SAND2017-3314C

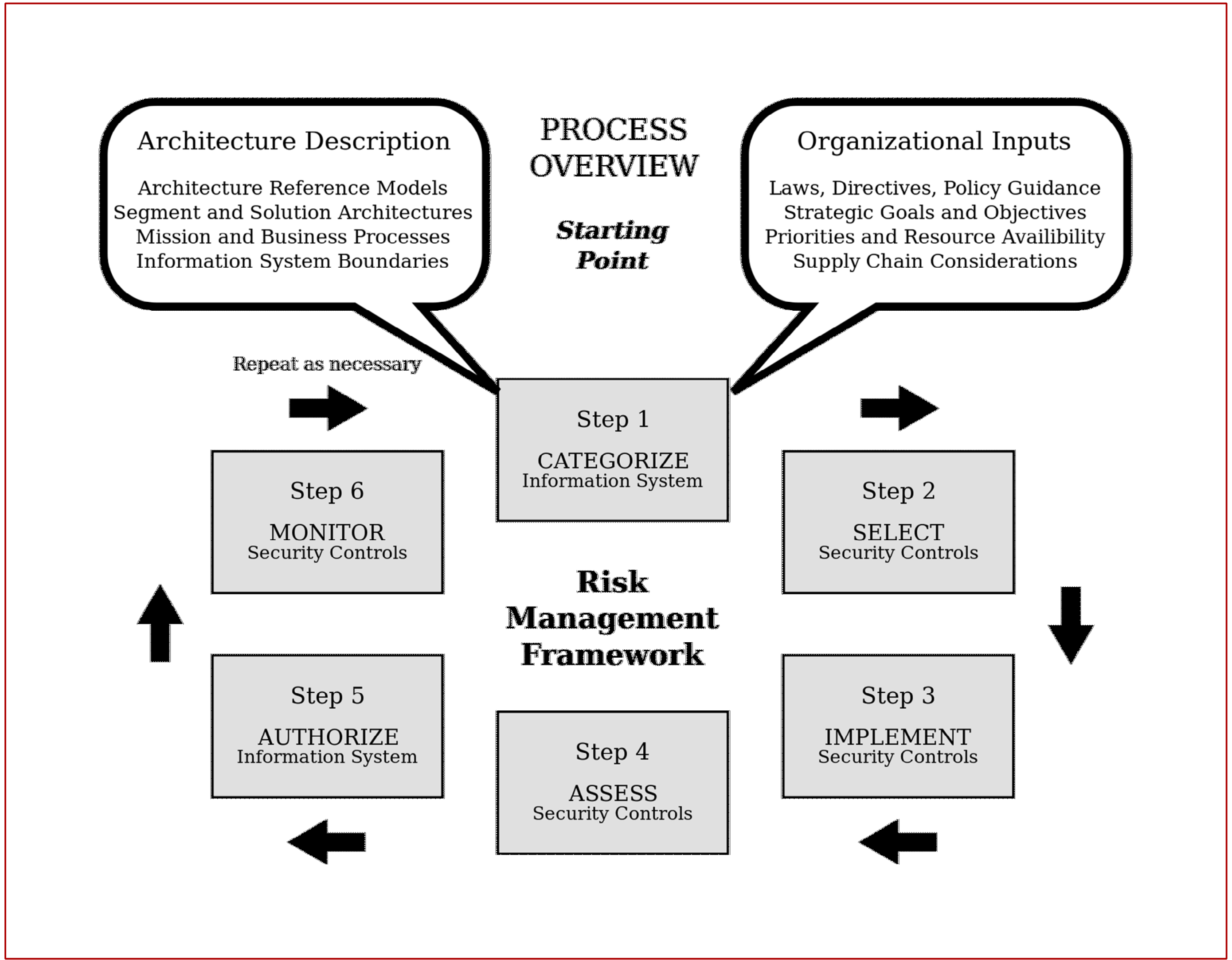
Achieving Continuous Risk Management

Max Blumenthal
Senior Cyber Assurance Architect
Sandia National Laboratories

Christie Gross
Senior Cyber Assurance Architect
Sandia National Laboratories

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

NIST Risk Management Framework



Continuous Monitoring

- Identify gaps through the assessment process and ongoing monitoring
- Determine continual effectiveness of controls
  - Automated and manual monitoring methods
- Monitoring frequency determination
- Evaluate security posture at different levels of the enterprise
  - Tier 3, Tier 2, Tier 1
- Feed effectiveness of controls into risk management and analysis

