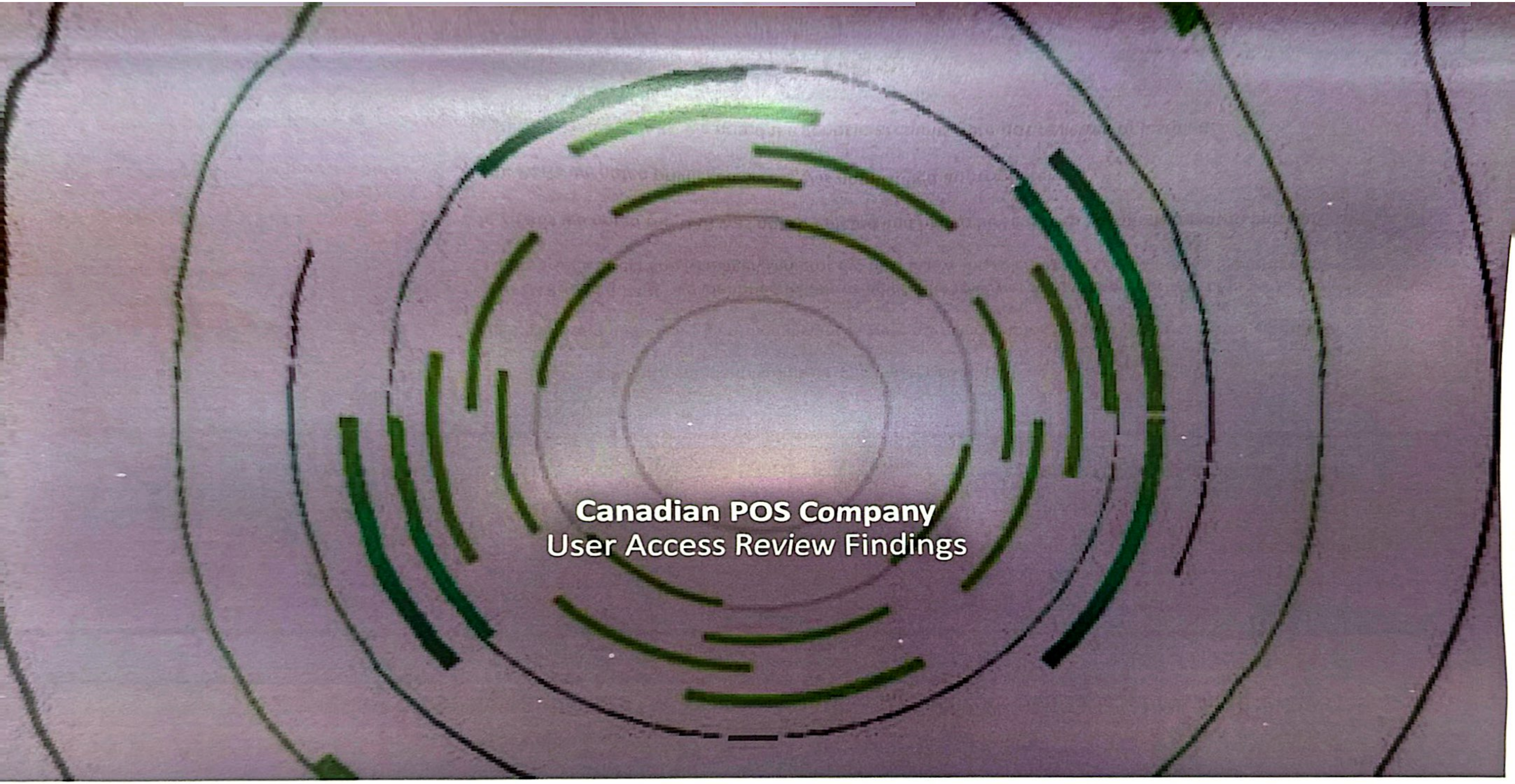

Canadian POS Company
User Access Review Findings

Scanned with CamScanner

User Access Review Findings

- Shiksha reviewed a total of 60 UARs and PARs. Of these we identified issues with 50 (83%) which would have led to reportable deficiencies if found by external Auditors.

	Reviewed	Failed UARs/PARs	Failed UARs/PARs excl. generic account issues
UAR	18	14 (77%)	12 (67%)
PAR	42	36 (86%)	23 (55%)
Total	**60**	**50 (83%)**	**35 (58%)**

	Reviewed	Issues Identified (excluding review of generic accounts)
UAR	18	19 Unique findings (excl. generic accounts)
PAR	42	34 Unique findings (excl. generic accounts)
Total	**60**	**53 Unique Findings (excl. generic accounts)**

Key Themes Identified	Impact (i.e. identified on X / Y / Z UARs/PARs)
Self review	In 6 UARs and 8 PARs, we identified users who had reviewed their own access
Corrective actions not being performed	In 4 UARs and 4 PARs, we identified instances were users flagged for removal were not removed prior to our review
Inappropriate reviewers	In 9 UARs and 6 PARs, we identified instances where the reviewer was not appropriate to be performing the review i.e the user's direct line Manager/Director did not review the role but a 3rd personnel reviewed the role
Incomplete UARs	In 2 PARs we noted the UAR was not completed and had to be sent back to management to finish off
Lack of justification for privileged accounts	In 14 PARs we noted privileged access was not justified appropriately
Lack of review of generic accounts	In 10 UARs and 25 PARs, we noted the generic accounts were not reviewed or justified.

Scanned with CamScanner

Corrective items

- Types of corrective items performed to properly complete the UAR

Corrective items	Details
Rework following deficiencies identified	In total across all deficiency types, there were 88 findings in 36 PARS and 14 UARs identified requiring multiple re-evaluation of attributes following BPO rework. Excluding generic accounts, there were issues identified in 23 PARs and 12 UARs (35 total, 58%).
Privileged Account Justification	Each privileged user or elevated access role required obtaining sufficient justification to deem the account's appropriateness to hold the elevated role / access. This was often not documented in the UAR / PAR which required multiple follow-ups with control owners
Control Owners Knowledge of Process	Although educated on the process, some control owners did not take into account the impact of control failures (e.g. SOD conflicts, wrong approvers, incomplete user listings and UAR corrective actions).
Generic account testing	Most Control Owners did not know that generic accounts had to be tested and were not familiar on how to test these accounts The testing of generic users was absent in 10 UARs and 25 PARs, and it had to be redone by the Control Owners

Scanned with CamScanner

Next steps

- Takeaways and recommendations

Key Themes Identified	Recommendations
PAR and UAR process	Educate BPOs on the process and key testing attributes
Large volumes and detailed reviews	Implement a similar template throughout all review controls and leverage tools existing at LSPD (e.g. replicate Guillaume's macro on "history of edited cell" in all reviews) Consider automation of the process to extract the data and attributes to test
Risk related to external consultants	Business knowledge being limited, ensure to have a Management resource support the consultant in the process of review instead of a resource in Internal audit. Ensure the management resource reviews the work of the consultant (this would have helped with 3 self reviews not caught as part of the review process).
Identification by BPOs of exceptions	Consider populating a delegation matrix for backup reviewers Add a testing attribute over the justification of the review done by the backup resource
Timing of reviews	Opt to perform the reviews prior the period end to apply corrective measures following the process review
Post mortem	Ensure that results are shared with BPOs and lessons learned shared

Scanned with CamScanner