DEKRA Business Assurance

Fundamentals of Risk Management

Pamela Bethune,
Automotive Regional
Competency Manager
DEKRA Certification, Inc.

July 27, 2017

GLOBAL PARTNER FOR A SAFE WORLD

We ensure safety …

on the Road.

at Work.

at Home.

DEKRA

DEKRA Overview

5

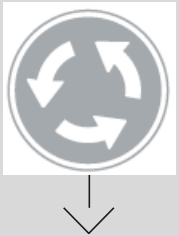
continents

50

countries

10

years, average period of employment

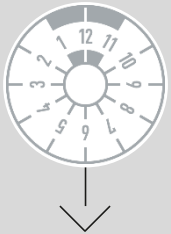


25,000

system certifications

306

accreditations



26,000,000

vehicle inspections

Thanks to its extensive testing, inspection and certification expertise, DEKRA is the European leader in Testing, Inspection and Certification sector (TIC) and the largest unlisted expert organization worldwide.

DEKRA

OUR SERVICES

Vehicle Inspection

Expertise

Automotive Solutions

Claims Services

Homologation & Type Approval

Industrial & Construction Inspection

Material Testing & Inspection

Product Testing & Certification

Business Assurance

Insight (Consulting)

Temporary Work

Training & Education

DEKRA Business Assurance

Certification and assessment services that help our customers:

- Meet their stakeholder requirements
- Develop new markets
- Reduce or mitigate risk
- Create a culture of continuous improvement.

CERTIFICATION

Quality, Environmental, Health, and Safety:

> ISO 9001: Quality Management

> ISO 14001: Environmental Management

> OHSAS 18001: Occupational health & safety

> IATF 16949: Automotive

> AS9100: Aerospace

> ISO 13485: Medical

> TL 9000: Telecom

Energy, Sustainability, and Risk:

> ISO 50001: Energy

> ISO 22301: Business continuity

> ISO 27001: Information security

> ISO 20001: Information technology

> ISO 26000: Corporate social responsibility

> ISO 55000: Asset management

DEKRA

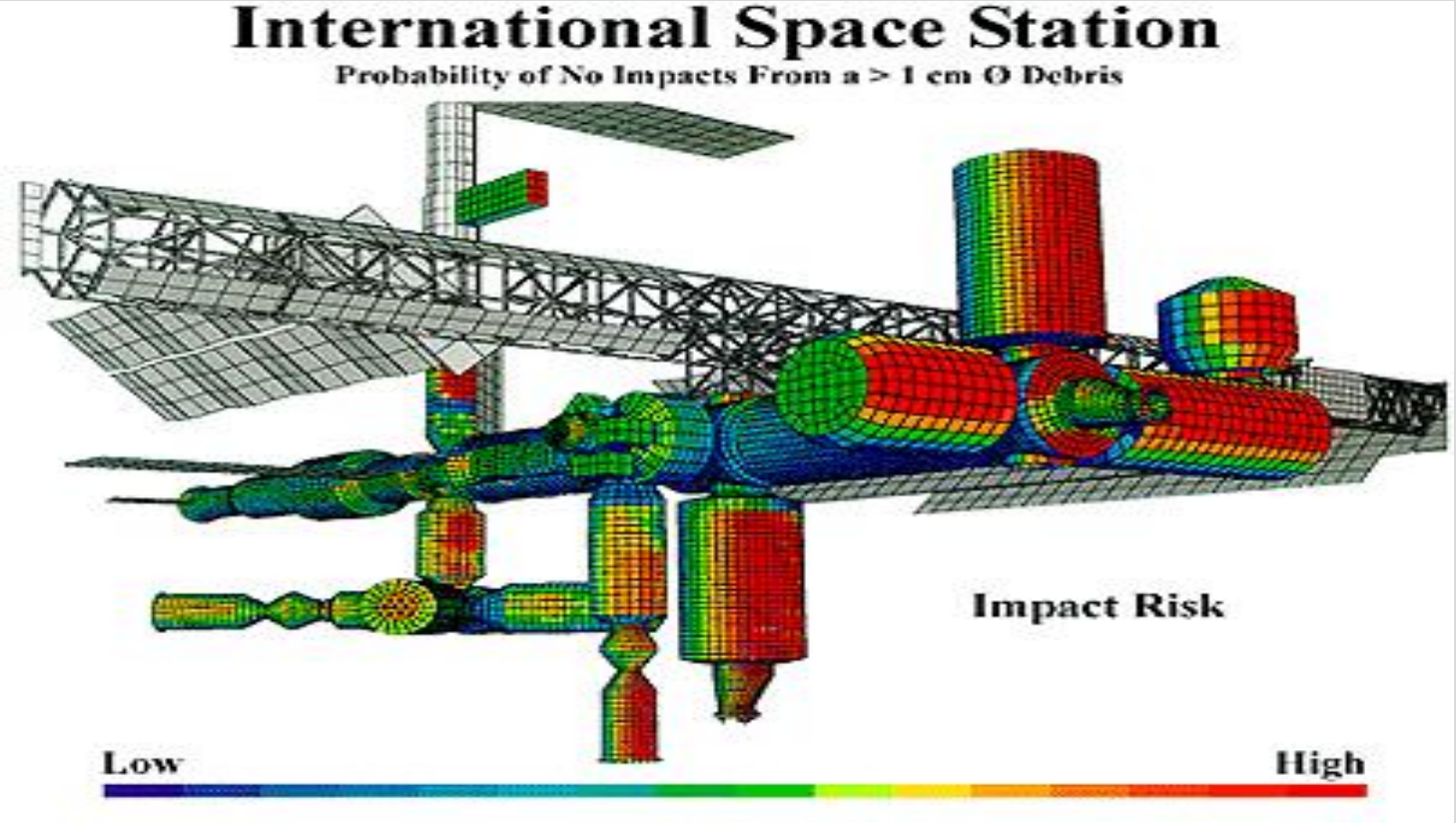
Our presenter

Pam Bethune

Lead Auditor:

- TS/IATF 16949
- ISO 9001
- ISO 14001
- ISO 13485
- ISO 45001

Risk Management Fundamentals



By National Aeronautics and Space Administration (NASA):NASA Johnson Space CenterOrbital Debris Program Office - Orbital Debris Education Package, Public Domain, https://commons.wikimedia.org/w/index.php?curid=2760870

DEKRA

Overall Concept

- Every company is in business to take risks.
- Every action or failure to take action has risk.
- Companies must identify and take opportunities.
- Companies have to take considered, measured risks.
- Companies need to decide many things: new business, new machinery, new markets, etc.
- So risks analysis is already built into companies.

This is about avoiding risks that need to be avoided, but more than that it is about taking the right level of the right risk

DEKRA

Overall Concept-Continued

Risk underlies all

Alignment is the key to success

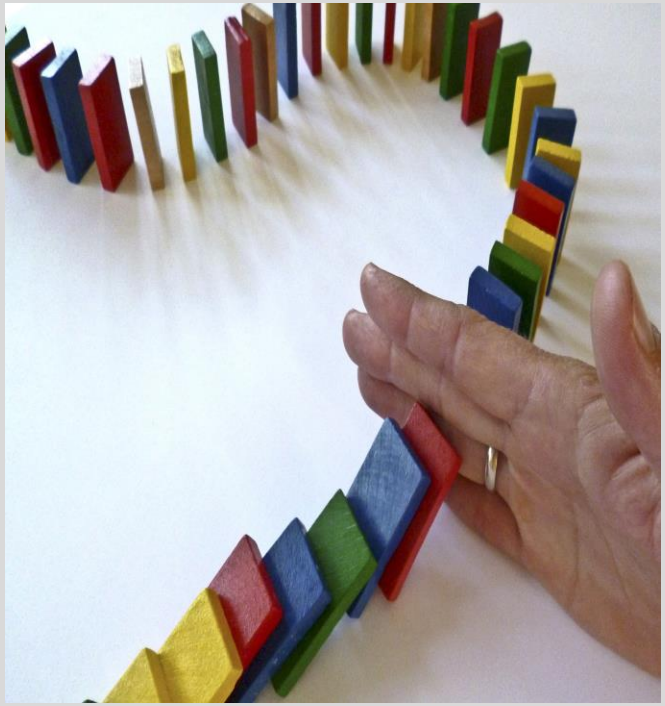
DEKRA

Risk Management and Management Systems

With the recent changes to management systems standards, the concept of risk management has never been more prominent or had more potential to be misunderstood. Risk management used to be confined to specific standards such as Business Continuity (ISO 22301), Information Security (ISO 27001), and Supply Chain Security (ISO 28001), but now is a fundamental concept in quality, health/safety, and environmental as well.

