MARK GANDY

A Journey from Compliance-Focused to Modernized Risk Governance

KEYS CONFERENCE

Disclaimer

A FEW THINGS FIRST

This presentation is for information only.
Evaluate risks before acting based on ideas from this presentation.

This presentation contains opinions of the presenters.
Opinions may not reflect the opinions of Tandem.

This presentation is proprietary.
Unauthorized release of this information is prohibited.

Agenda

H E R E ' S T H E P L A N

- Who is DCECU
- "Compliance" practices at the end of 2019
- "Risk Management (w/Compliance)" practices beginning in 2020
  - The Management Framework
  - The Steps Performed from Inherent Risk to Net Risk and Treatment
- Where we are today at the end of 2021
  - A few slides of the current executive summary (slides 11 and 13 …)

Note: I don't show much Tandem in this deck, but I cannot overstate how important the platform is to me and our stakeholders. Incredible value and catalyst to modern governance (and I hope to influence more development while here!)

Dow Chemical Employees' Credit Union

Midland, MI

Organizational Profile

- Single Branch
- SEG CU 74,000ish members
- US$2B asset size
- 160 employees (noses)

My Profile

- 3 years on the management team (after 20 years on SC)
- 29 years in global chemical manufacturing cyber and information security
- GO GREEN!

Compliance Focus

End of 2019….

IT Risk Assessment

Vendor DD

ISSP *Written Security Plan*

FFIEC CAT

I joined in 2019 and observed - Compliance based activities….

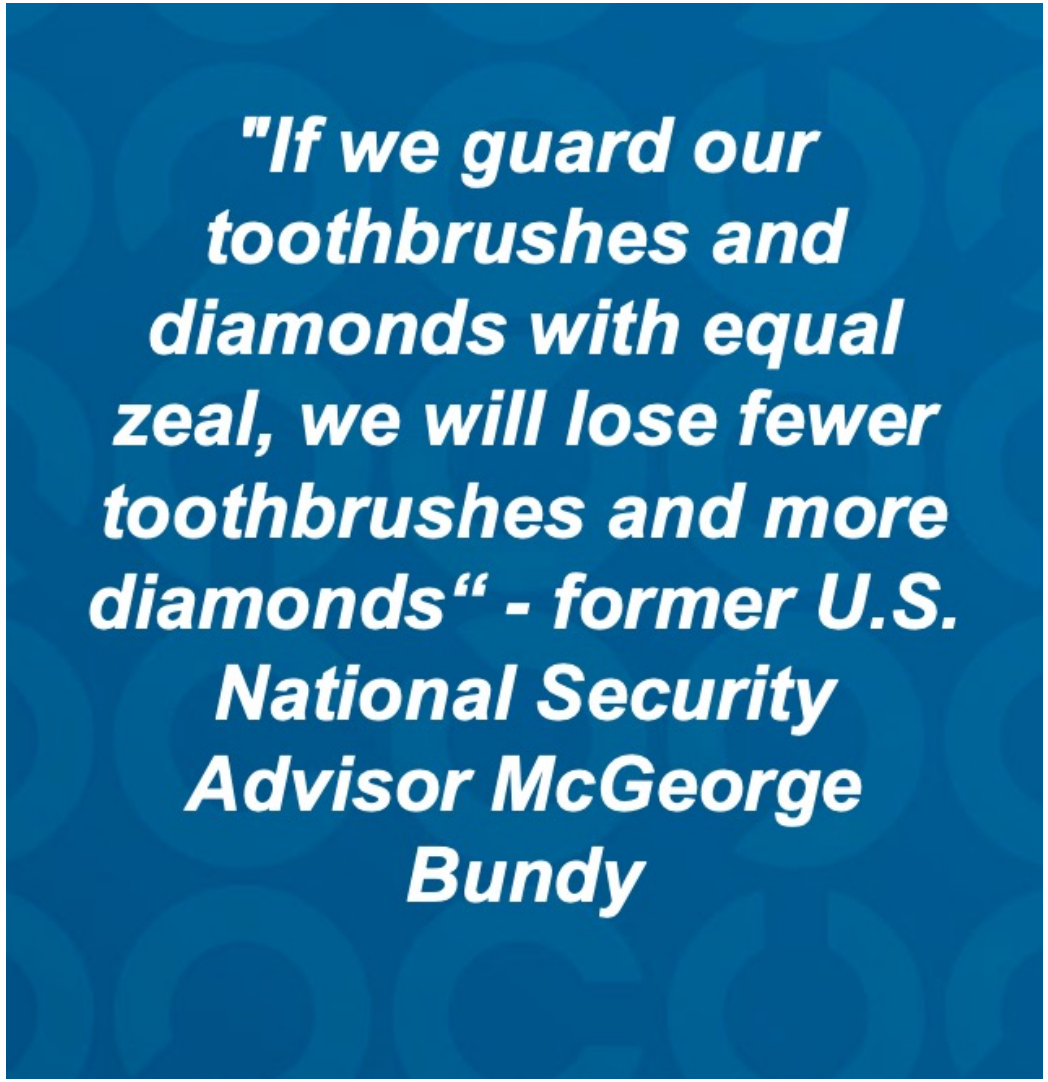
- Spreadsheet based
- In some cases purchased as template
- Thick and impressive(?), lots of words
- Not integrated with IT Design/Deployment (IT could not access ISSP)
- Performed “after the fact” in “catch up” mode…
- Still….positive Internal Audit and Examination results
  - *DCECU is compliant with regulatory expectations….*
  - *So what?*

