SMU
SINGAPORE MANAGEMENT UNIVERSITY

Deployment of Privileged Access Management for System Administrators

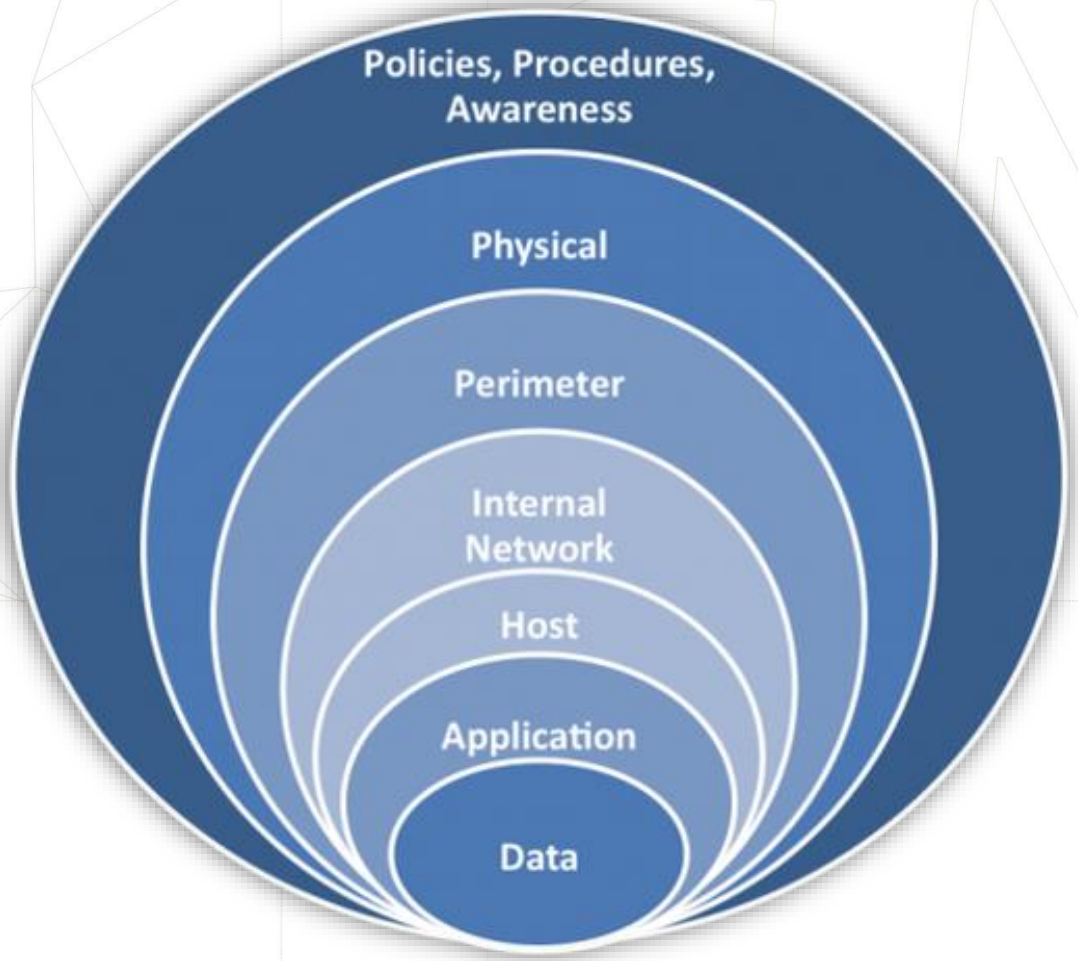
