Saviynt

Securing the Energy Sector in Australia

Application control is at the core of the upcoming AESCSF. Learn its key components and how Saviynt can help.

Contents

Introduction

The Australia Energy Sector Cyber Security Framework (AESCSF) is a framework developed by the Australian government to help ensure the security of the country's energy sector. The framework is designed to guide the management of the risk of cyber attacks and other cyber threats to the energy sector and to help ensure that the sector can operate reliably and securely.

In 2021, the program was expanded to include gas markets and non-Australian Energy Market Operator (AEMO) electricity grids and markets. In 2022, the AESCSF was also extended to the liquid fuels sector, to enhance uplift and support consistency across the energy sector.

The AESCSF is based on the Australian Cyber Security Centre's (ACSC) Essential Eight, which is a set of eight high-priority cybersecurity measures that organisations should implement to protect themselves from cyber threats. The framework also incorporates other best practices for cybersecurity in the energy sector, including guidance on securing critical infrastructure and responding to cyber incidents.

The AESCSF is intended to be used by all organizations within the energy sector, including:

- Energy utilities
- Energy infrastructure providers
- Energy service providers
- Natural gas markets
- AEMO electricity grids and markets
- Liguid fuels sector

It is designed to be flexible and adaptable and can be tailored to the specific needs of individual organisations.

Why Is the AESCSF Necessary?

The energy sector is a critical part of the Australian economy, and the security of the sector is vital to the overall security and prosperity of the nation. Cyber attacks on the energy sector could have significant consequences, including disruption to the supply of electricity and other energy sources, damage to infrastructure, and financial losses.

To help prevent these types of attacks, it is important for organisations in the energy sector to have robust cybersecurity measures in place. The AESCSF provides guidance on implementing these measures and helps organisations understand the risks they face and how to manage those risks effectively.

Key Components of the AESCSF

The AESCSF is based on the ACSC's Essential Eight, a set of eight high-priority cybersecurity measures organisations should implement to protect themselves from cyber threats.

These measures are:

- **Application whitelisting:** Only allowing approved software to run on computers and servers.
- **Patching applications:** Keeping software up to date with the latest security patches.
- **Patching operating systems:** Keeping the operating system of computers and servers updated with the latest security patches.
- **Multi-factor authentication:** Requiring more than one form of authentication (e.g., password and security token) to access systems.
- **Restricted administrative privileges:** Limiting the ability of users to install software or make other changes to systems.
- **Implementing application control:** Only allowing approved applications to be installed on computers and servers.
- **Implementing device control:** Restricting the use of removable storage devices (e.g., USB drives).
- **Implementing daily backups:** Regularly backing up important data to prevent data loss in the event of a cyber attack.

In addition to the Essential Eight, the AESCSF also includes guidance on securing critical infrastructure and responding to cyber incidents.

How Saviynt Supports the AESCSF

Saviynt Identity Cloud is the only converged cloud identity platform that provides intelligent access & governance for any app, any identity, and any cloud. The Identity Cloud helps modernize your identity program and build a zero-trust foundation designed to take on new challenges as they emerge.

A key area of the AESCSF includes application control. As more and more energy businesses move sensitive finance, accounting, and payroll data to ERP apps, maintaining continuous compliance becomes more and more critical — and complex. Each app that an enterprise relies on correlates to hundreds of functions, potentially to thousands of people. But it only takes one wrong role with the wrong type of access to create a toxic combination.

It's essential that companies implement high-quality internal controls to prevent users from executing both sides of a transaction — such as being able to create an invoice and pay an invoice. Regulations like Sarbanes Oxley (SOX), for example, exact stiff penalties for Separation-of-Duties (SoD) violations. To meet these challenges, Saviynt offers Application Access Governance - a product purpose-built to meet the Governance, Risk and Compliance (GRC) requirements for the energy sector.

The challenge for many organisations is knowing which GRC capabilities add the most value to an efficient system. Six key capabilities form the nucleus of a solid enterprise-ready solution. Together, they ease the burden on security teams, fast-track the provisioning process, and ensure SoD compliance for the long haul.

They include:

1. Out-of-the-Box Rulesets
2. Fine-Grained SoD Controls
3. Seamless Risk Reporting
4. Fast, Secure Emergency Access
5. Out-of-the-Box Compliance Management
6. Usage Analytics

1 Out-of-the-Box Rulesets

With the rapid adoption of cloud solutions, many organisations rely on ERP applications for critical business functions.