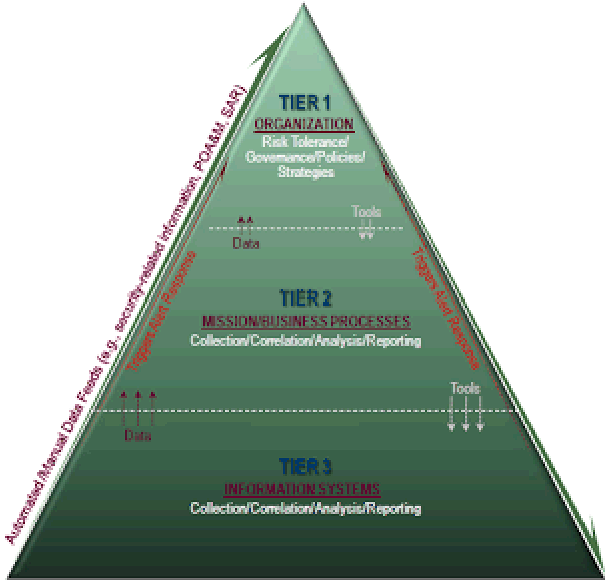
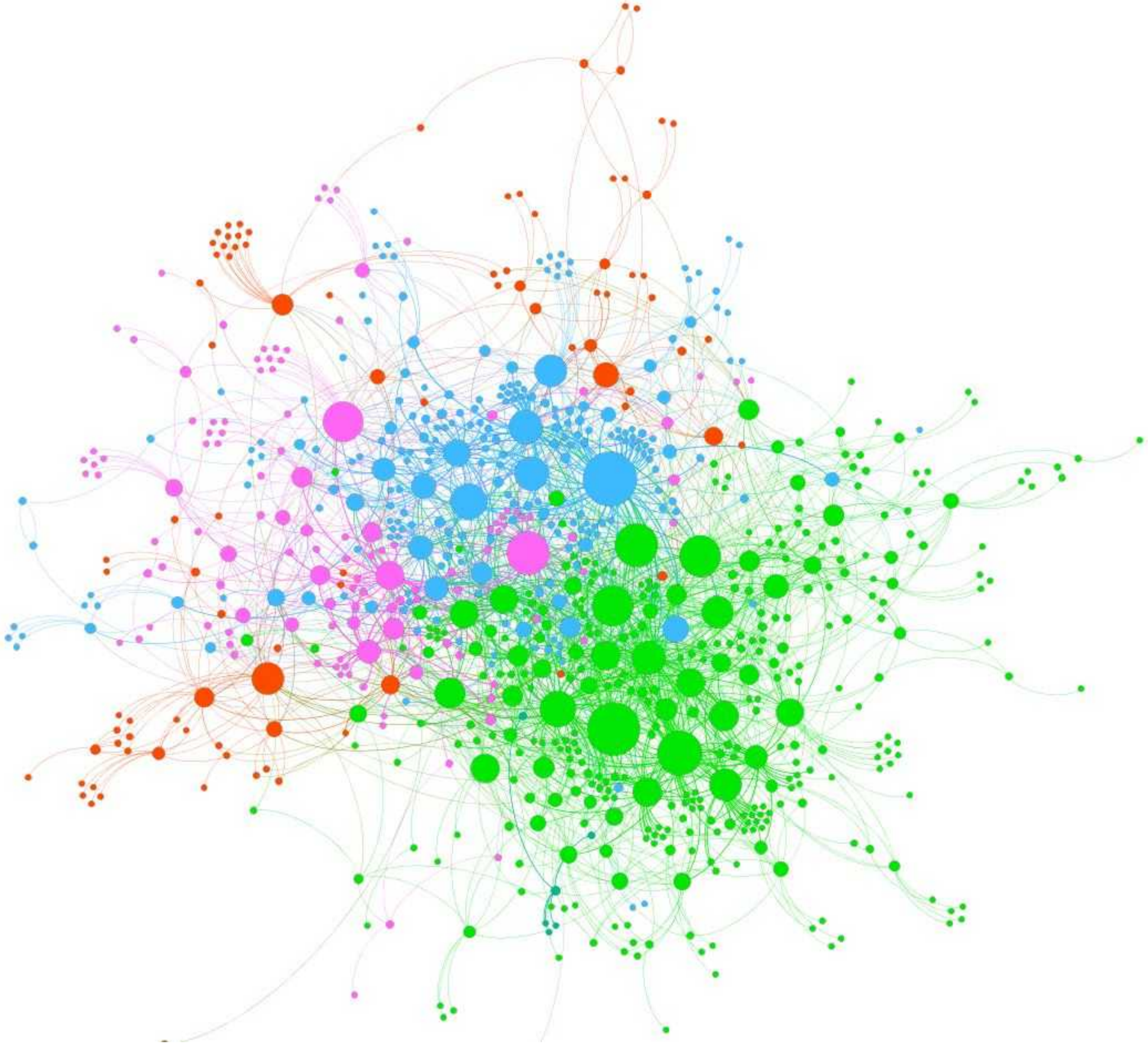
