CREATING ORDER OUT OF CHAOS – A PRAGMATIC APPROACH TO USER SECURITY

SESSION 6028
7 Nov 2018
1 – 2pm

PRESENTER

Ian Holmes

Senior Manager, Student Systems Projects

University of Queensland

i.holmes@uq.edu.au

UNIVERSITY OF QUEENSLAND

Staff – 6,703 FTE

Students –

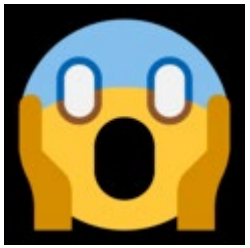
Undergrad –	about 35,860
Postgrad –	about 16,470
Total –	about 52,330

15,430 from >135 countries

UQ & ORACLE

CS 9.2
P/Tools 8.56
Oracle 12c

IAN, I HAVE A JOB FOR YOU …



Review CS user security

Largely by yourself

Implement any changes for CS9.2 go-live

OVERVIEW

1. BACKGROUND
2. SECURITY CONCEPTS OVERVIEW
3. THE REVIEW
4. THE OUTCOME
5. CURRENT SITUATION

BACKGROUND

SECURITY CHANGES OVER TIME

WHERE WE BEGAN

Implementation of SA7.6 ANZ in 2000 with Go-Live in January 2001.

A need/desire to tightly control user security, BUT …

With hindsight, a certain amount of naivety with respect to the security maintenance overhead for a student system that was far more complex than the legacy system.

CS 8.9 & THE BENEFIT OF HINDSIGHT
If only we knew in 2000 what we knew in 2007!

Major review of SI-net security as part of upgrade to CS 8.9 in 2007.

WHY?

Maintenance of original fine-grained approach to user security had become a very significant drain on support team resources.

OUTCOME?

Complete rebuild of user security.

Significantly less fine-grained.

Aligned with training modules (areas of functionality).

CS9.2
THE GROUND HAS MOVED UNDER OUR FEET

Since 2007 user security had become more complex over time and thus increasingly difficult to maintain.

Significant change to Support Team's structure and duties, and reduction in team size.

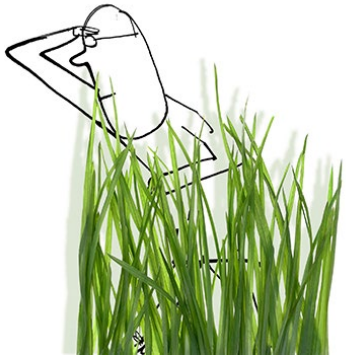
Significant change of approach to user training.

Audit concerns.

SECURITY CONCEPTS OVERVIEW

ROLES
PERMISSION LISTS
…

LET'S STAY OUT OF THE WEEDS



Our discussion does not require a detailed understanding of the security structure in the CS software, but …

A user's access to the CS pages is controlled via User Profiles, Security Roles and Permission Lists.

Permission Lists are the building blocks of user security authorisation.

A PL grants a degree of access to a particular combination of PeopleSoft elements.

BUILDING IT UP

A **Security Role** is a collection of PLs.

You can assign one or more PLs to a role.

You can assign a given PL to multiple roles.

A **User Profile** is a definition that represents one CS user.

Each user is unique.

Each Role that's assigned to a given user profile adds its Permission List(s).

BUT WAIT, THERE'S MORE

CS has a second layer of security – **Row Level** security.

Roles and PLs determine the pages a user can access.

RL security determines what actions a user can perform when they reach a specific page and/or what data set can these actions be performed upon.

RL security is only relevant to a subset of pages in SI-net.

THE REVIEW

WHAT DID WE FIND?

ADU 7-9 NOVEMBER 2018

WHAT WE FOUND

Review revealed drift / evolution to complexity.

For example, there were numerous Roles assigned to 4 or fewer staff.

