organization's overall information security program.

# Cloud Compliance is a shared responsibility

Security and Compliance is a shared responsibility between AWS and the customer.





# Continuous compliance requires insight and automation



Precise Visibility



Near-Real-Time Automation

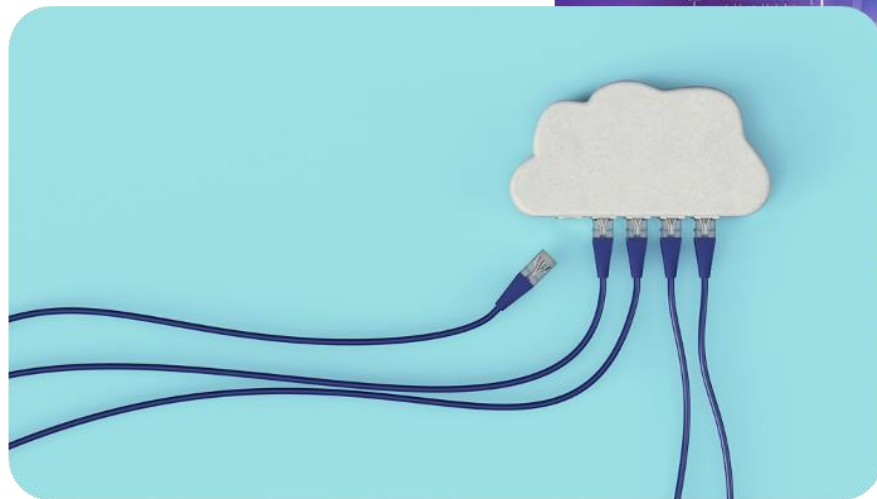


Continuous Compliance

Having the visibility into **WHO** made **WHAT** change from **WHERE** in near-real time enables you to **DETECT** mis-configurations and non-compliance and **RESPOND** quickly to **PREVENT** risks from materializing.