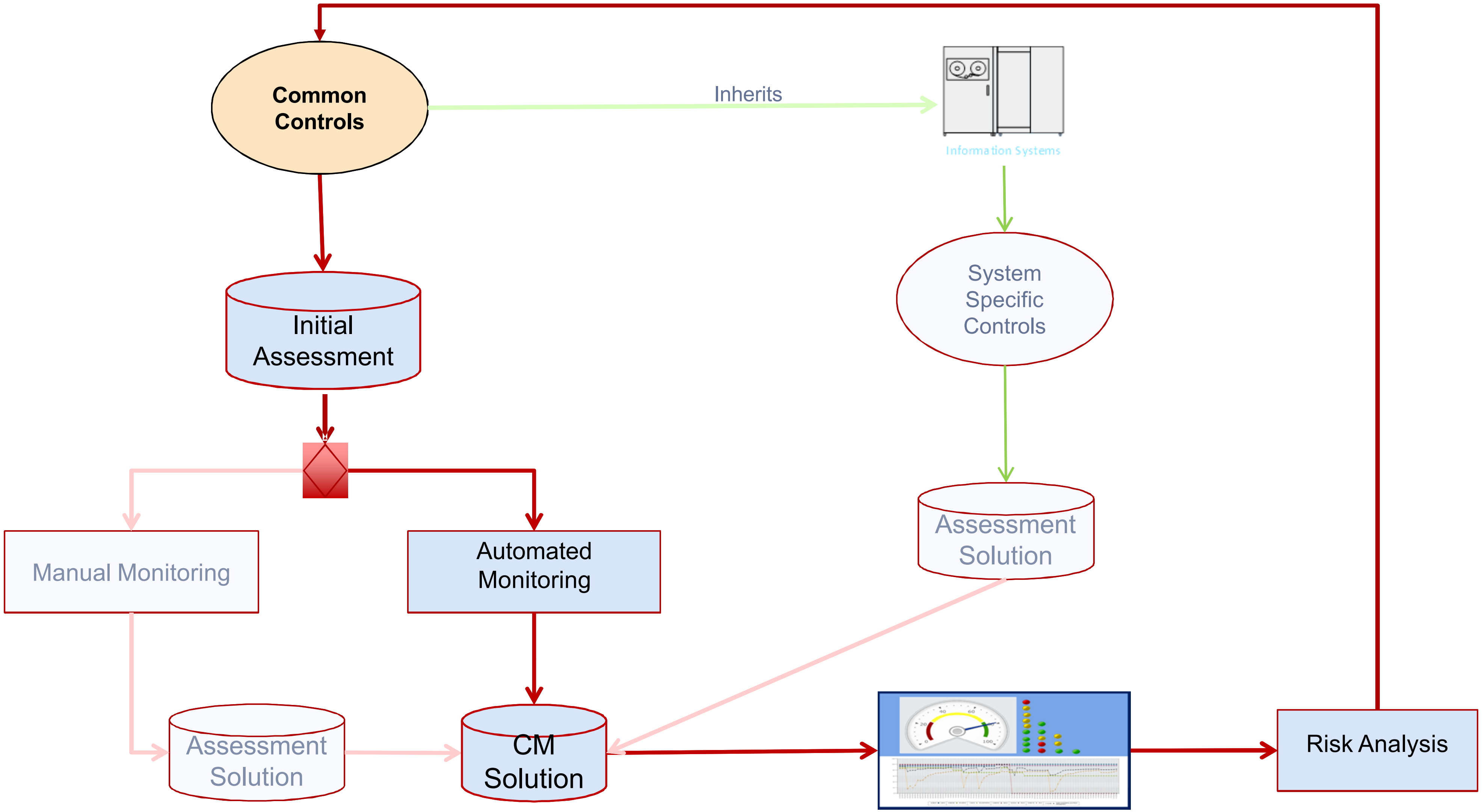

