Pioneering in Cyber Risk Management
Automated Controls Monitoring Powered by OSCAL

November 2023

PwC
ServiceNow IRM Proposal
Presenters

Tom Nash  
PwC | OSCAL Lead  
+44 (0) 7483 378370  
thomas.nash@pwc.com

Sivaram Mallampati  
PwC | Product Owner  
+44 (0) 748 345 2570  
sivaram.x.mallampati@pwc.com

Joshua Kong  
PwC | DevOps Engineer  
+44 (0) 748 333 7329  
joshua.kong@pwc.com
Automated controls monitoring…

- Reduces cost of compliance
- Reduces potential cost of non-compliance
The future of risk management...

Data driven

Extreme scalability

Complex business ecosystems

Real-time alerting

Extreme automation

Deep collaboration

... hinges off a common language of risk
Key commercial sector use cases supported by OSCAL

- Compliance
- Cloud security
- Cyber insurance
- Third party security
- Group posture monitoring
## Key personas impacted by OSCAL

<table>
<thead>
<tr>
<th>Persona</th>
<th>Value driver</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive</td>
<td>Real-time reporting</td>
</tr>
<tr>
<td>Engineer</td>
<td>Machine-readable control instructions</td>
</tr>
<tr>
<td>GRC analyst</td>
<td>Product level compliance insights</td>
</tr>
<tr>
<td>Product owner</td>
<td>Requirements baseline</td>
</tr>
<tr>
<td>Insurer/Regulator</td>
<td>Standardised compliance reporting</td>
</tr>
</tbody>
</table>
## PwC capability overview

PwC has built an OSCAL powered model that codifies risk management processes and enables the following…

<table>
<thead>
<tr>
<th>#</th>
<th>Capability</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Describe security control information in machine-readable format</td>
<td>● Codify your risk management processes and save hundreds of hours of assessors time</td>
</tr>
<tr>
<td>2</td>
<td>Run on-demand security assessments</td>
<td>● Zero marginal cost of assessment</td>
</tr>
<tr>
<td>3</td>
<td>Auto-validate security controls adherence</td>
<td>● Shift security left in the software product development lifecycle and save operational costs</td>
</tr>
<tr>
<td>4</td>
<td>Auto-generate system security plans</td>
<td>● Scale the production of application-level and enterprise-level compliance reports that can be shared with trusted third parties</td>
</tr>
<tr>
<td>5</td>
<td>Auto-remediate policy deviations</td>
<td>● Detect misconfigurations and reduce time to resolution</td>
</tr>
</tbody>
</table>
Demo

In the demo you will see...

- Architecture
- Pipeline
- GRC GUI
- OSCAL schema files
- Remediation

Key features:

- ✓ Environment agnostic
- ✓ Reporting can be shared with trusted third parties
- ✓ Enables risk aggregation within the GRC tool
- ✓ Supports control inheritance
- ✓ Powers automation and data-centricity
Solution conceptual architecture

Key Steps
- OSCAL Catalog
- OSCAL Profile / Baseline
- Control Data Collection
- Assessment Output/Results
- Control Remediation

Key Activity
- Select controls from policies
- Build a baseline for controls (incl. assigning values to the parameters)
- Use automated mechanisms to collect data for the assessment
- Document the System Security Plan (SSP) and output findings into GRC tool
- Integrate with platforms/services to remediate control findings
- Integrate with dashboards for executive reporting and SBOM views

Tools Utilised
- Github
- Docker
- JSON
- Chef Inspec
- Google Cloud Storage
- ServiceNow
- Cloud Service Provider APIs
- Power BI
- SBOM Frameworks

Roadmap
- Third-party Integrations
Demo workflow

1. Google Cloud
   - GCP controls
2. GitHub
   - Pipeline run
3. Google Cloud
   - GCP remediated controls
4. ServiceNow
   - Approval remediation
5. ServiceNow
   - System security plan
6. Google Cloud
   - Profile builder
Thank you