Developing a Cybersecurity Scorecard

U.S. Department of Agriculture

Farm Service Agency

FSA

FARM SERVICE AGENCY

Foundation

- People & Organizations Contribute to Outcomes
- Good Management Through Measurement
- Confidence Through Transparency Requires Evidence
- Performance Improves Through Recognition and Feedback
- All Levels Value Communication

NIST References

- NIST Special Publication 800-55 Revision 1: Performance Measurement Guide for Information Security
  - Elizabeth Chew, Marianne Swanson, Kevin Stine, Nadya Bartol, Anthony Brown, and Will Robinson
  - http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf
- ITL Bullentin Security Metrics: Measurements to Support the Continued Development of Information Security Technology
  - Shirley Radack
  - http://csrc.nist.gov/publications/nistbul/Jan2010_securitymetrics.pdf
  - Especially pages 2-4 “Issues In Developing Security Metrics”
- NISTIR 7564: Directions in Security Metrics Research
  - Wayne Jansen
  - http://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7564.pdf
  - Especially Section 3 “Aspects of Security Measurement”

Why a Scorecard?

People & Organizations Contribute to Outcomes

- Results-based Management (RBM) uses feedback loops to achieve strategic goals.

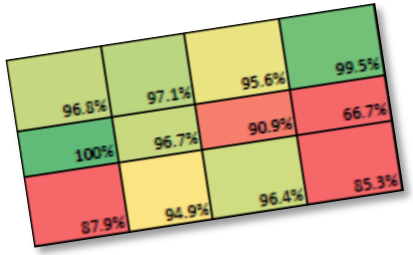
https://en.wikipedia.org/wiki/Results-based_management

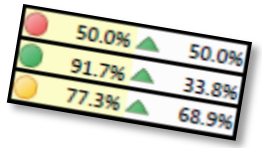
https://en.wikipedia.org/wiki/Results-based_management

Developing a Scorecard

Developing a Scorecard

- Define Success: What is the objective?
  - What does success (“good”) look like?
  - To the taxpayer, your customer, the Administration, your executive(s), you?
  - We are conditioned to respond to information presented in certain ways…

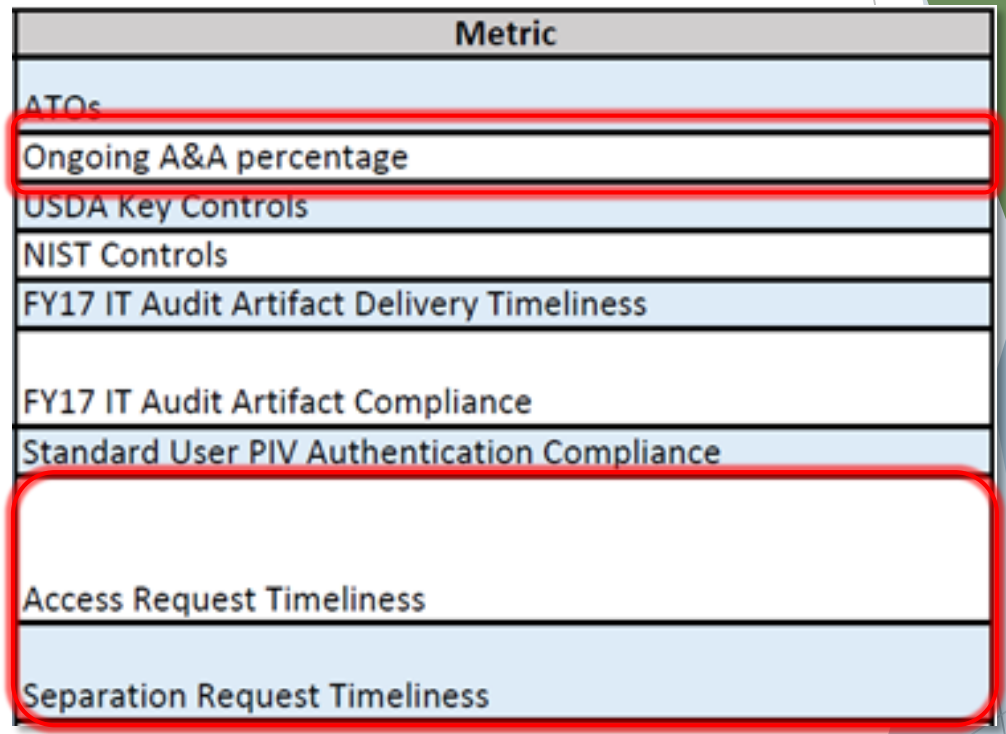




https://en.wikipedia.org/wiki/Balanced_scorecard

Developing a Scorecard

- Select targets and measures to track (progress) achievement of objectives
  - Management team is fully involved
  - Management team is the primary customer of the scorecard
  - Select leading indicators and lagging indicators

