TURNKEY CONSULTING
delivering SAP® security solutions

Transport for London

Achieving Business Ownership of Risk and Compliance

Profile

Transport for London (TfL) was created in 2000 and is the integrated body responsible for the Capital's transport system. Its main role is to implement the Mayor's Transport Strategy for London and manage transport services across the Capital for which the Mayor has responsibility.

Challenge

As a publicly funded body, Corporate Governance is critical to Transport for London. Because of this they chose to implement SAP Governance, Risk and Compliance (GRC) across their systems.

"GRC had already been implemented before I took on this role," explains Tobias Cowling. "My predecessor had appointed Turnkey Consulting as the project lead and together they had identified the business benefits they wanted to achieve from the project. We wanted to reduce the cost of audits, ensure compliance, and be able to add on extra packages like compliant user provisioning, and super user privilege management."

In addition, TfL wanted to transition the responsibility for compliance away from the SAP Security team, pushing responsibility back out to business owners. The idea here is to get the business bought in to the process and for them to identify what their risks are.

Solution

Turnkey Consulting was appointed as the project managers behind the solution. They worked closely with TfL's senior management and Security and Authorisations team to develop the vision and establish the groundwork and key principles. Their shared vision was to implement SAP GRC across the business, with a senior management Governance Council to provide the lead and a network of GRC gatekeepers to ensure that all business units identified and owned their own security risks.

> *"We've 100% transitioned out the responsibility for access to the business units, and now it's no longer the security team's responsibility which is as it should be."*

Tobias Cowling
SAP Security and Authorisations lead for Transport for London

Highlights:

- Business units empowered to take control of user risk and compliance issues
- A change in mindset achieved through involvement of business risk owners in the project
- Network of gatekeepers, training and Governance Council now in place
- Roles fully aligned with risk ruleset to remove segregation of duties risk
- Compliance has increased from 60% to 87% and still improving
- Now only takes 15 minutes, instead of days, to assign a new role

The project was then taken in-house and the final stages were implemented by the TfL SAP Security team. Turnkey Consulting remains active in supporting TfL and provides on-going technical assistance and training.

Network of gatekeepers

TfL now has in place a network of approximately 95 SAP role gatekeepers that cover all of the business units within the company. For each unit they have finance, procurement and HR gatekeepers and all of them are trained to use the GRC application.

"Turnkey identified that we needed key people trained to take responsibility in security and access," says Cowling. "Once the gatekeeper network was set up we removed the ability of TfL users to request access directly with my team. In its place we have the gatekeepers who make decisions about access for their functional areas. We supported the process by building a new area on our intranet detailing what GRC is, what the gatekeepers' role is, and a mechanism to identify a named business contact's area of responsibility. This helps the user community to recognise the appropriate approval party."

Training and responsibility for risk

Thorough training was critical to the success of the project. All gatekeepers are fully trained in the principles of GRC, the Risk Analysis and Remediation tool (RAR) and in how to use the system. As part of the training the gatekeepers perform simulations on positions and users to assess the business risks that changes might represent.

Cowling expands, "We are making sure that all business units have got an "eyes wide open" approach to the sort of access they're granting, and they understand the associated risks. By taking responsibility for GRC they are going through the whole journey: identifying what the risks are, how they can avoid them and how to put controls in place to mitigate any areas of concern."

After completing the initial groundwork, Turnkey provided training to the SAP Security team to support them in bringing the project in-house. "It gave my team the confidence to use the tool, navigate around it and execute all necessary functions," explains Cowling.

Corporate governance and the Governance Council

Initially TfL struggled to get people from the business on board. The solution was to set up a Governance Council and bring in senior business people to drive corporate governance down through their departments. As a result of the project, corporate governance is no longer viewed as an IT project but as a core strand of the business with a top-down approach.

This is what Cowling hoped to achieve: "Now corporate governance is completely business driven which makes us an IT service provision rather than trying to drive it, says Cowling. "The Governance Council has meant that we've been able to show that the gatekeepers have a very important job and they have the time and the responsibility to carry out this role."

Rule set

Turnkey worked closely with TfL to redesign the rule set and align the TfL access permissions to this. The default rule set was not customised to TfL's operations and, together with TfL business representatives, Turnkey completely reviewed and redesigned it to reflect TfL's business and operating risks.

"Turnkey took us away from the standard SAP rule set, which was not appropriate, and tailored it for Transport for London. They helped us to find what our real risks were," says Cowling.

Benefits

Business ownership of risks: It was a major business challenge to empower the individual business units to take control of their user risk and compliance issues. The tailored SAP GRC system developed by Turnkey has supported this through the network of gatekeepers, training and the Governance Council. Following training, these Gatekeepers now make informed access decisions. Cowling explains, "We've 100% transitioned out the responsibility for access to the business units, and now it's no longer the security teams responsibility which is as it should be."

Improved compliance: Under the new system TfL has gone from averaging 60 - 70% compliance to achieving more than 87% and this is still improving. The SAP Security team do spot checks, but the responsibility for managing risk in user access lies with the gatekeepers. "The gatekeepers are doing the simulations and making sure there are no additional problems in the system," Cowling explains.

Efficiency in dealing with access requests: TfL has significantly reduced the turnaround on user access requests for the business. Under the new system it now only takes 15 to 20 minutes to assign a new role onto the system once the request has been received from a gatekeeper. There is then an overnight process that releases these roles, as TfL currently operates an indirect role assignment policy. Previously it took the SAP Security team three to four hours to deal with individual requests, and as potential compliance issues needed to be checked, combined with the volume of calls received by the business, the provision of user access used to take up to 2 to 3 days.

Summary

Achieving buy-in from the business units was critical to the success of the project. It is important that the business has an understanding of why access can potentially be denied, and this leads to fewer complaints. Cowling concludes, "The best people to make the decisions about access are the ones who are ultimately going to bear the brunt of the risk to the business."

Cowling describes working with Turnkey, "They have an excellent understanding of GRC and security practices and principles. I've been very happy with the consultants we had on site. They understand what we've actually delivered here as a partnership. I trust them and that's important to me."