TIER 1
ORGANIZATION
Risk Tolerance/ Governance/Policies/ Strategies
Tools
Data
TIER 2
MISSION/BUSINESS PROCESSES
Collection/Correlation/Analysis/Reporting
Tools
Data
TIER 3
INFORMATION SYSTEMS
Collection/Correlation/Analysis/Reporting
Automated/Manual Data Feeds (e.g., security-related information, POA&M, SAR)
Triggers Alert Response
Triggers Alert Response

Figure 2-1. Organization-wide ISCM

Control Mapping for Gap Analysis

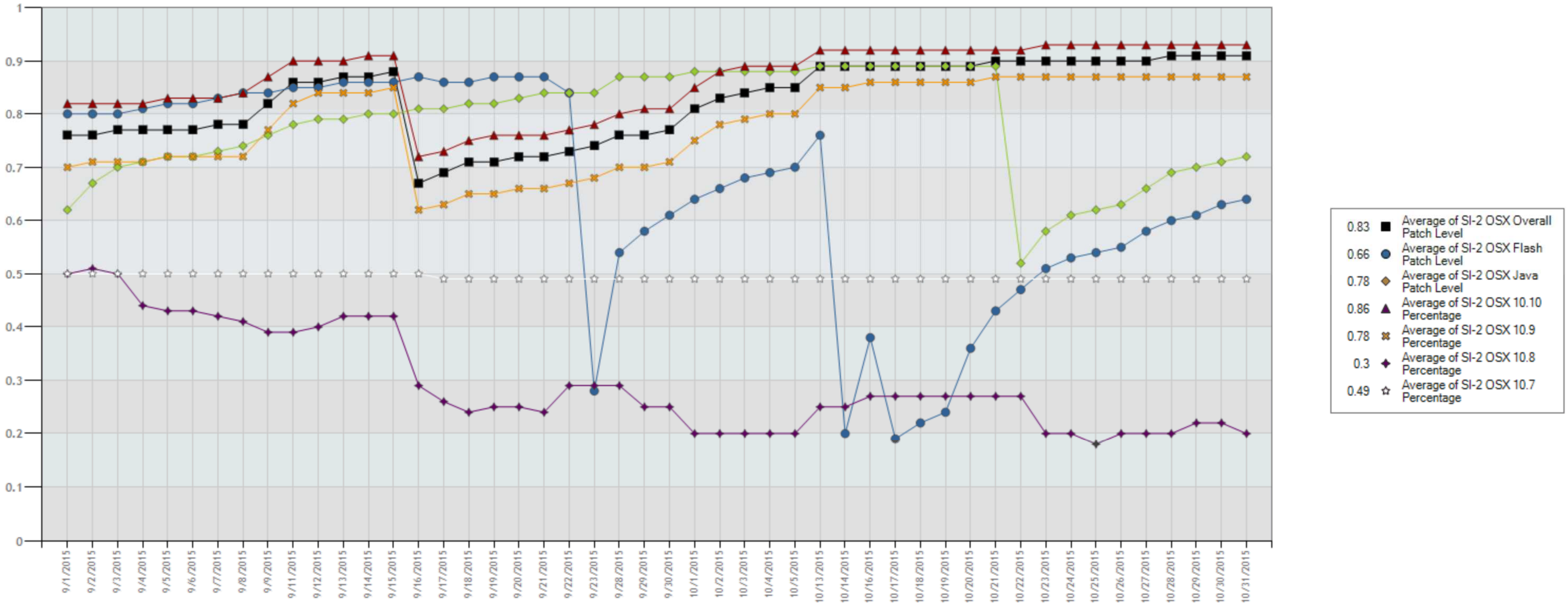


Continuous Monitoring Process

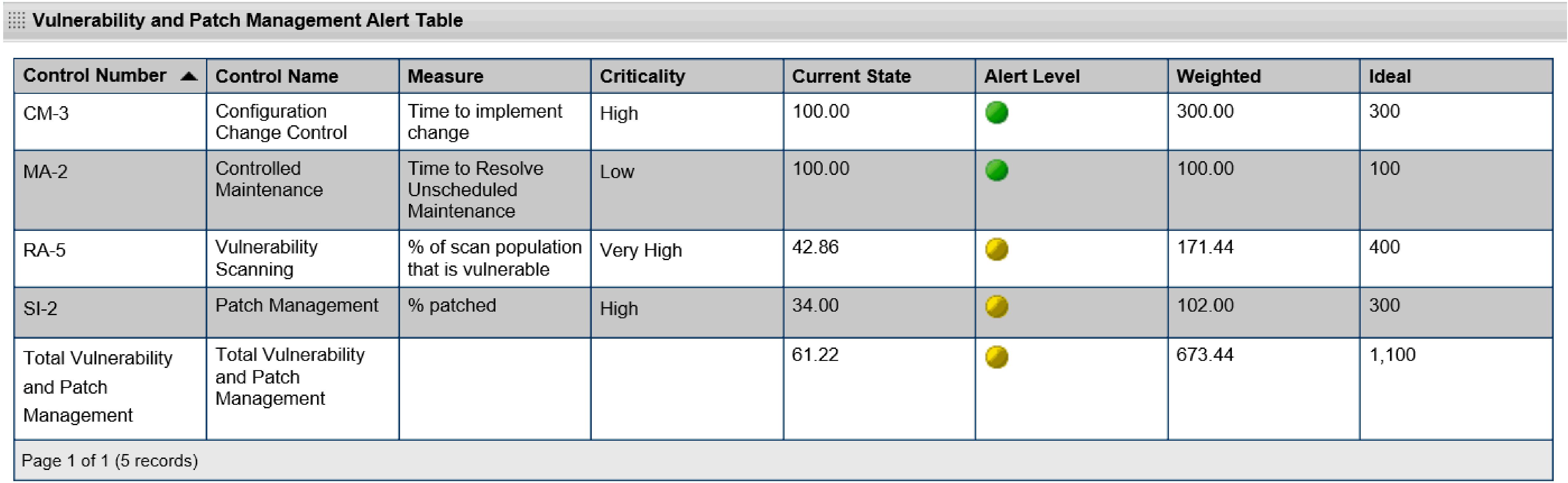


Continuous Monitoring Tier 3

SI-2 OSX Graph



Continuous Monitoring Tier 3