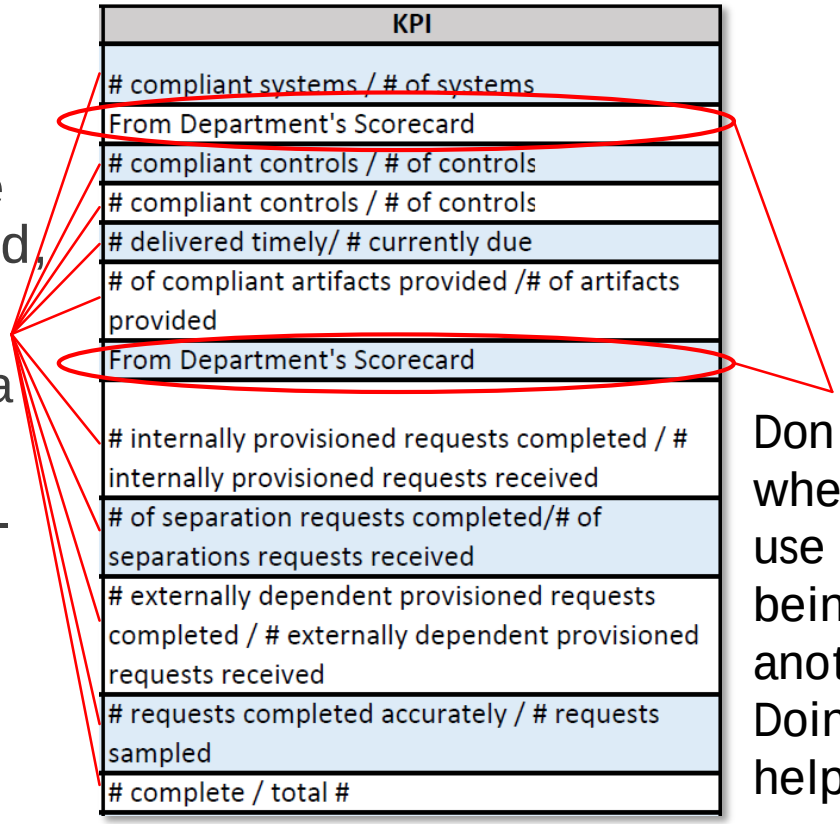


Metric
ATOs
Ongoing A&A percentage
USDA Key Controls
NIST Controls
FY17 IT Audit Artifact Delivery Timeliness
FY17 IT Audit Artifact Compliance
Standard User PIV Authentication Compliance
Access Request Timeliness
Separation Request Timeliness

https://en.wikipedia.org/wiki/Balanced_scorecard

Developing a Scorecard

- Data needs context
  - Data without context is meaningless. So what if there were 5734 events? Is that good, bad, normal?
    - Easiest way we've found is a percentage (ratio).
    - We also use some year-over-year comparisons to show trends.
  - Data with context becomes actionable information
    - Dispels F.U.D. (fear, uncertainty and doubt)
    - Enables management to take action.



Don't reinvent the wheel. It's OK to use existing KPIs being collected by another source. Doing this may help demonstrate cascading goals.

https://en.wikipedia.org/wiki/Balanced_scorecard

Developing a Scorecard

- Start small, start with one Key Performance Indicator (KPI)
- Try thinking about it this way:
  - It is important to me (and my management team) that our customers are happy.
    - My customers are happy when the right people receive the right access.
    - “My customers” are end users, supervisors, system owners, auditors, others.
    - When we deliver 100% on this metric, I am reasonably assured my customers are happy with our access provisioning service. (I should get no flaming emails or material weaknesses.)

Access Request Completion Accuracy	# requests completed accurately / # requests sampled	100%