WHAT WE FOUND

168 Security Roles

144 Permission Lists

Mostly 1xSR = 1xPL

WHAT WE FOUND – SECURITY ROLE EXAMPLES

UQ SR Course Catalogue	UQ SR Program/Plan Change
UQ SR Course Catalogue Correct	UQ SR Program/Plan Correct
UQ SR Enrolments	UQ SR Student Group
UQ SR Exclusions Officer	UQ SR Student Group Correct
UQ SR Maintain Class Meetings	UQ SR Scholarship Bank/Correct
UQ SR Maintain Grades	UQ SR Scholarship no Bank Info
UQ SR Mass Block Enrolment	UQ SR Update Degree
UQ SR Prog Info/C List Approve	UQ SR Viewer
UQ SR Prog Info/C List Update	UQ SR Viewer RRTD
UQ SR Academic Standing	UQ SR Awards OUE
UQ SR Awards Grad School	UQ SR CHESSN Read Only

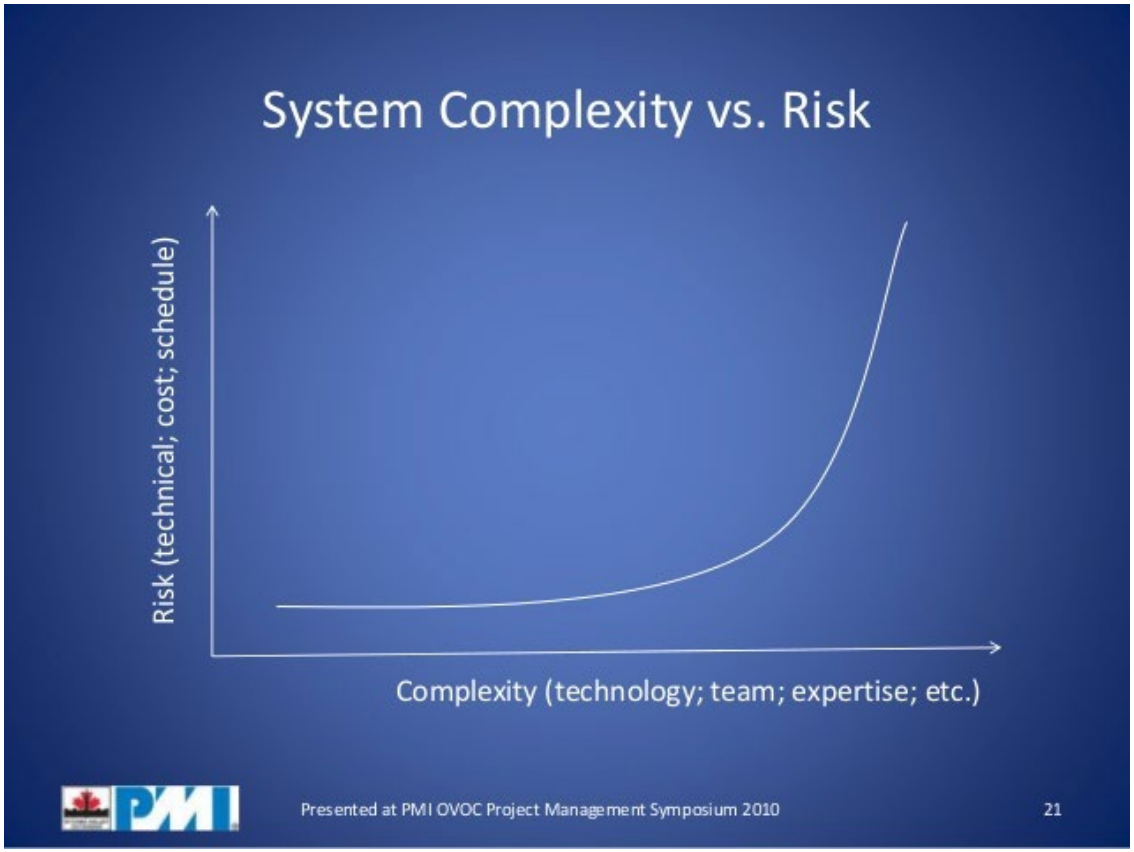
WHAT WE FOUND

Enrolment security not aligned with Roles.

Massive variability in assignment of ADM and PROG Actions. No alignment with Roles.

Transcript security – access to Official Transcript too widespread.