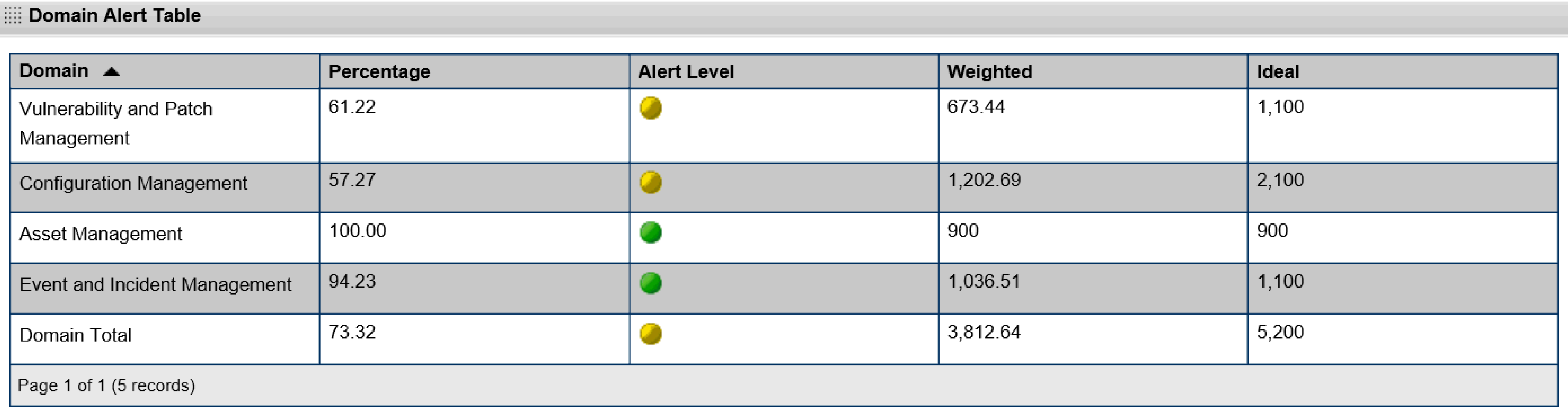


Vulnerability and Patch Management Alert Table

Control Number ▲	Control Name	Measure	Criticality	Current State	Alert Level	Weighted	Ideal
CM-3	Configuration Change Control	Time to implement change	High	100.00	🟢	300.00	300
MA-2	Controlled Maintenance	Time to Resolve Unscheduled Maintenance	Low	100.00	🟢	100.00	100
RA-5	Vulnerability Scanning	% of scan population that is vulnerable	Very High	42.86	🟡	171.44	400
SI-2	Patch Management	% patched	High	34.00	🟡	102.00	300
Total Vulnerability and Patch Management	Total Vulnerability and Patch Management			61.22	🟡	673.44	1,100

Page 1 of 1 (5 records)