If we are honest…

- *Inconsistent*
- *Out of date*
- *Poorly understood*
- *Largely ignored (i.e. IT director will…)*
- *Performed only to satisfy examiners*

Positioning the Change

Let's only do things that matter



Drivers Influencing Changes and Expectations

- Increasing complexity resulting from CU growth
  - Higher turnover in subject matter experts
  - New products and services, powered by new digital models
- Increasing sophistication from the board/committees and examiners
  - Asking better questions about cyber and information security (see below)
- Cyber and Information Threats (*I can't say they are increasing)*
  - *The vulnerability attack patterns remain about the same*
  - *Motives are evolving along with economic benefits to bad actors*
- **Modern Governance models have evolved**
  - Transition from "Are we compliant"? to "**Is management identifying and treating risks appropriately?"**
  - Manage the complexity with scale, completeness, and consistency and informing (value add) to all stakeholders
  - Audit Universe and Control Assurance Mapping for stronger conclusions

The Framework

What I expect my business partners to know about Risk Management

- **Know what you have and its relative importance to protect**
  - *This is known as the "Inherent Risk" and is evaluated by the need to keep information a secret, correct, and ready to use. (aka Confidentiality, Integrity, Availability)*
- **Determine, for each system, that reasonably foreseeable cyber and information threats are defended against using CU standards as expected.**
  - *Passwords, backups, monitoring, etc. are controls the CU uses to run safe and secure information systems and infrastructure*
- **What to do when standards are not implemented as expected?**
  - *If expected controls are not implemented, what does it mean? This is known as "Residual" or "Net" Risk.*
  - *Does the control need fixed? (Mitigation required) or does management think it is okay as is (Accept the Risk) because of other considerations…*
- **Communicate the results**
  - Documented results with considerations of compensating controls by by the system owner and management
  - More serious exceptions reviewed more frequently with executive management and the board/committees
- **Bonus**
  - **This is NOT a one time/year deliverable, this is *continuous* risk management (at the end of 2021 this is now well understood…)**

Step One

Know what you have

&

Why it needs to be protected…

Step 1 of Step One
- Import assets from all existing inventories
- Business Partner interviews