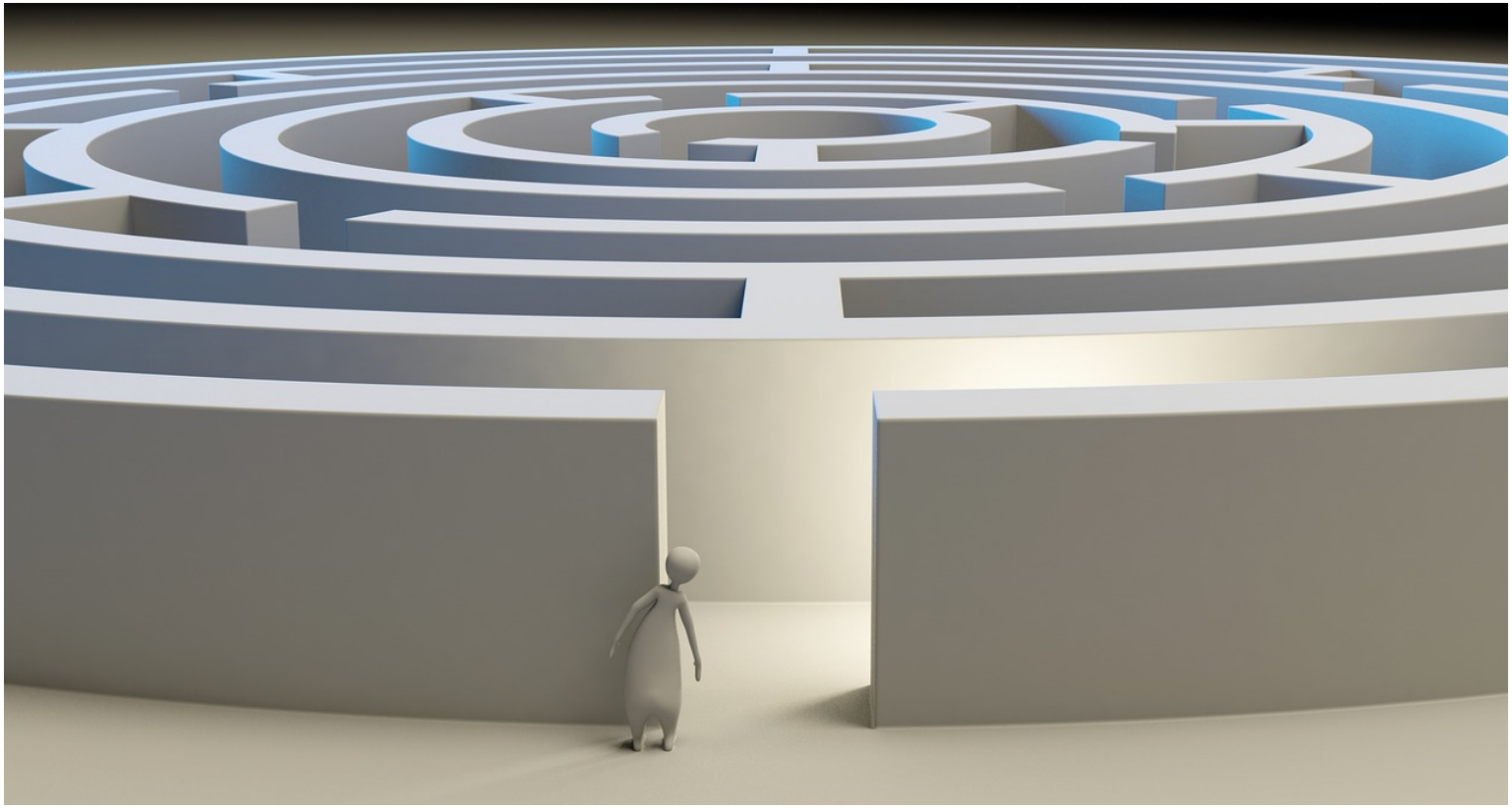
COMPLEXITY = RISK



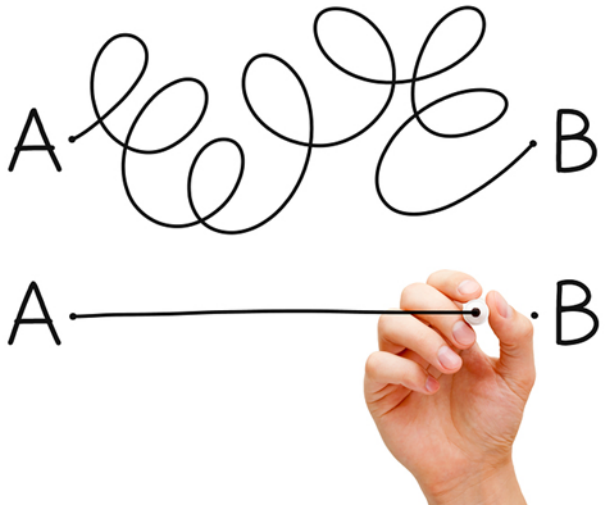
THE OUTCOME

WHAT DID WE DO?

INITIAL FEELING



WHAT WE NEEDED TO ACHIEVE



OVERCOMING THE COMPLEXITY

Pop Quiz!

What is it on the left? Who is it on the right?

OR SOMETIMES YOU JUST HAVE TO . . .

AFTER REVIEW, DECIDED TO FOCUS ON

- Permission Lists
- Security Roles
- Row Level Security – BUT only for key areas of risk.

DON'T GO THERE

Limited time/resources for testing security changes.