Let’s Take A Closer Look

Domain	Metric	KPI	6/9/2017	6/2/2017	5/26/2017	5/19/2017	5/12/2017	5/5/2017	4/28/2017	4/21/2017	4/14/2017	4/7/2017	3/31/2017	3/24/2017	Notes
Hygiene	ATOs	# compliant systems / # of systems	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100.0%	100%	
	Ongoing A&A percentage	From Department's Scorecard	100%	97.1%	97.1%	85.7%	85.7%	85.7%	77.1%	77.1%	62.9%	88.6%	88.6%	88.6%	
	USDA Key Controls	# compliant controls / # of controls	99.5%	99.5%	99.5%	99.5%	99.5%	99.5%	99.5%	99.5%	99.7%	97.7%	97.7%	96.1%	
	NIST Controls	# compliant controls / # of controls	98.4%	98.4%	98.4%	98.4%	98.4%	98.4%	98.4%	98.3%	98.4%	98.0%	98.0%	97.7%	
	FY17 IT Audit Artifact Delivery Timeliness	# delivered timely/ # currently due	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	
	FY17 IT Audit Artifact Compliance	# of compliant artifacts provided /# of artifacts provided	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	
Access	Standard User PIV Authentication Compliance	From Department's Scorecard	98.9%	99%	99%	99%	99%	99%	98.6%	98.6%	98.9%	98.9%	98.7%	98.7	
	Access Request Timeliness	# internally provisioned requests completed / # internally provisioned requests received	97.6%	98%	95.1%	96.8%	96.8%	97.1%	95.6%	99.5%	99%	99.3%	96.9%	97.7%	
	Separation Request Timeliness	# of separation requests completed/# of separations requests received	90.9%	98.4%	96%	100%	100%	96.7%	90.9%	66.7%	70.6%	76.7%	91.7%	77.8%	
	Service Provider (or other Non-[IT Director E]) Request Timeliness	# externally dependent provisioned requests completed / # externally dependent provisioned requests received	91.2%	89.5%	92.5%	87.9%	87.9%	94.9%	96.4%	85.3%	84.4%	85.7%	74.6%	74.3%	
	Access Request [illegible]ccuracy	# requests completed accurately / # requests sampled	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	
Awareness	[SES Org A]	# complete / total #	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	
	[SES Org B]	# complete / total #	99.4%	99.4%	99.4%	99.4%	99.4%	99.4%	99.4%	99.4%	99.4%	99.4%	99.4%	99.4%	
	[SES Org E.1]	# complete / total #	99.9%	99.9%	99.9%	99.9%	99.9%	99.9%	99.9%	99.9%	97.2%	97.0%	97.0%	96.9%	
	[SES Org E.2]	# complete / total #	97.7%	97.6%	98.6%	99.2%	99.2%	98.5%	98.5%	98.4%	81.7%	81.3%	80.9%	80.7%	
	[SES Org F]	# complete / total #	98.7%	100%	100%	100%	100%	100%	99.6%	100%	99.6%	100%	99.6%	99.6%	
	[SES Org I]	# complete / total #	98.9%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	
	[SES Org J]	# complete / total #	96.9%	97%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	
	Externals (Contractors, Volunteers, Affiliates & Interns)	# complete / total #	93.5%	93.5%	93.1%	93.2%	93.2%	92.7%	92.5%	92.8%	92.1%	92.1%	91.8%	91.6%	
	Total Users Basic ISAT (minus committee members)	# complete / total #	98.1%	98.1%	98.7%	98.7%	98.7%	98.6%	98.6%	98.5%	98.5%	98.5%	84.6%	84.4%	
	Committee Members Alternate ISAT (Protecting PII)	# complete / total #	17.9%	15.3%	12.5%	9.6%	9.6%	5.4%	4.4%	2.3%	N/A	N/A	N/A	N/A	
	Total ISAT and PII (per USDA)	From Department's Scorecard	83.3%	82.6%	82.6%	82.6%	82.0%	82.0%	81.9%	81.9%	81.3%	0.27	0.27	0.24	
	FY17 Specialized Role-Based Training	# complete / total #	13%	12.4%	1.9%	1.9%	1.9%	1.9%	1.9%	1.9%	N/A	N/A	N/A	N/A	
Vulnerabilities	Vulnerabilities/Endpoint	From Department's Scorecard	0.87	1.31	1.31	1.31	2.05	2.05	5.86	5.86	58.72	0%	73.1%	73.1%	
	[IT Operations A] Vulnerability Remediation Tickets on Schedule	# of on schedule [IT Operations A] tickets/# of open [IT Operations A] tickets	20%	87.5%	87.5%	87.5%	87.5%	87.5%	0%	0%	0%	84.6%	16.7%	16.7%	
	[IT Operations A] Vulnerability Remediation Tickets Remed	# of [IT Operations A] tickets closed/# of [IT Operations A] tickets	84.8%	75.8%	75.8%	75.8%	75.8%	75.8%	96.2%	92.3%	88.5%	0%	81.3%	81.3%	
	[IT Operations B] Vulnerability Remediation Tickets on Schedule	# of on schedule [IT Operations B] tickets/# of open [IT Operations B] tickets	50%	100%	100%	100%	100%	90.9%	0%	0%	0%	84.4%	-67.0%	-66.1%	
	[IT Operations B] Vulnerability Remediation Tickets Remediated	# of [IT Operations B] tickets closed/# of IPSUO tickets	90.5%	83.3%	83.3%	81%	81%	73.8%	96.9%	93.8%	90.6%	-65.5%	[illegible]%	-45.5%	
Cyber Incidents	Trend of FSA incidents to USDA incidents this FY	Trend of # of incidents / # of incidents expected per ratio of FSA to USDA employees	-68.6%	-69.4%	-69.6%	-69.3%	-69.3%	-69.1%	-69.3%	-68.6%	-65.8%	-46.5%	[illegible]%	22.2%	
	Compar[IT Director E]n of FSA Incidents this FY to last FY	Incidents so far this FY / Incidents so far this time last FY	-51.9%	-52.8%	-52.7%	-51.2%	-51.2%	-51.0%	-52.1%	-50.5%	-46.9%	-23.8%	-58.4%	-53.8%	
	Trend of FSA PII incidents to USDA PII incidents this FY	Trend of # of PII incidents / # of incidents expected per ratio of FSA to USDA employees	-20.8%	-9.1%	-9.3%	-5.7%	-5.7%	-0.8%	-0.8%	5.4%	23.8%	-57.2%	96.4%	96.4%	
	Compar[IT Director E]n of FSA PII Incidents this FY to last FY	PII Incidents so far this FY / Incidents so far this time last FY	-67.9%	-67.0%	-66.0%	-65.0%	-65.0%	-63.9%	-62.7%	-61.5%	-58.7%	98.1%	100%	100%	
Exceptions	All OCIO Plan of Actions and Milestones (POA&Ms)	# of On Schedule POA&Ms / total # of POA&Ms	100%	100%	100%	94.6%	94.6%	94.6%	94.6%	97.5%	97.7%	98.1%	96.4%	96.4%	
	[IT Director A] Plan Of Actions & Milestones (POA&Ms)	# of On Schedule [IT Director A] POA&Ms / total # of [IT Director A] POA&Ms	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	
	[IT Director C] Plan Of Actions & Milestones (POA&Ms)	# of On Schedule [IT Director C] POA&Ms / total # of [IT Director C] POA&Ms	100%	100%	100%	50%	50%	50%	50%	50%	50%	50.0%	50.0%	50.0%	
	[IT Director E] Plan Of Actions & Milestones (POA&Ms)	# of On Schedule [IT Director E] POA&Ms / total # of [IT Director E] POA&Ms	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	100.0%	100.0%	100.0%	
	[IT Director F] Plan Of Actions & Milestones (POA&Ms)	# of On Schedule [IT Director F] POA&Ms / total # of [IT Director F] POA&Ms	100%	97%	97%	97%	97%	97%	97%	100%	100%	98.1%	97.8%	97.8%	
	Milestones	# of On Schedule milestones/ total # of milestones	100%	100%	100%	96%	95.7%	95.7%	95.7%	96.6%	96.8%	95.5%	95.6%	95.4%	
	Risk Based Decision (RBD)	# of unexpired / total # approved	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	