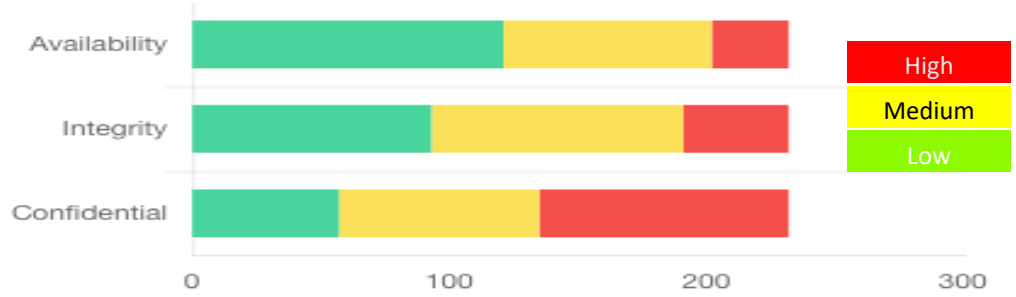
Step 2 of Step One
- Using reasonable terms/definitions to get to the technical C/I/A qualified ratings

Results!
- Very powerful – I can now show an asset's C/I/A profile to stakeholders and at a glance they understand the inherent risks (even if they don't know the "what" the asset does….)

Count of Information Assets **by Inherent Risk** Factors

DCECU Information Risk: *before mitigation* *n=225 systems*

Enlightened stakeholders!!



Confidentiality (C): the risk of unauthorized disclosure
Integrity (I): the risk of incorrect or loss of data
Availability (A): the risk the information/service isn't available

Confidential	Integrity	Availability
• High: *storage of* Sensitive Member Info, Employee PII • Medium:*processing* Sensitive Member Info, Employee PII • Low: public or internal, no SMI/Emp PII	• High: used in reconciliation, relied on for key control, *system of record* • Medium:used in processing, *generally* relied on, but not system of record; i.e. metrics data warehouse • Low: no reliance	• High: operational impact same day (all hands on deck!) • Medium: operational impact within a few days to a week • Low: could go weeks, months….

Step Two

Consider Reasonably Foreseeable Threats

Using a risk-based approach DCECU began with the “high” IRP’s and began conducting RA’s for expected controls….

And is still playing catch upfor the remaining assets.

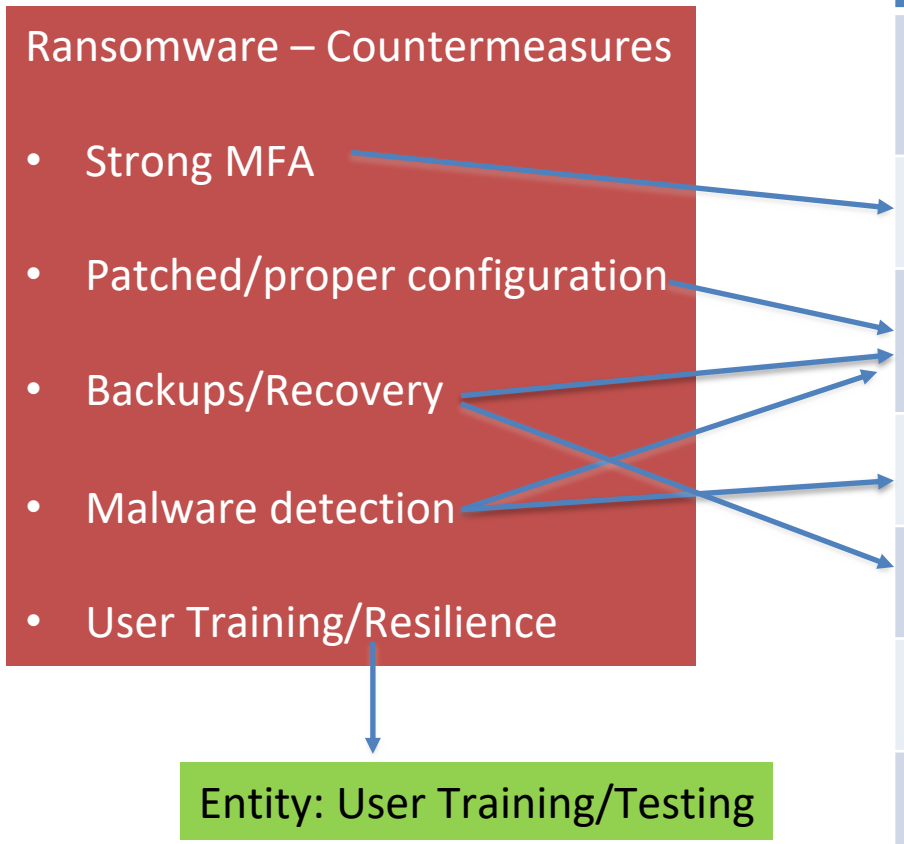
Regulations require DCECU to risk assess operations and establish controls to mitigate risks for “reasonably foreseeable threats” to cyber and information processing. DCECU has developed the following general Threat profiles ***based on industry best practices*** to address a wide range of common threats. More threat profiles are planned, but you can’t get there without being here to start.