OLA-related security – don't touch!

PERMISSION LISTS

- If it ain't broke, don't fix it.
- **Simplification via amalgamation** – reduction in number via amalgamation of related PLs.
- Done with SQL scripts rather than manual rebuilding.

HCCPUQADIASRESTRICT AD Admissions IAS Restricted	HCCPUQADINTLENTRY	HCCPUQADRECRATES	HCCPUQADRECCATTBL	HCCPUQADWAIVERCODEUPDATE

SECURITY ROLES

Simplification and **alignment** with key staff roles.

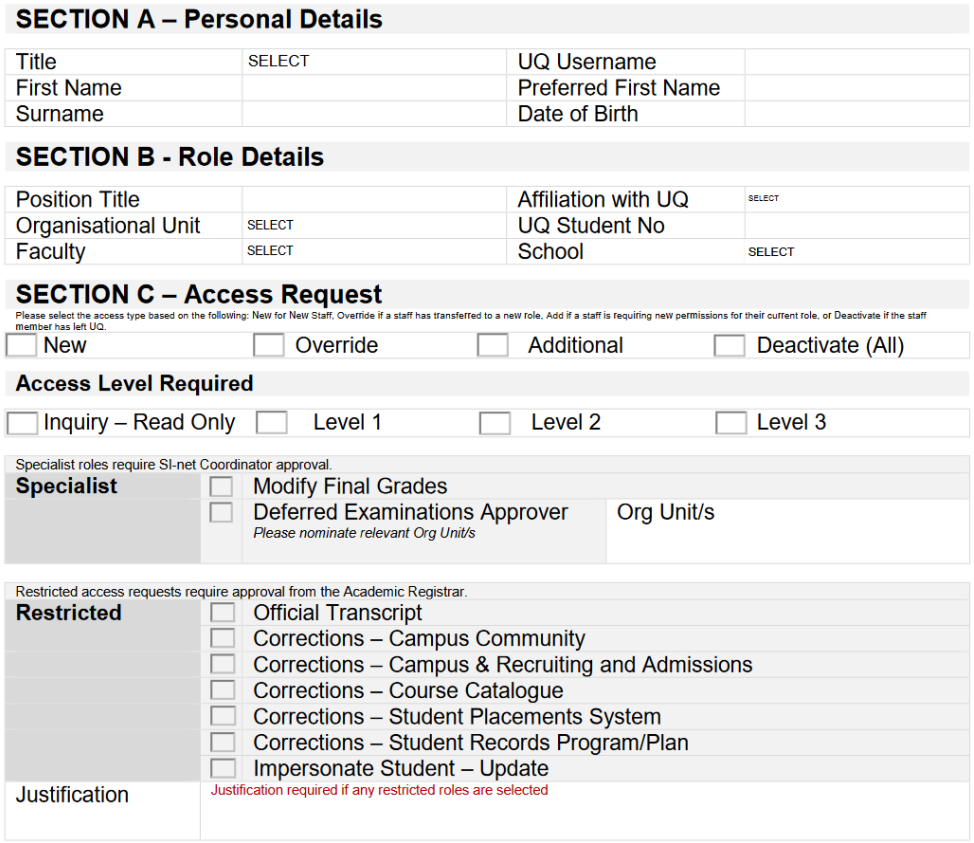
Make use of **Dynamic Roles** where possible.