Continuous Monitoring Tier 2

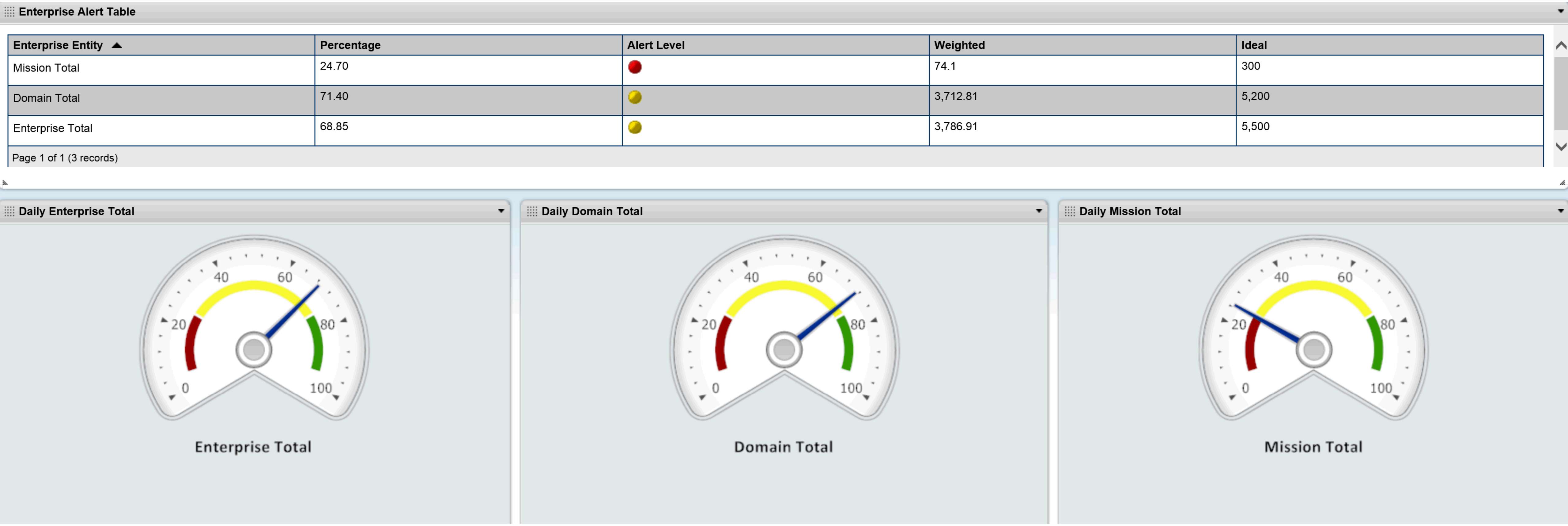


Domain Alert Table

Domain ▲	Percentage	Alert Level	Weighted	Ideal
Vulnerability and Patch Management	61.22	🟡	673.44	1,100
Configuration Management	57.27	🟡	1,202.69	2,100
Asset Management	100.00	🟢	900	900
Event and Incident Management	94.23	🟢	1,036.51	1,100
Domain Total	73.32	🟡	3,812.64	5,200

Page 1 of 1 (5 records)

Continuous Monitoring Tier 1



Enterprise Alert Table

Enterprise Entity ▲	Percentage	Alert Level	Weighted	Ideal
Mission Total	24.70	🔴	74.1	300
Domain Total	71.40	🟡	3,712.81	5,200
Enterprise Total	68.85	🟡	3,786.91	5,500

Page 1 of 1 (3 records)