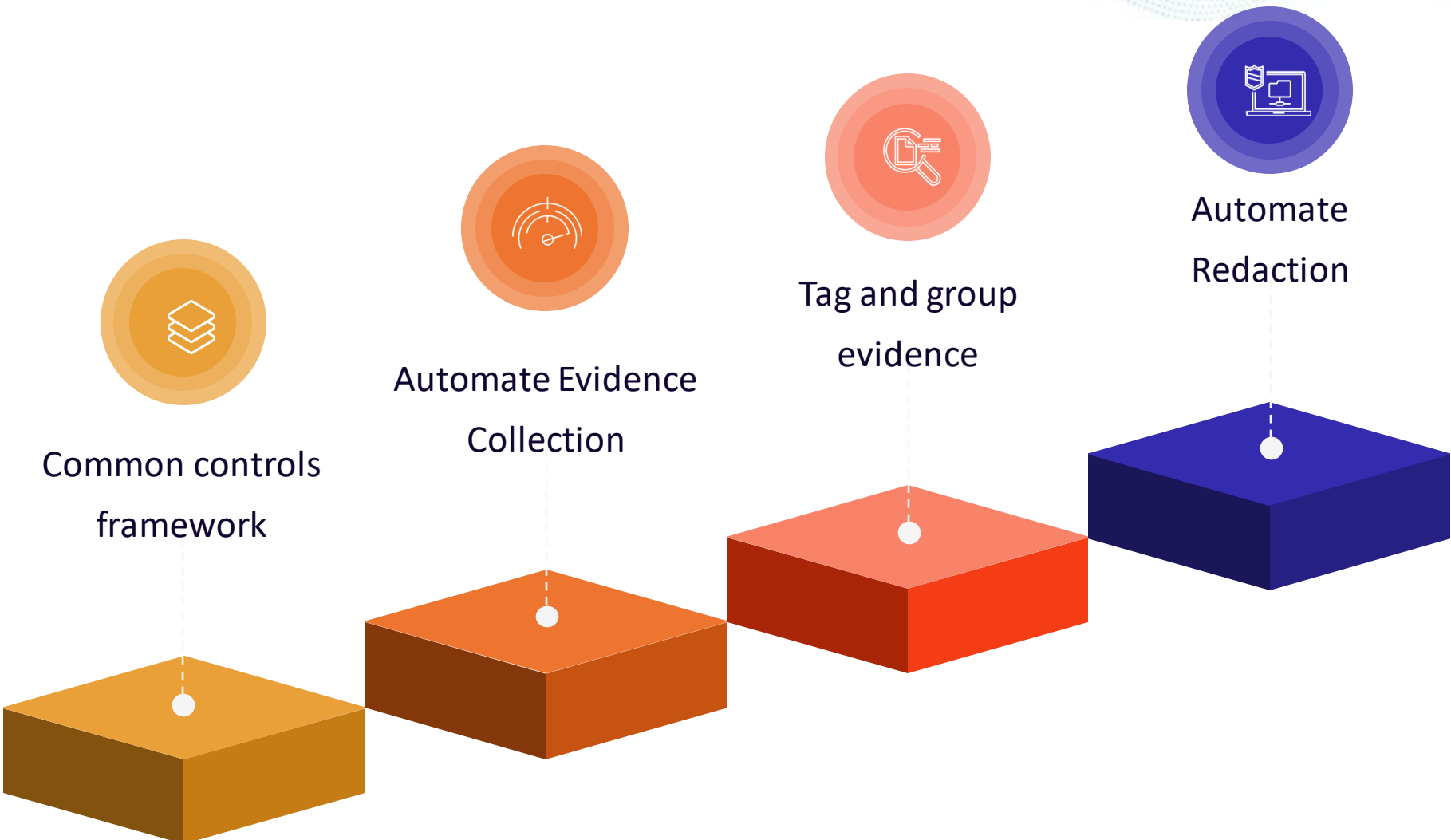
# Cloud audits : where automation is not an option but a necessity

Highly dynamic environments  
Micro-services connected via  
API



- Data segmentation
- Data access controls
- API security & authentication
- CSP security controls
- Inheritance / reliance

# Gaining Efficiency via automation





# Advantages of Automation

- Save time, effort
- Improve speed and accuracy
- Better reporting
- Build employee morale



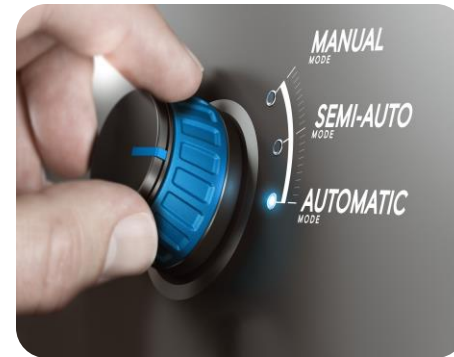
# How does Audit Manager help?



Immutable storage  
of evidence



Verifiable  
provenance



Automated testing



Evidence mapped to  
framework controls

# PCI audit example

Requirement: 1.2.1.c Examine firewall and router configurations to verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit “deny all” or an implicit deny after allow statement....

## On-premise audit considerations

- firewalls
- routers
- switches
- WAN / LAN considerations

## Cloud audit considerations

- security groups
- network access control lists (NACLs)



# PCI audit example – on premise evidence

Requirement: 1.2.1.c Examine firewall and router configurations to verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit “deny all” or an implicit deny after allow statement...