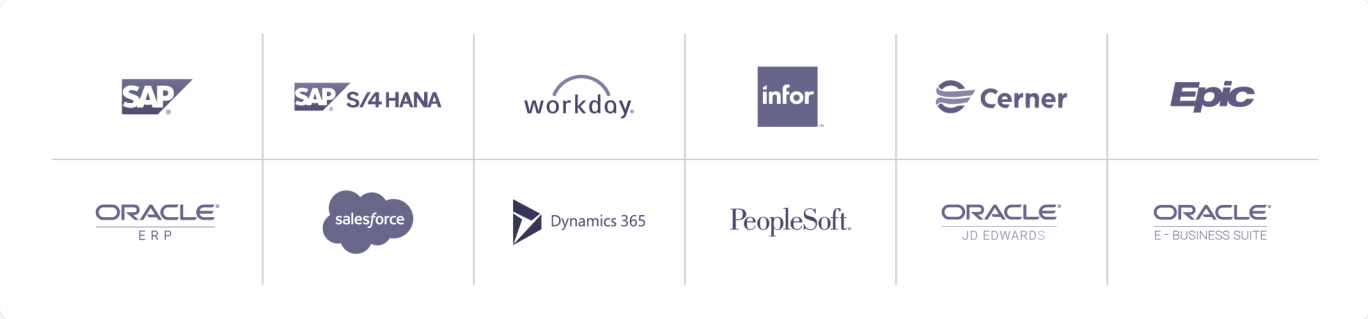
Each business function includes "rulesets" or entitlements that provide internal checks and balances against inappropriate actions. For example, they might prevent an employee who hires vendors from being able to also pay those vendors. Or they might ensure that employees who fill out timesheets aren't also able to approve those invoices. These types of internal controls are the foundation of SoD controls — and good compliance.

However, when you're dealing with ERP applications designed by different software vendors, each with their own security model, each speaking a different security "language," it becomes very difficult to build rulesets from scratch. When you're provisioning many different functions across different apps with different rulesets, how do you maintain healthy SoD between sales orders in Salesforce and Accounts Receivable in Oracle EBS?

Most organisations rely on point solutions or time-intensive, burdensome spreadsheets for in-scope apps. Admins often have to put new users on hold while they follow outdated or manual procedures to hunt down access approvals from other team members.

While other GRC solutions may focus on a single application, like SAP, Saviynt's intuitive workbench comes with built-in out-of-the-box SoD management controls for a long list of ERP applications. Pre-loaded fine-grained rulesets can identify SoD violations across applications deep within the security models of such popular software offerings as SAP, Oracle, Active Directory, Cerner, Epic, and others.

Saviynt ERP Integrations:



2 Fine-Grained SoD Controls

Once you've detected risks, you need a GRC workflow that can show you how many risks are in play, how many are being addressed, which were accepted, and whether they were closed and remediated — both in a single application and across applications.

Historically, this has been a workload-intensive challenge. Some solution providers can get you partly compliant by assessing SoD at the role level, but if your organisation is adding custom roles or functionalities, this level of risk analysis won't be enough for auditors. Effective SoD controls must be "fine-grained" — equipped to identify risks where transactions for critical tasks occur: deep in your applications at the page, function, TCode, Auth Object, or privilege level. Coarse-grained GRC solutions simply can't detect violations at this level.

With AAG, security teams and auditors can detect and confront or accept a wide variety of risks using an extensive built-in library of user-friendly controls. Saviynt's risk scoring tools include static and inherent risk scores assigned to an account and dynamic risk scores derived from usage, behavior analytics, peer group analytics, and data gathered from external systems.

3 Seamless Risk Reporting

While visualizing the risks associated with user access across multiple applications is foundational to a good GRC system, the true value is being able to report on risks continually using a predictive model.

When it comes time to pull the data together for auditors, one of the biggest challenges for risk managers is establishing a clear line of sight into how tasks interact across a wide range of cloud, on-prem, and hybrid applications. How do they run an airtight report for multiple apps with siloed security models? The answer: not very easily.

Ideal reporting covers cross-application rulesets and can identify:

- The risk code
- The functions causing the risk
- A risk priority
- A clear description
- Status — whether it's potential or active

You'll also need to know the user's account information and whether a dashboard is open, in-process, closed, remediated — or assessed and accepted without further action needed.

Most application GRC solutions can help you with one major ERP application, like SAP or Oracle. But Saviynt's comprehensive cross-application governance can manage your SaaS and on-prem applications.

Automated Certifications are scheduled access reviews that determine whether a user's access is still valid or should be discontinued. These controls give organisations the proof needed to make the grade with external auditors.