SECURITY ROLES – THE 'RISKY' ONES

Split out the 'high risk' (contentious) Roles – simpler to approve, monitor and remove.

UQ SA Official Transcript	UQ SA Student Fees Refunds
UQ SA Acad Progression	UQ SA Scholarships High
UQ SA Exams	UQ SA Scholarships Approver
UQ SA Graduations High	UQ SA Awards OUE
UQ SA IAS Restricted	UQ SA Enrolment Page
UQ SA Student Fees High	UQ SA AD CC Correction
UQ SA Student Fees FBS	UQ SA SR Crse Cat Correction
UQ SA Student Fees FBS High	UQ SA SR Prog Plan Correction

SECURITY ROLES – APPROVAL & ASSIGNING



SECTION A – Personal Details

Title	SELECT	UQ Username	
First Name		Preferred First Name	
Surname		Date of Birth	

SECTION B - Role Details

Position Title		Affiliation with UQ	SELECT
Organisational Unit	SELECT	UQ Student No	
Faculty	SELECT	School	SELECT

SECTION C – Access Request

Please select the access type based on the following: New for New Staff, Override if a staff has transferred to a new role, Add if a staff is requiring new permissions for their current role, or Deactivate if the staff member has left UQ.

☐ New ☐ Override ☐ Additional ☐ Deactivate (All)

Access Level Required

☐ Inquiry – Read Only ☐ Level 1 ☐ Level 2 ☐ Level 3

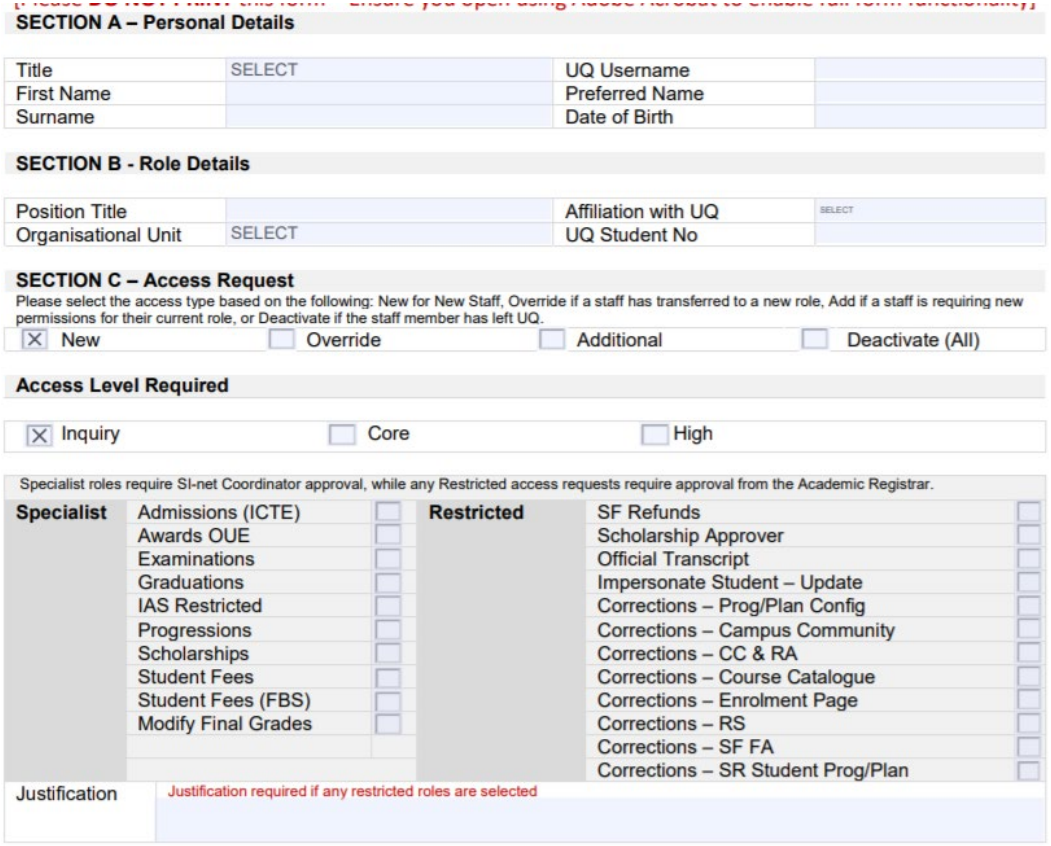
Specialist roles require SI-net Coordinator approval.