Threat Profiles **more will be added in 2021*	**”Key Control” Objectives to Mitigate Threats**
Covid Continuous Operations	Applied to services operated by critical/significant+ vendors to ensure they have plans for ongoing operations during the pandemic.
Identity and Authorization Management	Controls to manage the full lifecycle of user ID management, authentication, and appropriate access is managed.
Configuration Reliability	Controls to manage reliable system configurations and detect/recover from data loss, keep systems up to date.
Security Monitoring	Controls to ensure cyber and information access logs are correctly logged and available for analysis.
Transport and Storage	Controls for secure network access and transmission, as well as the secure encryption, of information.
Vendor Due Diligence	Controls to ensure appropriate alignment with vendor management program
Service Organization Controls	Ensure that DCECU receives assurance from vendors of security design and operations of controls with independent testing.

Without controls designed and operating correctly to manage these common threats, there is risk to the confidentiality, integrity, and/or the availability of DCECU’s member information or operational capability

The usefulness of Step Two

How Many Risk Assessments does it take?



Threat Profile **more will be added in 2021* *typical threats*	Description
Covid Continuous Operations	Applied to services operated by critical/significant+ vendors to ensure they have plans for ongoing operations during the pandemic.
Identity and Authorization Management	Controls to manage the full lifecycle of user ID management, authentication, and appropriate access is managed.
Configuration Reliability	Controls to manage reliable system configurations and detect/recover from data loss, keep systems up to date.
Security Monitoring	Controls to ensure cyber and information access logs are correctly logged and available for analysis.
Transport and Storage	Controls for secure network access and transmission, as well as the secure encryption, of information.
Vendor Due Diligence	Controls to ensure appropriate alignment with vendor management program
Service Organization Controls	Ensure that DCECU receives assurance from vendors of security design and operations of controls with independent testing.

Understanding “Net” Risk Qualifications

R a t e d S F W

We look at the qualified net risk labels in this way….

Low: Belt and Suspenders are on, no known exposure

Medium: “Your fly is down” so some exposure, but can be managed

High: Pants are around your ankles! Direct exposure

Which allows my business partners to understand the technical nuances of likelihood and consequence when considering the implementation status of expected controls….

Step Three

Communicate, Manage, and provide stronger Assurance

Management
1st/2nd Line Internal Controls

Policy 901
- Know where the inherent risks are by CIA
- Manage Cyber and Information Risks appropriately

CIA Composite Inherent Risk Assets (n=239)

High	Medium	Low
32	131	76

Risk Appetite
- Assess High Inherent Risk assets for expected controls (ISSP)
- Communicate

Risk Management Plans Count by Residual Risk (IRP = H/M Only)

	Mitigate Further	Accept
High: (CEO Owner)	**0**	**0**
Medium: (Exec Owner)	3	9

Internal Audit
3rd Line Assurance

Risk Based Internal Audit Plan						
	Threat/Controls					
Inherent Risk	Identity	Configuration	Data Protect	Monitor	3rd Party	
High	Annually					
Medium	*every 5 years					
Low	Discretionary					

3rd Line Internal Audit Results

Domain	Findings		
	High	Moderate	Low
Domain 1: Cyber Risk Management and Oversight	-	-	1
Domain 2: Threat Intelligence and Collaboration	-	1	-
Domain 3: Cybersecurity Controls	-	3	3
Domain 4: External Dependency Management	-	-	1
Domain 5: Cyber Incident Management and Resilience	-	-	-