Effective certification campaigns can certify from various owner types, such as entitlement owner, organisation owner, service account, or user manager.

But there are three predictable stumbling blocks to certifying correct access:

Joiners, Movers, and Leavers: Security teams are usually very good at providing access as users join or move positions within the company. Unfortunately, "leavers" often take their access with them when they go.

Rubberstamping: When admins need to conduct separate access certification campaigns for standard and privileged access, they may copy other users' access to prevent a logjam.

Loss of Productivity: Access reviewers often get mired during audits in time-consuming cross-application complexity or multiple SoD risks.

With Saviynt's intelligent access request capabilities and prevent-and-detect risk analysis, your teams can reduce the number of potential violations found during user access reviews and ensure your organisation stays focused on the riskiest exposures first.

4 Fast, Secure Emergency Access

The needs of a business can change quickly — and attack surfaces can expand faster than the ability to defend them.

When users request elevated or 'firefighter' permissions to critical resources and sensitive data, time is of the essence. How quickly can your security teams gather all the information they need to provide privileged access to an application? How many people are involved in providing the information? When the work is completed, are you immediately de-provisioning privileged sessions?

To avoid chokepoints and ensure smooth audits, admins need a solution that rapidly enables real-time emergency access with a clear line of sight into what users are doing with that access — and the ability to raise the drawbridge fast when users perform unauthorized activities.

With Saviynt AAG Emergency Access Management and Log Reviews, emergency capabilities can be added as a role with existing credentials or as a customized ID. With an emergency access role, we use existing credentials to grant additional access to that role. With an emergency access ID, the user doesn't have existing credentials, so organisations set up IDs with an approved set of access.

With either access type, admins need to be able to monitor sessions and immediately revoke access to eliminate standing privileges or orphaned identities. With AAG, automated session monitoring gives admins the flexibility they need to implement time-bound and customized access that expires when the session is over.

5 Out-of-the-Box Compliance Management

With the rapid adoption of cloud solutions, many organisations rely on ERP applications for critical business functions. One of the primary reasons for deploying an application GRC solution is to maintain regulatory compliance and ensure you have strong cybersecurity controls in place. How many times each year do you have to audit the same access controls for different compliance regulations? How many different solutions do you need to make sure those controls work — and how much time and money is that costing you?

Most GRC technologies can assist with compliance requirements for only certain critical apps. Integrating application governance with an IDM platform becomes complex, burdensome, and time-intensive if you have multiple regulations to meet across multiple applications. With Saviynt's out-of-the-box compliance reporting, your security teams can vastly simplify the compliance review and management process.

6 Usage Analytics

Analytics should form the basis of configuring tests that can run on an ad-hoc or scheduled basis — and should be able to be filtered by application or by specific regulation.

With AAG's Usage Analytics, you can generate compliance reports against a wide range of industry-specific requirements, including SOX, NIST, ITGC, FINRA, PCI-DSS, and many more. Healthcare organisations, for example, can scan user activities for HIPAA violations. Companies that do business in Europe can check risks against GDPR rules. Configuration testing can be run on your schedule and filtered by application or by regulation. Saviynt's built-in, one-click reporting saves resources, streamlines audit preparation, and ensures ongoing compliance.

Saviynt converges all of these security tools into one dashboard, empowering internal auditors and risk managers with a comprehensive, automated, and seamless line of sight.

Implementing the AESCSF

Organisations in the energy sector are encouraged to adopt the AESCSF and to use it as a guide for implementing effective cybersecurity measures. The framework is designed to be flexible and adaptable, and can be tailored to the specific needs of individual organisations.

To implement the AESCSF, organisations should follow the following steps:

- **Review the AESCSF:** Familiarize yourself with the framework and understand its key components.
- **Assess your current cybersecurity posture:** Determine your current level of cybersecurity and identify any areas that need improvement.
- **Develop a cybersecurity plan:** Use the AESCSF as a guide to developing a plan.

ABOUT SAVIYNT

The Saviynt Identity Cloud converges IGA, granular application access, cloud security, and privileged access into the industry's only enterprise-grade SaaS solution.

Saviynt PAM solution is delivered via an agentless, zero-touch cloud-architecture so you can quickly deploy privileged access capabilities. Achieve zero-standing privileges with just-in-time (JIT) access and intelligent risk insights to power your PAM program.

Saviynt

Headquarters, 1301 E
El Segundo Bl, Suit e D, El Segundo, CA
90245, United States

310. 641. 1664 | info@saviynt.com
www.saviynt.com