Presented by

Lim Ken Lee
Ho Soo Ming

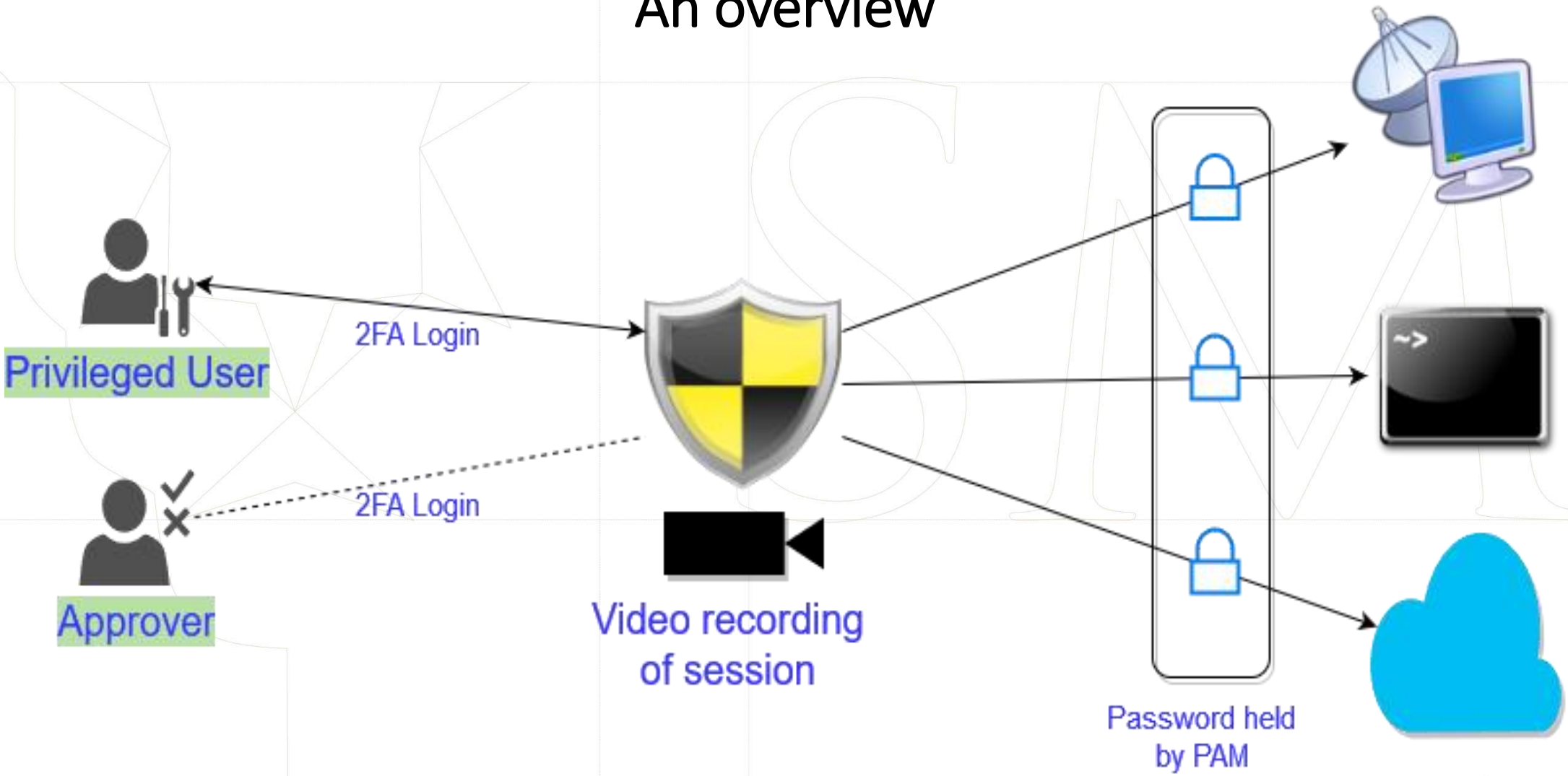
Let's make SMU safer by restricting administrative access