Specialist	☐ Modify Final Grades	
	☐ Deferred Examinations Approver *Please nominate relevant Org Unit/s*	Org Unit/s

Restricted access requests require approval from the Academic Registrar.

Restricted	☐ Official Transcript
	☐ Corrections – Campus Community
	☐ Corrections – Campus & Recruiting and Admissions
	☐ Corrections – Course Catalogue
	☐ Corrections – Student Placements System
	☐ Corrections – Student Records Program/Plan
	☐ Impersonate Student – Update
Justification	Justification required if any restricted roles are selected

SECURITY ROLES – APPROVAL & ASSIGNING



SECTION A – Personal Details

Title	SELECT	UQ Username	
First Name		Preferred Name	
Surname		Date of Birth	

SECTION B - Role Details

Position Title		Affiliation with UQ	SELECT
Organisational Unit	SELECT	UQ Student No	

SECTION C – Access Request

Please select the access type based on the following: New for New Staff, Override if a staff has transferred to a new role, Add if a staff is requiring new permissions for their current role, or Deactivate if the staff member has left UQ.

☒ New ☐ Override ☐ Additional ☐ Deactivate (All)

Access Level Required

☒ Inquiry ☐ Core ☐ High

Specialist roles require SI-net Coordinator approval, while any Restricted access requests require approval from the Academic Registrar.

Specialist	Admissions (ICTE)	☐	**Restricted**	SF Refunds ☐
	Awards OUE	☐		Scholarship Approver ☐
	Examinations	☐		Official Transcript ☐
	Graduations	☐		Impersonate Student – Update ☐
	IAS Restricted	☐		Corrections – Prog/Plan Config ☐
	Progressions	☐		Corrections – Campus Community ☐
	Scholarships	☐		Corrections – CC & RA ☐
	Student Fees	☐		Corrections – Course Catalogue ☐
	Student Fees (FBS)	☐		Corrections – Enrolment Page ☐
	Modify Final Grades	☐		Corrections – RS ☐
				Corrections – SF FA ☐
				Corrections – SR Student Prog/Plan ☐

Justification — Justification required if any restricted roles are selected

SECURITY ROLES – APPROVAL & ASSIGNING

Level 1	Update Comments and Checklists Add/Update a Person Add/update student's personal information Deferred exams - Read Only Deferred exams - Upload Documents mySI-net Staff Functions tile - Update Grade upload Maintain the Course Catalogue Schedules Courses Update Student enrolment Update Term activation Update Milestones Update Transfer credit Update Student groups Placements (Medicine only) ***Note: The user will also be assigned the Inquiry role.***

SECURITY ROLES – APPROVAL & ASSIGNING

Level 2	Admissions processing Core Graduations processing Update Program/Plan Update Course Update Quota management Block enrolment Deferred exams - Approver (Mid-Semester) ** Additional info is required on the form to determine mid-semester and which Faculty, or end of semester exams. Note: specialist access "Deferred Examinations Approver" must be selected on the form* ***Note: The user will also be assigned the Inquiry and Level 1 roles.***

SECURITY ROLES – APPROVAL & ASSIGNING

SECTION D – Personal Agreement

I have read and agree to abide by the conditions detailed in the following policies:

- Code of Conduct: https://ppl.app.uq.edu.au/content/1.50.01-code-conduct
- Privacy Management: https://ppl.app.uq.edu.au/content/1.60.02-privacy-management
- Access to Student Systems: https://ppl.app.uq.edu.au/content/6.10.03-access-student-system
- Acceptable Use of UQ ICT Resources: https://ppl.app.uq.edu.au/content/6.20.01-acceptable-use-uq-ict-resources

I have liaised with my SI-net expert user to ensure the permissions levels are appropriate for my duties.