The image displays several pieces of evidence related to network security configurations:

- Table 1: Firewall Rules**

No.	Protocol	Source IP	Destination IP	Dest. Port	Action
1	TCP	10.1.1.1	1.1	80	Accept
2	TCP	10.1.1.2	1.1	80	Deny
3	TCP	10.1.1.0/24	1.1	80	Deny
4	TCP	10.1.1.3	1.1	80	Deny
5	TCP	10.2.2.0/24	1.1	80	Accept
6	TCP	10.2.2.5	1.1	80	Deny
7	TCP	10.3.3.0/24	1.1	80	Deny
8	TCP	10.3.3.9	1.1	80	Deny
9	IP	0.0.0.0/0	1.1	80	Deny

- Windows Firewall Settings:** A screenshot of the Windows Firewall control panel. The "Firewall state" is set to "On (recommended)". The "Inbound connections" are set to "Block (default)", which is highlighted with a red box. The "Outbound connections" are set to "Allow (default)".
- Cisco Router CLI:** A screenshot of a Cisco CLI terminal window for router R1. The prompt is R1(config)#. The terminal shows the command `R1(config)#exit` and the prompt returns to R1#.
- Network Switch Configuration:** A screenshot of a network switch configuration window showing VLANs. The "SWITCH\_A#show vlan brief" command output is displayed. The output shows three active VLANs: 1 (default), 10 (FINANCE), and 20 (SALES). The "20 SALES" entry is highlighted with a red box. The output also shows ports assigned to each VLAN.

# PCI audit example – cloud configuration evidence

Requirement: 1.2.1.c Examine firewall and router configurations to verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit “deny all” or an implicit deny after allow statement...

```
NetworkAcls": [
  {
    "Associations": [
      {
        "NetworkAclAssociationId": "aclassoc-0e8cd78c1d8857a03",
        "NetworkAclId": "acl-06e9829e9b8db400d",
        "SubnetId": "subnet-073ef6280824e8dcb"
      },
      {
        "NetworkAclAssociationId": "aclassoc-00b7233eb7b09c4a1",
        "NetworkAclId": "acl-06e9829e9b8db400d",
        "SubnetId": "subnet-0d44aa499211f9d5c"
      }
    ],
    "Entries": [
      {
        "CidrBlock": "0.0.0.0/0",
        "Egress": true,
        "PortRange": {
          "From": 1,
          "To": 65535
        },
        "Protocol": "6",
        "RuleAction": "allow",
        "RuleNumber": 100
      },
      {
        "FromPort": 443,
        "IpProtocol": "tcp",
        "IpRanges": [
          {
            "CidrIp": "10.100.0.0/16"
          }
        ],
        "Ipv6Ranges": [],
        "PrefixListIds": [],
        "ToPort": 443,
        "UserIdGroupPairs": []
      }
    ]
  }
],
"OwnerId": "423428496460",
"GroupId": "sg-019d9aec33eda4a34",
"IpPermissionsEgress": [
  {
    "FromPort": 80,
    "IpProtocol": "tcp",
    "IpRanges": [
      {
        "CidrIp": "0.0.0.0/0"
      }
    ],
    "Ipv6Ranges": [],
    "PrefixListIds": [],
    "ToPort": 80,
    "UserIdGroupPairs": []
  }
],
"IpPermissionsIngress": [
  {
    "FromPort": 80,
    "IpProtocol": "tcp",
    "IpRanges": [
      {
        "CidrIp": "0.0.0.0/0"
      }
    ],
    "Ipv6Ranges": [],
    "PrefixListIds": [],
    "ToPort": 80,
    "UserIdGroupPairs": []
  }
]
```

# Out of the box framework support

- HIPAA Security Rule 2003
- SOC 2
- GxP EU Annex 11
- GxP 21 CFR Part 11
- NIST 800-53 (Rev. 5) Low-Moderate-High
- NIST Cybersecurity Framework version 1.1
- NIST SP 800-171 Rev. 2
- Essential Eight
- PCI DSS V3.2.1
- Canadian Centre for Cyber Security - Medium
- AWS Foundational Security Best Practices
- ISO-IEC 27001:2013 Annex A
- FedRAMP Moderate Baseline
- CIS Controls v8 IG1