SMU
SINGAPORE MANAGEMENT UNIVERSITY

How PAM achieves this



An overview

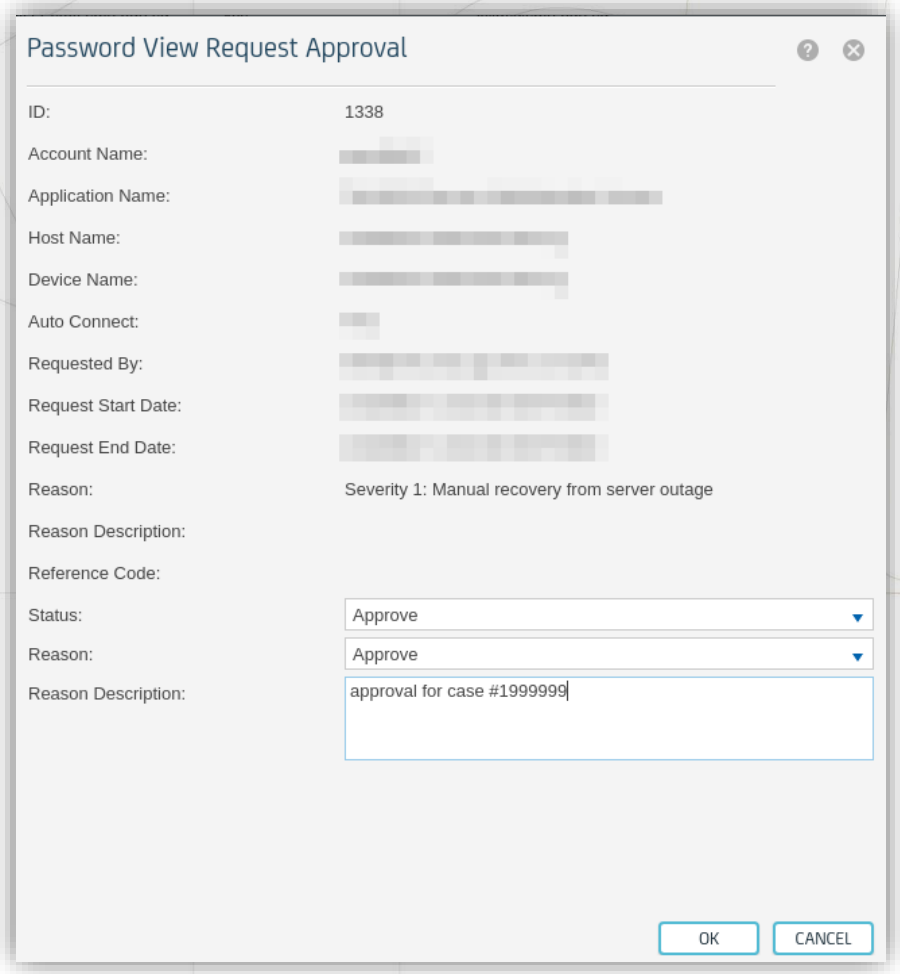

Privileged User
2FA Login
Approver
2FA Login
Video recording of session
Password held by PAM

We are able to address these issues now

1. Lack of 2 factor authentication
2. Approval Workflow
3. Provide audit records of access
4. Administrative access not monitored

2FA

Access approval



SMU
SINGAPORE MANAGEMENT UNIVERSITY

Auditing

View Password Requests

Report Generated: 2018/07/24
Time Zone: Asia/Singapore
Date Range 2018/07/24 to 2018/07/24