Agenda

- What is risk management and where does it fit in the new standards?
- How does it apply to my business?
- Is it just limited to what happens within our walls?
- What level of action is appropriate?
- Common Misconceptions
- Understanding and applying the intent and best practices.



What is risk management?

Risk is basically the effect of uncertainty on objectives. Definitions include:

- The forecasting and evaluation of risks together with the identification of processes that try to avoid or minimize the impact of the risks
- The process of identifying, assessing and controlling risks to an organization
- The identification, assessment and prioritization of risks followed by coordinated and economic application of resources to minimize, monitor and control the probability and/or impact of events or to maximize opportunities

Our Definition

The processes of identifying, analyzing and then evaluating whether the risk should be modified or controlled in order to satisfy risk criteria followed by data driven application of resources to minimize, monitor and/or control identified risks and opportunities

Sources of Risk

Negative (threats)

- Financial markets
- Project success or failure
- Legal changes
- Human factors
- Natural causes & disasters
- New competitors entering market
- Deliberate attack by competitors
- Accidents

Positive (opportunities)

- New markets or customers
- Improved products or services
- Legal changes
- Competitors leaving market
- Waste reduction
- Productivity improvements

Risk Strategies

Negative (threats)

- Avoid the threat
- Reduce the negative effect
- Reduce the probability of the threat
- Transfer all or part of the threat
- Be prepared for the potential consequences

Positive (opportunities)

- Active design process
- Active search for new markets

Where is risk in the new standards?

Underlying principles

- QMS principles
- Process approach
- Plan-Do-Check-Act Cycle
- Risk-based thinking

Risk based focus throughout the standard

- Taking risks and opportunities into account in all processes

Requirement

- Must plan and implement actions to address risks and opportunities
- Manage risk within a system of integrated processes, not procedures and departments
- Manage risk by setting, monitoring and measuring measureable objectives using data