Ensure you have saved the pdf file locally after adding your signature – this ensures the form is added to the email as a pdf rather than a data file.

Signature		SUBMIT TO SI-NET COORDINATOR

SECTION E – Authorisation by SI-net Coordinator

I confirm the applicant has received the training to match their access request and their requested access is required to undertake the duties of their job.

Signature	

SECTION F – Authorisation by Academic Registrar

Justification for restricted role access has been approved.

Signature	

ROW LEVEL SECURITY

After review, decided to focus on:

- ADM & PROG Actions
- Enrolment Security (ENRL_ACCESS_ID)
- Transcript security

ROW LEVEL SECURITY – ADM & PROG ACTIONS

AA	PA	Action	Action Description	AA-ALL	AA-CORE	PA-ALL	PA-CENT	PA-CORE
	✓	ACTV	Activate			✓	✓	✓
✓	✓	ADMT	Admit	✓	✓	✓	✓	✓
✓	✓	ADRV	Admission Revocation	✓		✓	✓	
✓	✓	APPL	Application	✓	✓	✓	✓	✓
	✓	COMP	Completion of Program			✓		
✓	✓	COND	Conditional Admit	✓	✓	✓	✓	✓
✓	✓	DATA	Data Change	✓	✓	✓	✓	✓
✓	✓	DDEF	Defer Decision	✓	✓	✓	✓	✓
✓	✓	DEFR	Defer Enrolment	✓	✓	✓	✓	✓
✓	✓	DEIN	Intention to Matriculate	✓	✓	✓	✓	✓
✓	✓	DENY	Deny	✓	✓	✓	✓	✓
	✓	DISC	Discontinuation			✓	✓	✓
	✓	DISM	Dismissal			✓		
	✓	LEAV	Leave of Absence			✓	✓	✓
✓	✓	MATR	Matriculation	✓	✓	✓	✓	✓
✓	✓	PLNC	Plan Change	✓	✓	✓	✓	✓
	✓	PRGC	Program Change			✓	✓	✓
	✓	RADM	Readmit			✓	✓	✓
✓	✓	RAPP	Readmit Application	✓	✓	✓	✓	✓
✓	✓	RECN	Reconsideration	✓	✓	✓	✓	✓
	✓	REVK	Revoke Degree			✓		
	✓	RLOA	Return from Leave of Absence			✓	✓	✓
	✓	SPND	Suspension			✓	✓	✓
✓	✓	WADM	Administrative Withdrawal	✓	✓	✓	✓	✓
✓		WAIT	Waitlist	✓	✓			
✓		WAOF	Waitlist Offer	✓	✓			
✓	✓	WAPP	Applicant Withdrawal	✓	✓	✓	✓	✓
			High level AA/PA					
			High level PA					

ROW LEVEL SECURITY – ADM & PROG ACTIONS

ROLENAME (30)	AA	PA
UQ SA Staff Viewer		
UQ SA Helpdesk		
UQ SA Admissions High	AA-CORE	
UQ SA Admissions Standard		
UQ SA Admissions Domestic	AA-CORE	
UQ SA Admissions Int High	AA-CORE	PA-CORE
UQ SA Admissions Int Standard	AA-CORE	PA-CORE
UQ SA Faculty High	AA-CORE	PA-CORE
UQ SA Faculty Standard		
UQ SA School High	AA-CORE	PA-CORE
UQ SA School Standard		
UQ SA School Low		
UQ SA Central High	AA-ALL	PA-CENT
UQ SA Central Standard		
UQ SA Graduate School	AA-CORE	PA-CORE
UQ SA Official Transcript		
UQ SA Acad Progression		PA-ALL
UQ SA Exams		
UQ SA Graduations High		PA-ALL