# Consolidated View of Control testing

➤ Integrated test results for GRC controls from Manual and Automated testing

➤ Easy Access to evidences gathered across control testing

The screenshot displays a web application interface for 'IT COMPLIANCE CONTROL TESTING'. The page title is 'IT COMPLIANCE CONTROL TESTING' and it shows 'Last updated a few seconds ago'. The interface includes a 'Saved Layout' dropdown, a 'Show Filters' button, and an 'Options' menu. The main content is a table with columns: Control Name, Design Effectiveness, Operating Effectiveness, CCM Rating, # Rules, and Start Task. The table is grouped into two sections: 'HIPAA Security Rule (10)' and 'PCI DSS v3.2.1 (14)'. The table rows show various control names with their respective effectiveness ratings and CCM ratings. The table footer indicates 'Page 1 of 9' and 'Records Per Page: 20'.

Control Name	Design Effectiveness	Operating Effectiveness	CCM Rating	# Rules	Start Task
<b>AREA OF COMPLIANCE : HIPAA Security Rule (10)</b>					
<a href="#">PM-15 Contacts With Security Groups And Associations</a>	Designed Effectively	Operating Effectively	N/A		▶
<a href="#">PM-09 Risk Management Strategy</a>	Designed Effectively	Operating Effectively	N/A	1	▶
<a href="#">RA-02 Security Categorization</a>	Designed Effectively	Operating Effectively	N/A		▶
<a href="#">PM-02 Senior Information Security Officer</a>			Passed		▶
<a href="#">PM-03 Information Security Resources</a>			Failed		▶
<a href="#">PM-04 Plan Of Action And Milestones Process</a>			Failed	1	▶
<a href="#">PM-05 Information System Inventory</a>			Passed	1	▶
<a href="#">PM-06 Information Security Measures Of Performance</a>	Designed Effectively	Operating Effectively	Failed	1	▶
<a href="#">PM-07 Enterprise Architecture</a>	Not Designed Effectively	Not Operating Effectively	Failed	1	▶
<a href="#">PM-08 Critical Infrastructure Plan</a>	Designed Effectively	Operating Effectively	N/A	1	▶
<b>AREA OF COMPLIANCE : PCI DSS v3.2.1 (14)</b>					
<a href="#">AC-10 Concurrent Session Control</a>	Designed Effectively	Operating Effectively	N/A	2	▶
<a href="#">AC-25 Reference Monitor</a>	Designed Effectively	Operating Effectively	N/A		▶
<a href="#">AC-24 Access Control Decisions</a>			Failed	1	▶
<a href="#">AC-21 Information Sharing</a>			Passed		▶
<a href="#">AC-03 Access Enforcement</a>					▶

# Forward and Future outlook



- Cloud provides access to a '**continuous compliance**' mindset in risk management
- As technology continues to evolve, **audit quality** increases as organizations deploy automated solutions
- Audit space is swamped with data and there are many **AI opportunities** to intelligently analyze this data and make some sense of it for the end user
- Need for **upskilling** of current audit professionals to increase cloud fluency

The logo for the GRC Summit 2023, featuring the letters 'GRC' in a bold, teal, sans-serif font. The background of the entire slide is a photograph of a modern building at dusk, with palm trees in the foreground and colorful neon lights (blue, red, purple) illuminating the scene. A decorative teal wave graphic with multiple parallel lines flows across the top of the image.

**GRC**

SUMMIT 2023

MIAMI, JUNE 14 & 15

Hosted by MetricStream

EXPERIENCE  
the Power of Connection

**Q & A**



An aerial photograph of Miami, Florida, showing a wide sandy beach on the left, turquoise ocean waves, a green parkway with palm trees, and a dense urban skyline of high-rise buildings on the right. A semi-transparent green wireframe grid is overlaid on the scene, curving from the beach towards the buildings.

**GRC**

SUMMIT 2023

MIAMI, JUNE 14 & 15

Hosted by MetricStream

**Thank You**

 **metricstream**  
thrive on risk™