Daily Enterprise Total

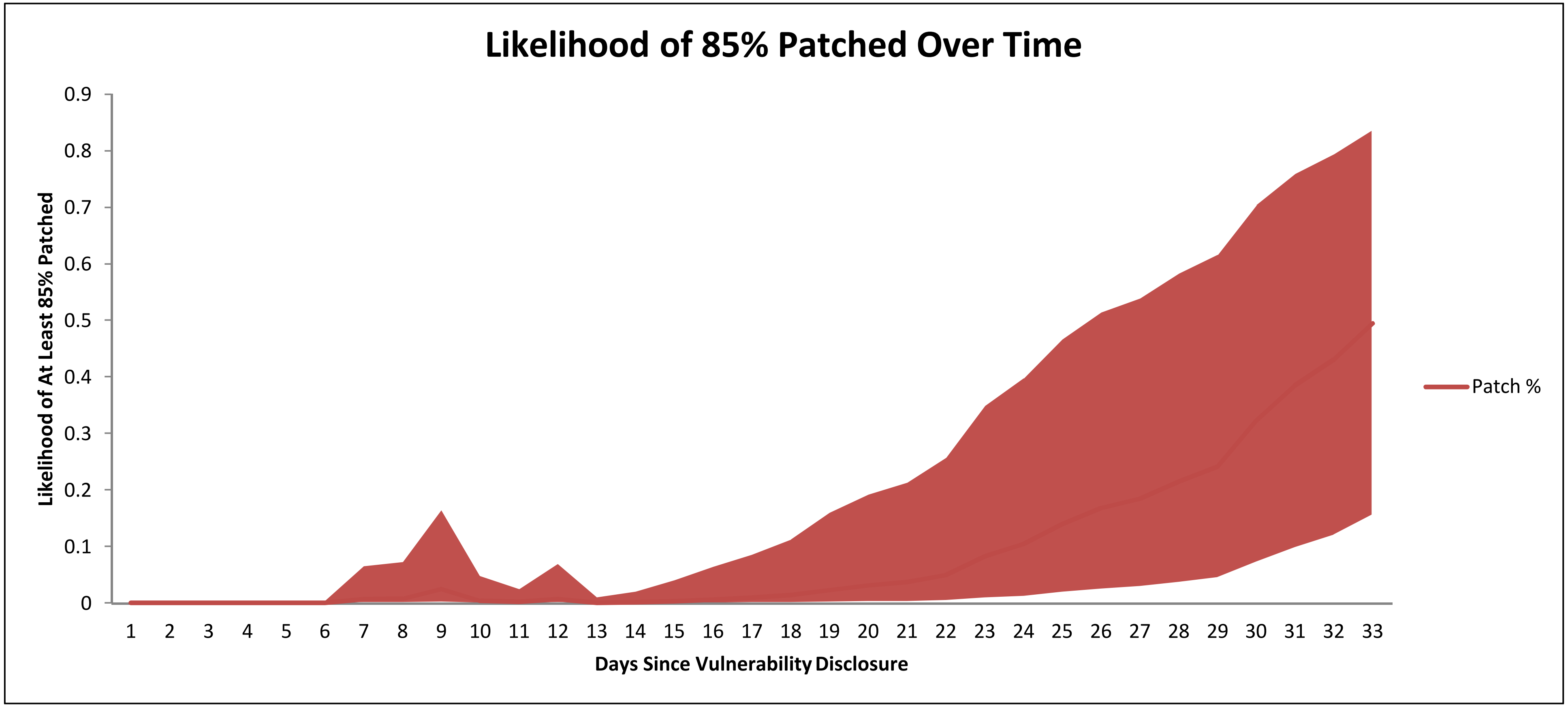
Daily Domain Total

Daily Mission Total

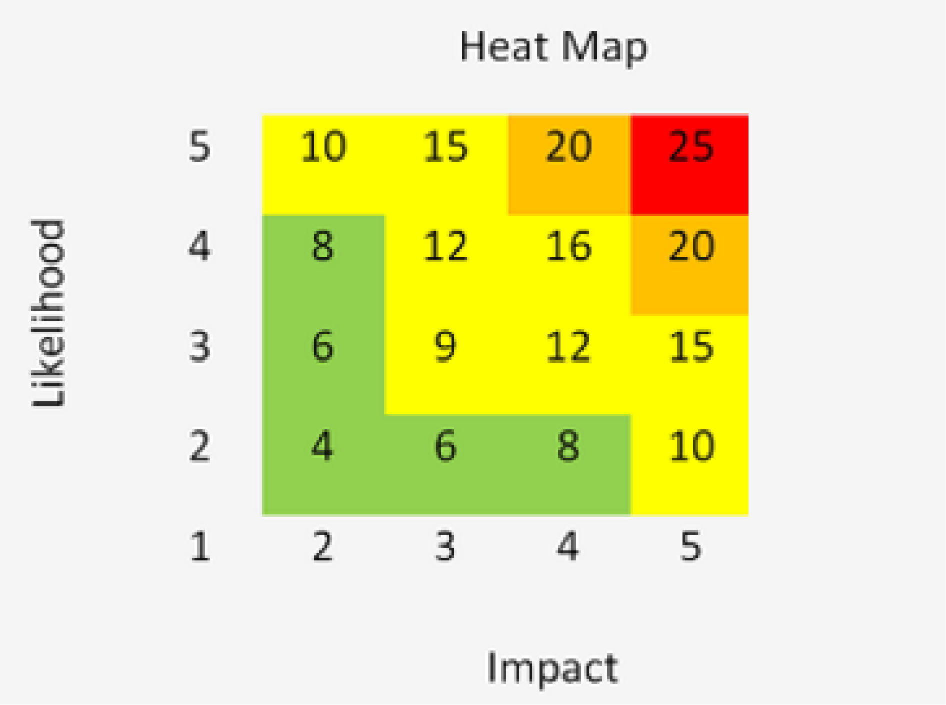
From Monitoring to Risk Quantification

- Using Continuous Monitoring data, we can determine our risk exposure
- Once quantified, these risks can be prioritized
- Multiple methods of risk analysis
  - Qualitative, semi-quantitative, quantitative
- Examples
  - Patching Risk

Patching Use Case



Mathematically-Sound Risk Matrix

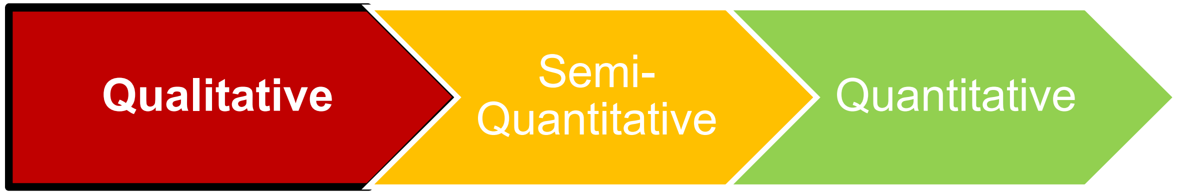


Heat Map

Likelihood				
5	10	15	20	25
4	8	12	16	20
3	6	9	12	15
2	4	6	8	10
1	2	3	4	5

Impact

- Qualitative Risk Matrix
- No Definition for Each Value
- Clear Mathematical Derivation of Values
- Useful for Prioritization
- Subjective, but Simple



Qualitative → Semi-Quantitative → Quantitative

Semi-Quantitative Risk Matrix

5	$ 1,000.00	$ 10,000.00	$ 100,000.00	$ 1,000,000.00	$ 10,000,000.00	$ 100,000,000.00	$ 1,000,000,000.00
4	$ 100.00	$ 1,000.00	$ 10,000.00	$ 100,000.00	$ 1,000,000.00	$ 10,000,000.00	$ 100,000,000.00
3	$ 10.00	$ 100.00	$ 1,000.00	$ 10,000.00	$ 100,000.00	$ 1,000,000.00	$ 10,000,000.00
2	$ 1.00	$ 10.00	$ 100.00	$ 1,000.00	$ 10,000.00	$ 100,000.00	$ 1,000,000.00
1	$ 0.10	$ 1.00	$ 10.00	$ 100.00	$ 1,000.00	$ 10,000.00	$ 100,000.00
	1	2	3	4	5	6	7