ROW LEVEL SECURITY – ENROLMENT SECURITY

ENRL_ACCESS_ID	DESCR	ENR FUNC_ ENRL	ENR FUNC_ ENRL PERM	ENR FUNC_ DROP	ENR FUNC_ DROP PERM	ENR FUNC_ GBCH G	ENR FUNC_ UNIT_ CHG	ENR FUNC_ WAIT CHG	ENR FUNC_ GRADE_ ADD	ENR FUNC_ GRADE_ CHG	ENR FUNC_ REPEAT	ENR FUNC_ RD_ CHG	ENR FUNC_ INSTR_ CHG	SSR_ DYND_ LDRP_ OVRD
ENRF (ALL)	Enrolments Full Access ID	999	999	999	999	999	999	000	999	999	999	000	000	N
L3EN	Level 3 Enrol Access ID	160	160	999	999	000	160	000	999	400	000	000	000	N
L3EG	Level 3 Enrol GC Access ID	160	160	999	999	000	160	000	999	999	000	000	000	N
L2EN	Level 2 Enrol Access ID	160	160	200	200	000	160	000	999	000	000	000	000	N
L2EG	Level 2 Enrol GC Access ID	160	160	200	200	000	160	000	999	400	000	000	000	N
L1EN	Level 1 Enrol Access ID	160	160	200	200	000	000	000	000	000	000	000	000	N
CNEN	Central Enrol Access ID	200	200	999	999	000	999	000	999	400	000	000	000	N
CNEG	Central Enrol GC Access ID	200	200	999	999	000	999	000	999	999	000	000	000	N
GREN	Grad School Enrol Acc Id	200	200	999	999	000	000	000	999	000	000	000	000	N
GREG	Grad School Enrol GC Acc Id	200	200	999	999	000	000	000	999	999	000	000	000	N
GCHG	Grade Change Enrol Access ID	000	000	000	000	000	000	000	999	999	000	000	000	N
SPRG	Stdnt Progression Enrol Access ID	999	999	999	999	000	000	000	000	999	000	000	000	N
STFF	Staff Low Enrol Access ID	120	120	200	200	000	000	000	000	000	000	000	000	N
STNT	Student Enrol Access ID	120	120	200	200	000	000	000	000	000	000	000	000	N

ROW LEVEL SECURITY – ENROLMENT SECURITY

ROLENAME	EAID
UQ SA Staff Viewer	
UQ SA Helpdesk	
UQ SA Admissions High	
UQ SA Admissions Standard	
UQ SA Admissions Domestic	
UQ SA Admissions Int High	L1EN
UQ SA Admissions Int Standard	
UQ SA Faculty High	FHEN
UQ SA Faculty Standard	FSEN
UQ SA School High	SENH
UQ SA School Standard	SENS
UQ SA School Low	
UQ SA Central High	STCR
UQ SA Central Standard	
UQ SA Graduate School	GRAD
UQ SA Acad Progression	SPRG*
UQ SA Exams	GCHG*
UQ SA Graduations High	SPRG*
UQ SA Student Fees High	STCR
* Allocated in preference to STCR	

ROW LEVEL SECURITY

After review, decided to focus on:

- ADM & PROG Actions
- Enrolment Security (ENRL_ACCESS_ID)
- Transcript security

BUT WHAT ABOUT TRAINING?

Training no longer delivered ‘face to face’ by the system support team.

On-line training modules being developed and rolled out.

On the job advice and guidance provided by designated Expert Users.

Fitness to practice certified by SI-net Coordinators.

CURRENT SITUATION

SECURITY NIRVANA?

Adjustments to security were required post go-live, but we got the big things right.

No changes to security structure unless approved by Academic Registrar. Determined to 'hold the line' and not add Roles unless absolutely necessary. KISS is the operating principle.

BUT we are in a far better place (security wise).

QUESTIONS?

PRESENTER

Ian Holmes

Senior Manager, Student Systems Projects

University of Queensland

i.holmes@uq.edu.au

ALL ALLIANCE PRESENTATIONS WILL BE AVAILABLE FOR DOWNLOAD FROM THE CONFERENCE SITE

THANK YOU!

ADU 7-9 NOVEMBER 2018