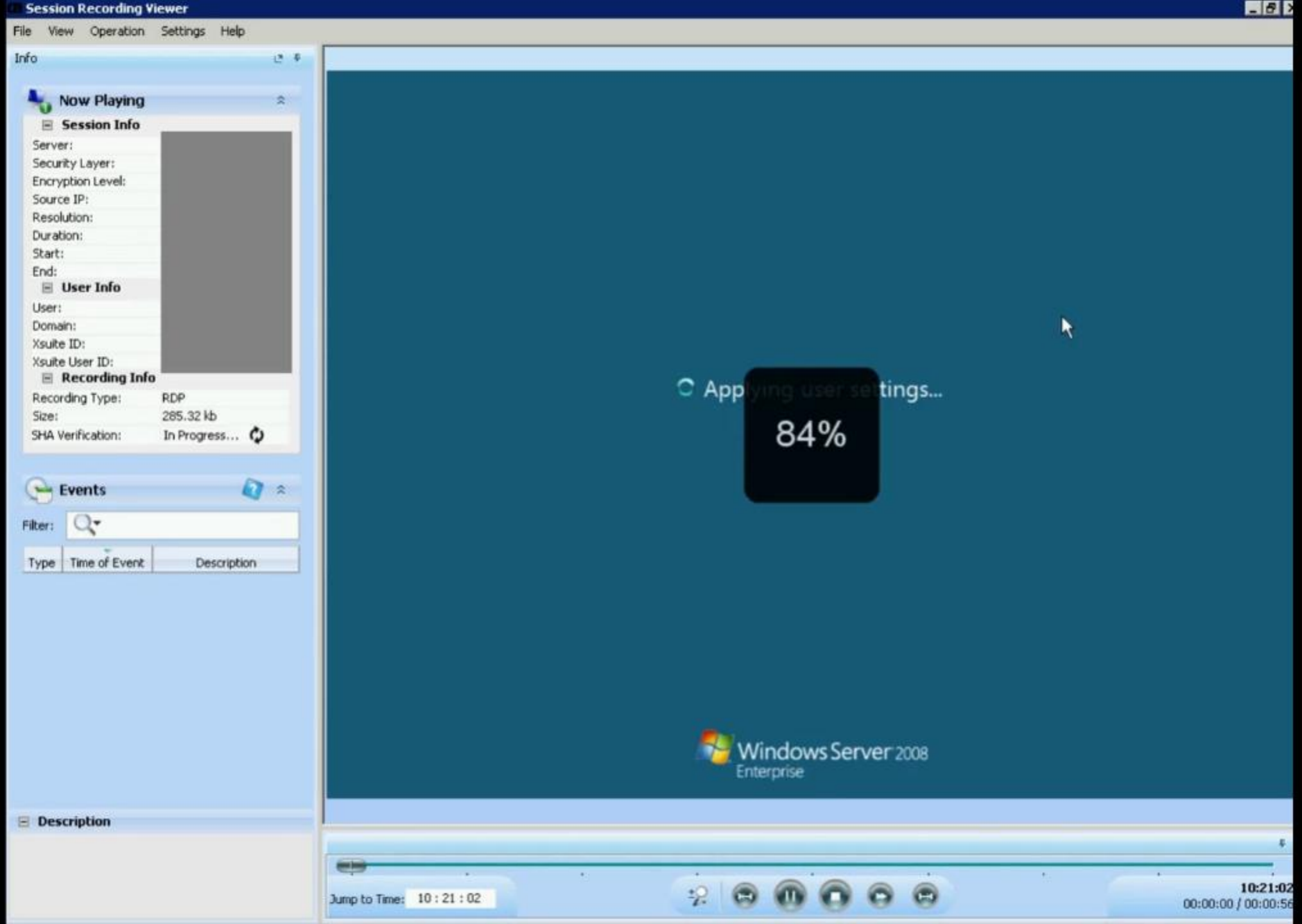
Sorted by: Date
Total entries: 6

Date	Hostname	Application	Account	Reason	Details	Code	Requestor
2018/07/24 17:06	[redacted]	[redacted]	[redacted]	Other	[redacted]		[redacted]@smu.edu.sg
2018/07/24 16:04	[redacted]	[redacted]	[redacted]	Other	[redacted]		[redacted]@smu.edu.sg
2018/07/24 14:41	[redacted]	[redacted]	[redacted]	Other	[redacted]		[redacted]@smu.edu.sg
2018/07/24 09:02	[redacted]	[redacted]	[redacted]	Other	[redacted]		[redacted]@smu.edu.sg
2018/07/24 08:34	[redacted]	[redacted]	[redacted]	Other	[redacted]		[redacted]@smu.edu.sg
2018/07/24 08:20	[redacted]	[redacted]	[redacted]	Other	[redacted]		[redacted]smu.edu.sg