DEKRA

Risk Management in IATF 16949

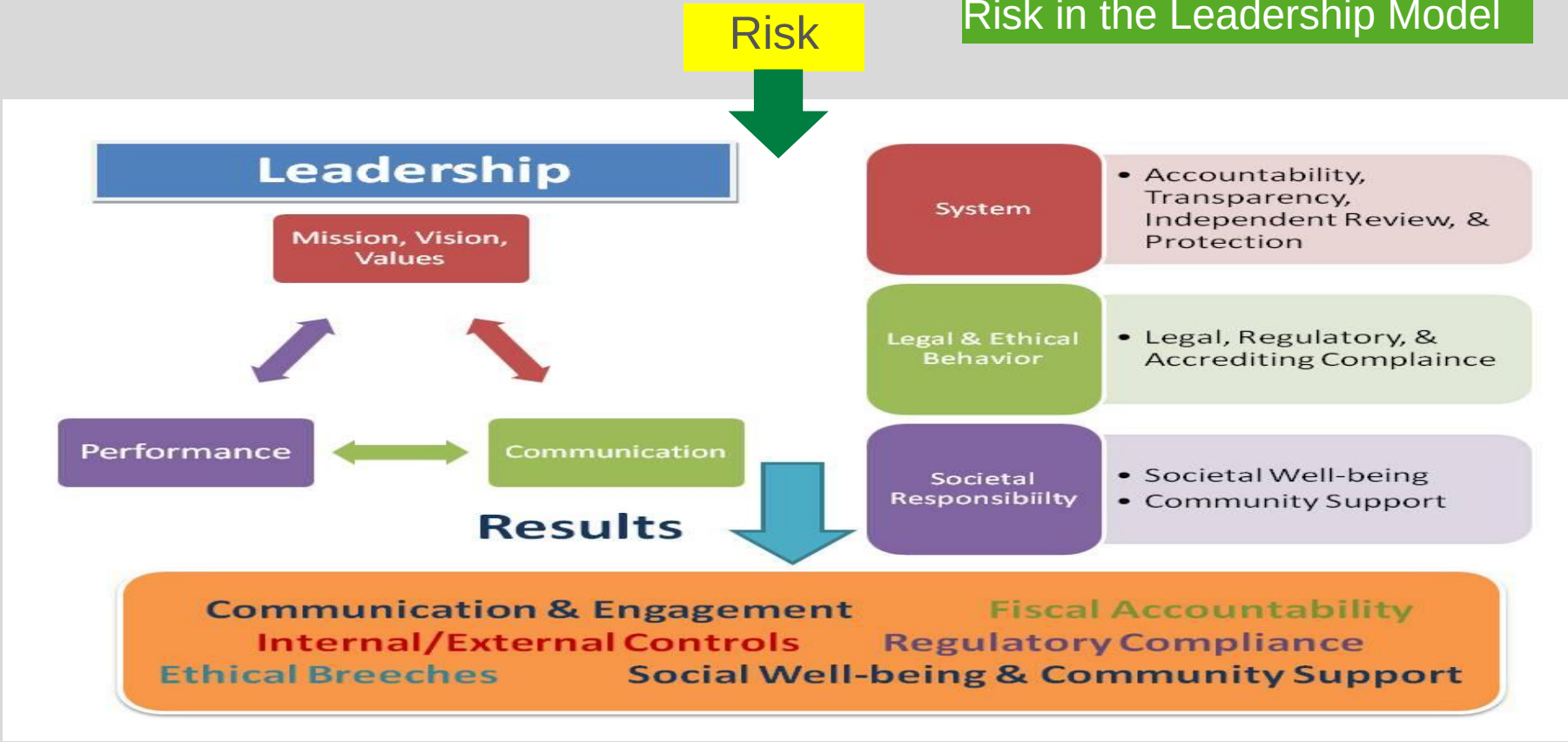
TS 16949 mentioned risk in 7 places

IATF 16949 mentions risk in 49 places

DEKRA

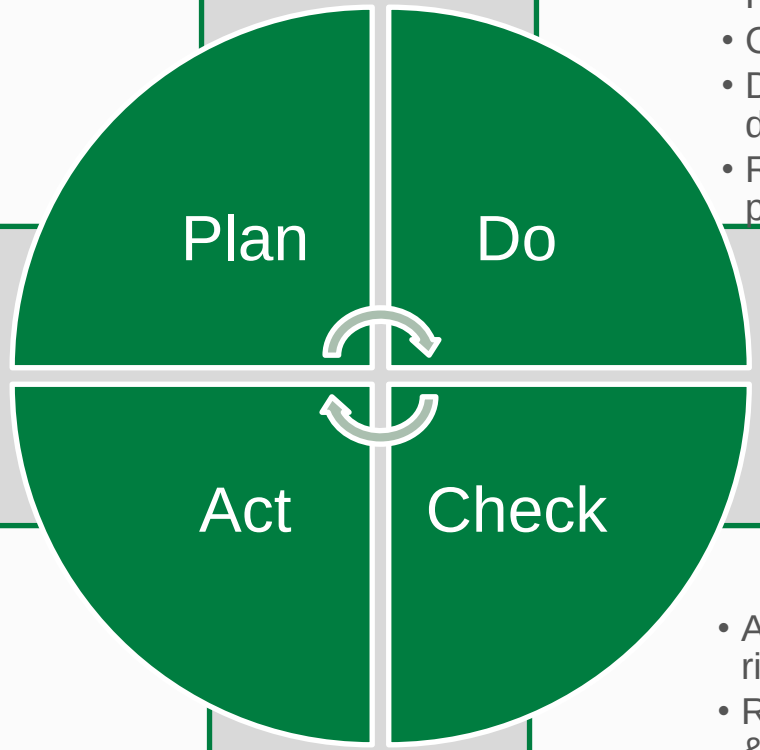
How does it apply to my business?