Step Three

Risk Treatment Communications

Residual Risk/Sign-off/Reporting
Low: Review/Annual Report
Medium: Executive sign-off/Quarterly
High: CEO sign-off/Monthly (ASAP)

Risk Assessment	IR	Threat Control Profile	Residual	RMP	Description
	H	ITGC - Identity and Authorization	M	MF	No MFA ITSD-9258; Reauth of privileged users ITSD-1671
	H	ITGC - Security Monitoring	M	MF	Logging to SIEM not performed. ITSD-9926
	H	ITGC - Identity and Authorization	M	MF	Reauthorizations not performed annually. SEC-1660
	H	Main Office Physical Security Controls	M	MF	Internal door lock bypass (CG) SEC-1689
	M	ITGC - Service Organization Controls	M	A	Report of audited controls not available.
	H	ITGC - Identity and Authorization	M	A	Shared account password rotation.
	H	ITGC - Storage and Transmission of Info	M	A	No encryption at rest. (1)
	H	ITGC - Identity and Authorization	M	MF	Reauthorization of privileged users ITSD-1645
	H	ITGC - Service Organization Controls	M	A	Report of audited controls not available.
	M	ITGC - Service Organization Controls	M	MF	SOC not current. SEC-1653
	H	ITGC - Identity and Authorization	M	A	"Doe" account controls improvements. SEC-9773/9774
	H	ITGC - Identity and Authorization	M	A	Account type standard documention. (2)
	H	ITGC - Security Monitoring	M	MF	Logging to SIEM not performed. ITSD-8412
	H	ITGC - Service Organization Controls	M	A	Report of audited controls not available.
	H	ITGC - Service Organization Controls	M	A	Report of audited controls not available. (3)
	H	ITGC - Identity and Authorization	M	MF	Reauthorization of privileged users ITSD-1637

Notes

1 Documented in Cybersecurity Assessment Tool
2 ISSP will be updated in-house 2021
3 Service is new and SOC is planned.

Wonderful, wonderful Tandem

W h e r e w o u l d I b e w i t h o u t t h e e ?

There are 2 Tandem Reports provided on a quarterly basis to the Board and Committees in support of the Dashboard (as the gory details for the interested reader….)

1) Asset Security Requirements
   - The “inventory” of all assets assessed for inherent risk by C, I, and A.

2) Risk Management Plan Summary
   - Provides the Risk Management program definitions
   - Assessment and conclusions on the implementation status of each threat profile/control objectives for each Risk Assessed Information Asset
   - The Net Risk conclusion from management
   - Risk Management Plans (if needed):
     - Mitigate: what control element is missing and how will this be corrected and monitored in the interim
     - Accept: what control element is missing and what controls will be relied on, and a frequency for review

Questions?

- I love to talk about governance HMU!
  - mgandy@dcecu.org

- In the interest of time – I omitted the some of the hard work…
  - What are the most important (key) controls for each threat profile
  - Teaching system owners and IT what the expectations are ….
  - Establishing common control procedures to enhance audit efficiency

- And some of the future….
  - New threat profiles (privacy, Online Banking, mobile)
  - Being used across all operational areas of the CU (non-IT)
  - The use of Tandem and integration with Audit Management, IR, VM, etc….

KEYS
CONFERENCE

DON'T FORGET!

Fill out the survey to get your sticker!

Upcoming Sessions

TANDEM

All About Third Parties

Jonathan Garner, Tandem

RISK & COMPLIANCE

7 Ways to Transform How You Report Cybersecurity

Alyssa Pugh, Tandem

CYBERSECURITY

The Human Element of Cybersecurity

BJ Taylor, CoNetrix Security / Boost Consulting

KEYS CONFERENCE

Example Threat Profile

Identity Management

Key Controls to protect the authentication and authorization of an identity throughout the lifecycle…

1) Accounts are disabled immediately upon termination/suspension
2) Authentication factors are strong for the operating environment
3) “Least Privileged” RBAC is designed and operated
4) Privileged Users are reauthorized every 6 months
5) Standard Users are reauthorized every 12 months