SMU
SINGAPORE MANAGEMENT UNIVERSITY

Access recording

SMU
SINGAPORE MANAGEMENT UNIVERSITY


Session Recording Viewer
File View Operation Settings Help
Info
Now Playing
Session Info
Server:
Security Layer:
Encryption Level:
Source IP:
Resolution:
Duration:
Start:
End:
User Info
User:
Domain:
Xsuite ID:
Xsuite User ID:
Recording Info
Recording Type: RDP
Size: 285.32 kb
SHA Verification: In Progress...
Events
Filter:
Type
Time of Event
Description
Description
Applying user settings...
84%
Windows Server 2008
Enterprise
Jump to Time: 10 : 21 : 02
10:21:02
00:00:00 / 00:00:56

Issues

Your password or your life

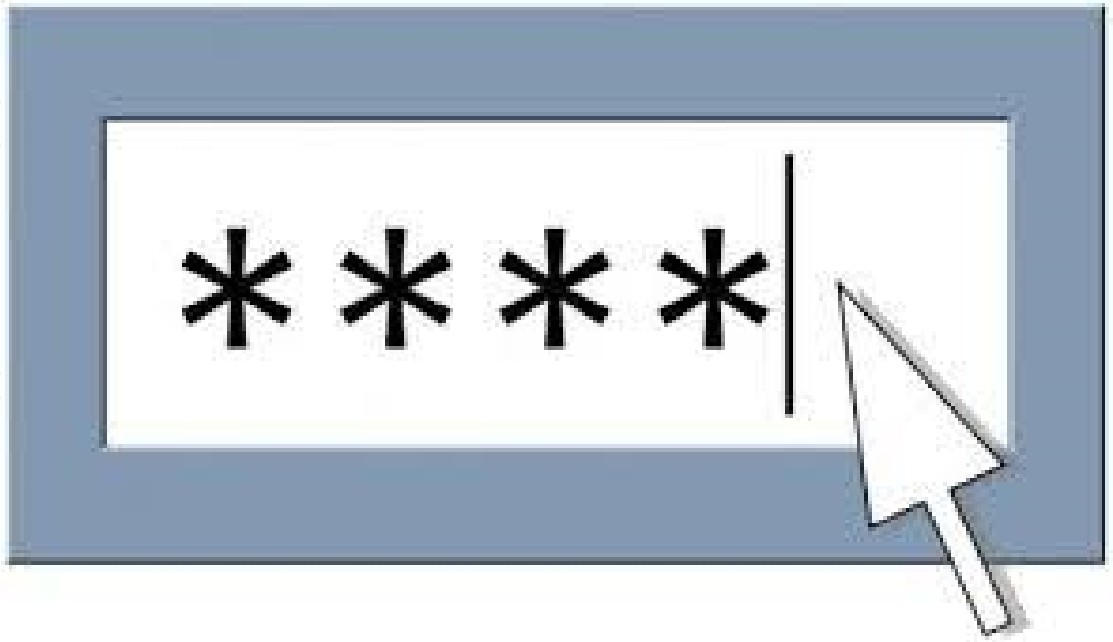
Not a one size fits all deployment

Approver unavailable == No access

Key takeaways

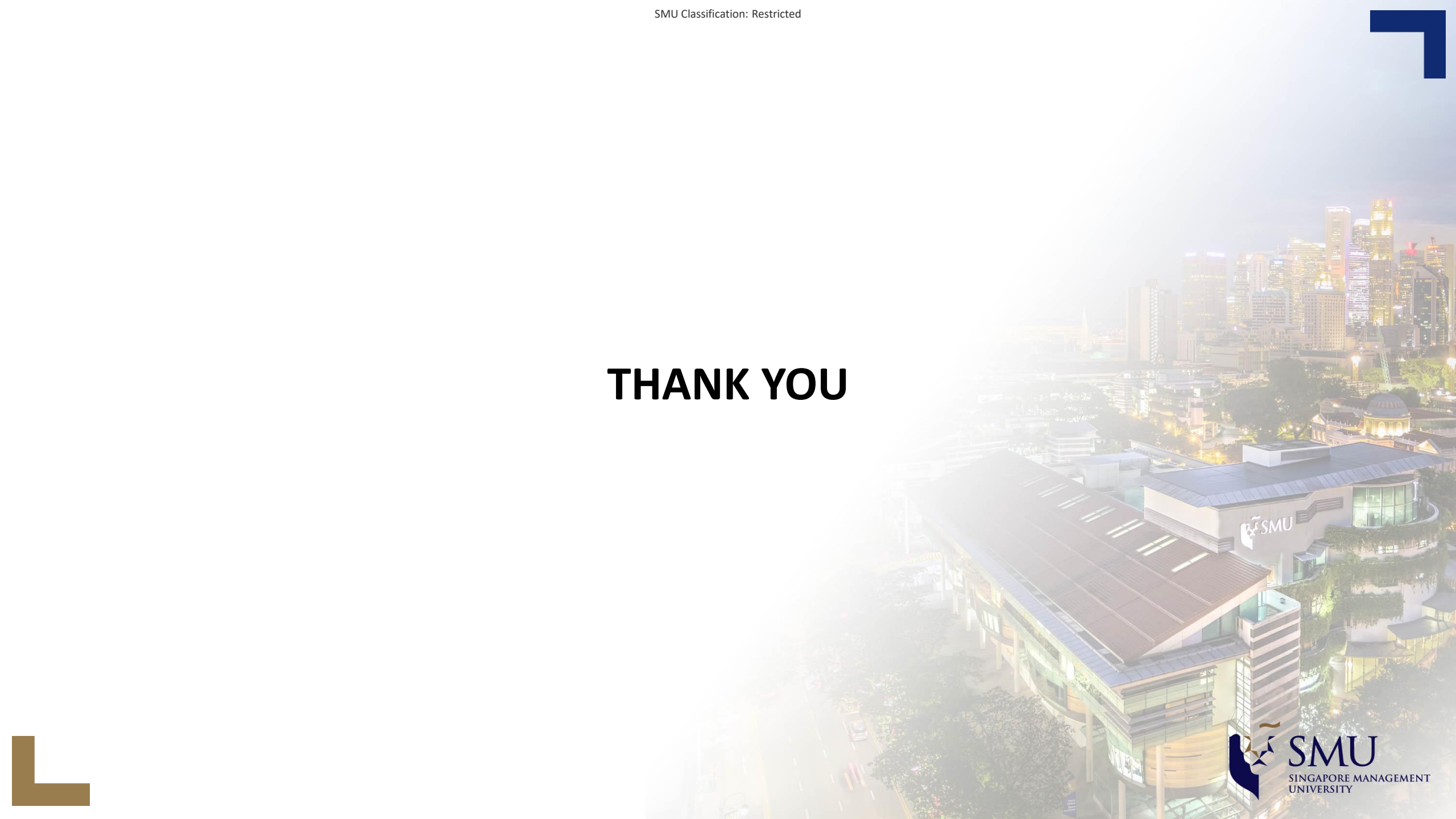
Administrative accounts are the greatest asset, secure it