Risk in the Leadership Model



Risk in the new standards

- Context
- Interested parties
- QMS & processes
- Risk analysis & plan



- Policy & objectives
- Customer focus
- Design & development
- Risk plan in process

- Corrective actions
- Continuous improvement to reduce risk

- Actions to address risks & opportunities
- Resources planned & utilized

DEKRA

Is it just limited to what happens within our walls?

CONTEXT is required to start the process and is both internal and external

4.1: The organization shall determine external and internal issues that are relevant to its purpose and its strategic direction and that affect its ability to achieve the intended result(s) of its quality management system. (Legal, technological, competitive, market, cultural, social and economic environments, whether international, national, regional or local.)

DEKRA

Is it just limited to what happens within our walls?

INTERESTED PARTIES derives from context and involves both internal and external parties

Subclause 4.2 specifies requirements for the organization to determine the interested parties that are relevant to the quality management system and the requirements of those interested parties. **BUT**

4.2 does not imply extension of quality management system requirements beyond the scope of this International Standard. As stated in the scope, this International Standard is applicable where an organization needs to demonstrate its ability to consistently provide products and services that meet customer and applicable statutory and regulatory requirements, and aims to enhance customer satisfaction.

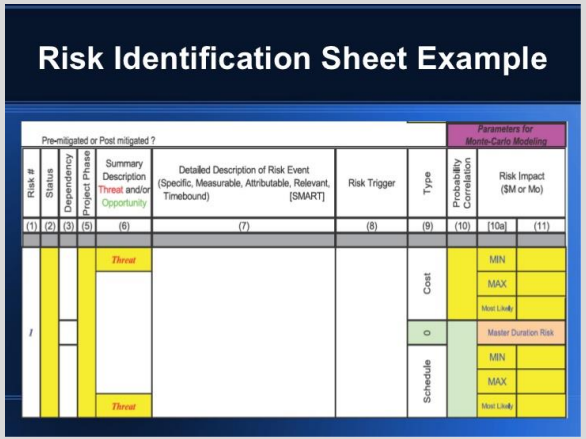
DEKRA

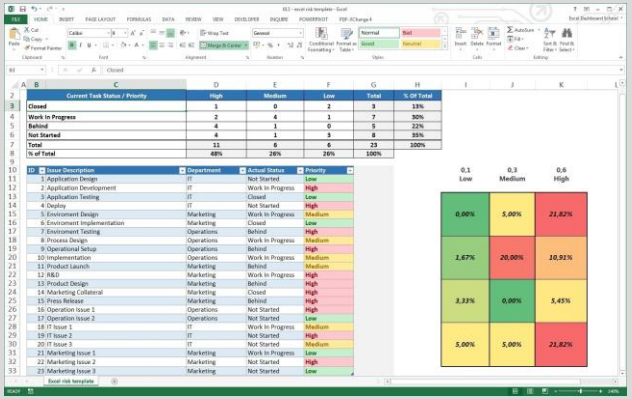
What level of action is appropriate?

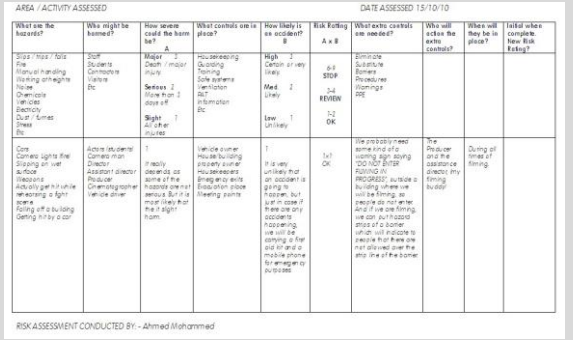
Basic methods to address risks & opportunities

Requirements per the standard

Although 6.1 specifies that the organization shall plan actions to address risks, there is no requirement for formal methods for risk management or a documented risk management process. Organizations can decide whether or not to develop a more extensive risk management methodology than is required by this International Standard, e.g. through the application of other guidance or standards.