Not All KPIs Show Variations

- Access Request Timeliness
  - Our access request team processes 500+ system access requests a week. Weekly variance of +/-5% is not concerning.
- Some metrics run at 100% week after week.
  - These are scrutinized to make sure we are measuring the right things.
  - The ones that remain we've determined have value because we want to know if even small variations from 100% occur.

Benefits

Good Management Through Measurement

- Lagging KPIs help identify problems that contribute to risk
  - Improving the lagging KPIs indirectly reduces risk
- Leading KPIs help serve as an early warning on potential risks
  - Improving the leading KPIs helps resolve unrealized risks
- Information provides evidence of results

- Returning to the RBM model…

Transparency + Accountability = Confidence

- Showing good, bad, ugly ➔ Transparency
- Produces evidence through information
- Gives confidence that programs are being managed

Recognition + Feedback = Improvement

- Document Quality Assurance Surveillance Plan (QASP) results for contracts
- Document team performance results
- Document service provider performance results

Future

Future of the Scorecard

- Pivot to Cybersecurity Framework (identify, protect, detect, respond, recover)
  - Transition domains to align with CSF functions
  - Identify KPIs that support OMB cyber memo objectives
- Continue to look for KPIs that are indicators of risk
  - Security Impacts of Change Requests
  - Vulnerability Impacts
- Continue to look for leading indicators of performance
- Expand information received from service providers

Thank You

About Me

Jeff Wagner, CISSP
Chief Information Security Officer
Information Security Office Director

Beacon Facility Mail Stop 2040
P. O. Box 419205
Kansas City, MO 64141-6205

816-926-6747

jeff.wagner@kcc.usda.gov

https://www.linkedin.com/in/jeff-wagner-cissp-16453217/

About FSA

The Farm Service Agency (www.fsa.usda.gov) delivered over $6B in direct and guaranteed farm loans and nearly $9B in farm program payments in 2016. FSA helps to ensure the security of commodities distributed worldwide. FSA delivers its mission through a network of over 2,100 field offices supported by headquarters and regional offices throughout the United States.