Use a PAM to provide access without revealing password



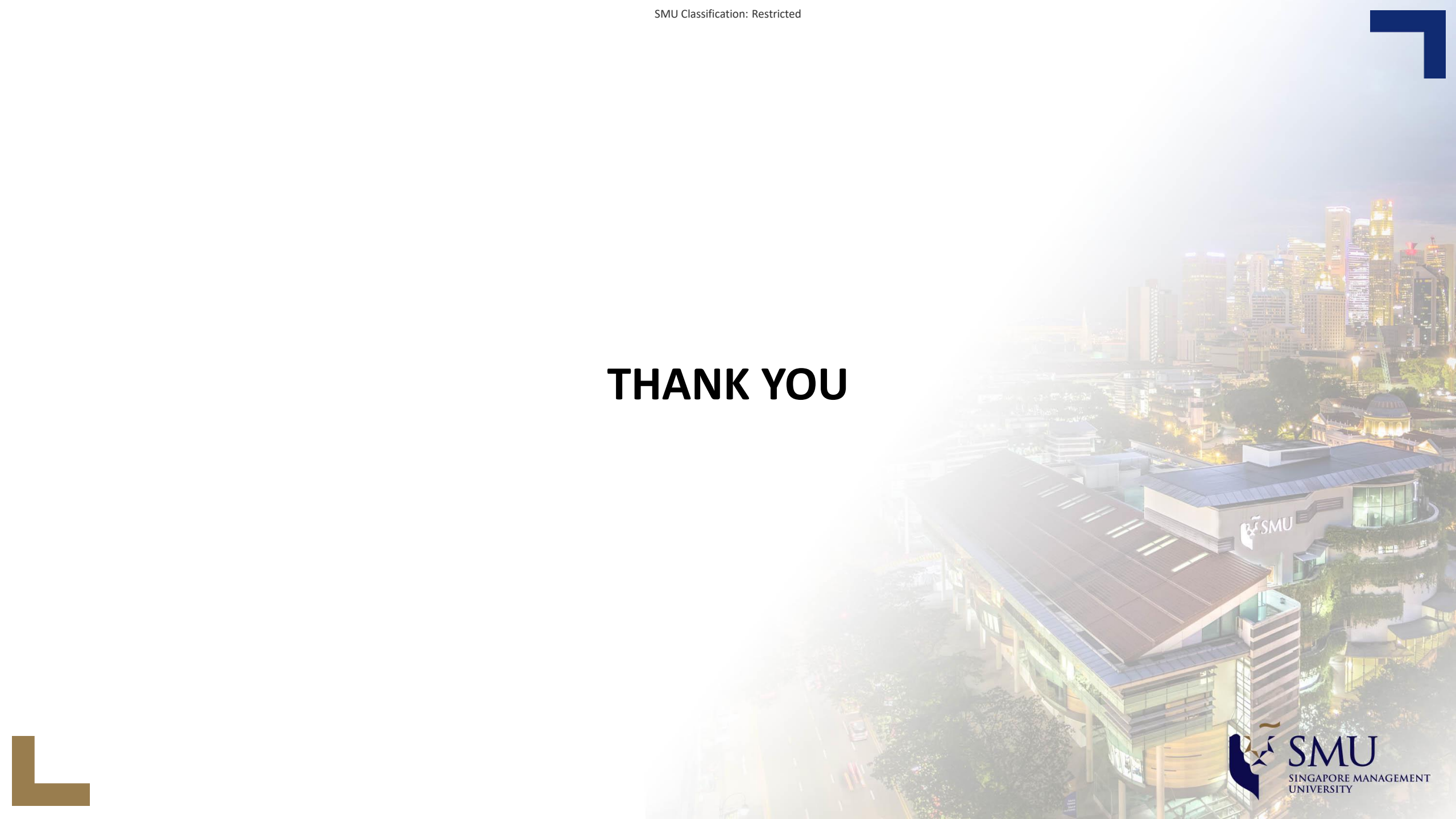
And finally a "break glass account"

THANK YOU



SMU
SINGAPORE MANAGEMENT UNIVERSITY

THANK YOU



SMU
SINGAPORE MANAGEMENT UNIVERSITY