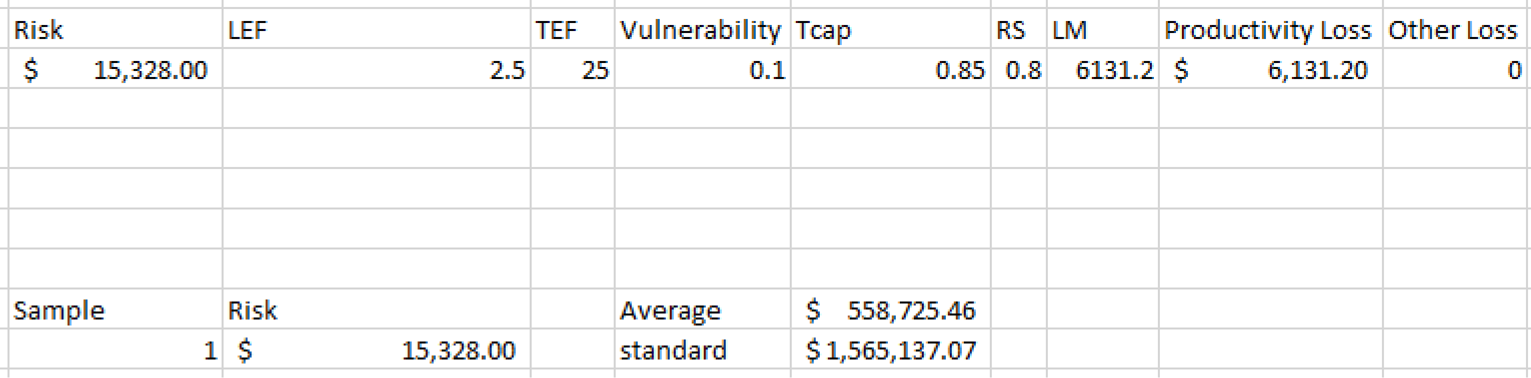
- Semi-Quantitative Risk
- Definition for Each Risk Value
- Clear Mathematical Derivation of Values
- Useful for Prioritization
- Useful for Mitigation Selection

Qualitative

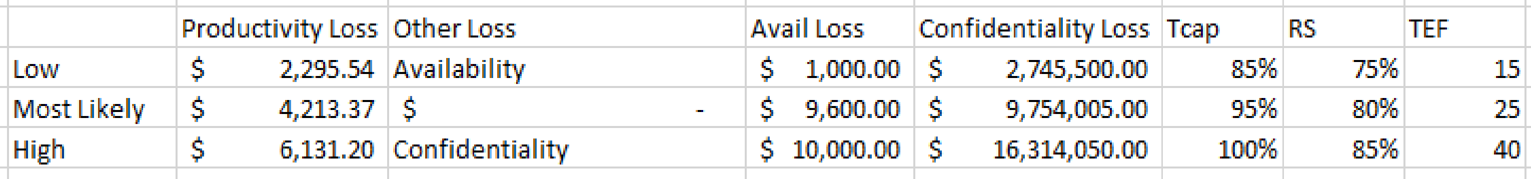
Semi-Quantitative

Quantitative

Quantitative Risk Algorithm



Risk	LEF	TEF	Vulnerability	Tcap	RS	LM	Productivity Loss	Other Loss
$ 15,328.00	2.5	25	0.1	0.85	0.8	6131.2	$ 6,131.20	0
Sample	Risk		Average	$ 558,725.46				
1	$ 15,328.00		standard	$ 1,565,137.07				



	Productivity Loss	Other Loss	Avail Loss	Confidentiality Loss	Tcap	RS	TEF
Low	$ 2,295.54	Availability	$ 1,000.00	$ 2,745,500.00	85%	75%	15
Most Likely	$ 4,213.37	$ -	$ 9,600.00	$ 9,754,005.00	95%	80%	25
High	$ 6,131.20	Confidentiality	$ 10,000.00	$ 16,314,050.00	100%	85%	40

- Quantitative Risk
- Incorporates Continuous Monitoring and Threat Information
- Clear Mathematical Derivation of Values
- Useful for Prioritization
- Useful for Mitigation Selection
- Utilizes simulation to build a range of risk, given inherent uncertainties

Qualitative
Semi-Quantitative
Quantitative

Quick-start Guide to Risk Management

- During implementation, map applicable policies to identify areas of focus and potential gaps
- Use manual and automated monitoring of individual policies to measure ongoing effectiveness at a granular level
- Create reports at multiple tiers to identify effectiveness at different levels of the enterprise
- Feed continuous monitoring data into risk analysis solutions
- Utilize quantitative risk to prioritize weaknesses and determine appropriate mitigations

Questions