Common misconceptions and issues

It is hard or impossible to demonstrate value in doing the exercise

It’s too complex

It’s just an exercise without any value in the real world

All we have to do is rely on our insurance and insurance company

Only important for financial risk

Focuses on the negative risks – something to be prevented

Failure to tie risk management to the firm’s overall business

Reliance on decentralized risk management practices without central controls

Failure to develop skills related to risk management

Reliance on reaction to events

Intent and Best Practices

Where to start? It depends…

Risk for some organizations has such terrible consequences that they have risk departments. Think nuclear power plants, fireworks plants and plants making safety critical items like airbags…

That is why context and interested parties are the first actions in risk management.

Some companies just add risk to their individual process analyses while others use more elaborate techniques depending on their circumstances.

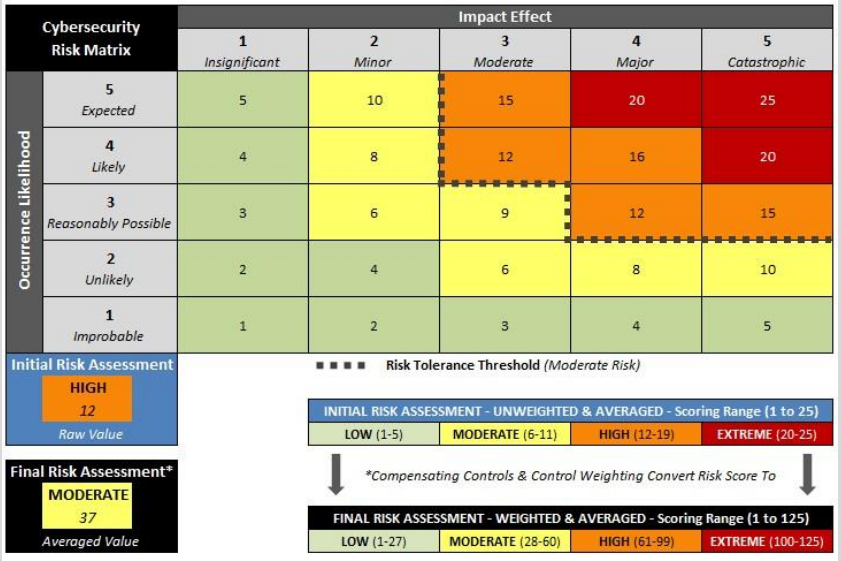
DEKRA

Principles in the standard

- Create value: resources expended to mitigate risk or take advantage of an opportunity should be less than the consequences of inaction
- Integral part of processes
- Part of leadership decision making process
- Explicitly address uncertainty and assumptions
- Be a systematic and structured process
- Based on the best available information
- Take human factors into consideration
- Be transparent and inclusive
- Be dynamic, iterative and responsive to change & periodically re-assessed

Risk Mitigation Techniques

- Risk register
- Analysis of alternatives
- Hazard analysis
- Fault tree analysis
- Failure mode & effect analysis (FMEA)
- HAZOP (hazard & operability) study
- Risk traceability analysis



DEKRA

Safety Assurance Check

A structured argument reasoning about systems appropriate for scientists and engineers, supported by a body of evidence, that provides a compelling, comprehensive and valid case that a system is safe for a given application in a given environment.

Examples:

Safety critical devices such as infusion devices

ISO 26262 for automotive functional safety

DEKRA Insight's Blueprint for Safety Transformation™

DEKRA

Example - Basic

Risk Management Analysis and Mitigation								
Context	**Interested Parties**	**Risks & Opportunities**	**Issues**	**Assignments**	**Is action required?**	**What actions?**	**Timing**	**Status**
Customer base	Sales, finances, quality, operations, shipping	New customer	CSR need to be reviewed. Capacity evaluation. Financial check	Finance: Perform financial check. Sales: Get CSR and work with Quality to evaluate Ops: evaluate capacity	No - typical of existing customers Yes - Very different customer	Sales & quality - work with customer to exclude CSR we cannot meet	3 days	
Process expertise	Customers, sales, finances, quality, operations, shipping	New process	How different from current processes? Training/ expertise of employees?	Ops: Evaluation of differences HR: work with Ops on expertise required. Hire? Train?	No - similar to existing processes Yes - Very different process	Ops and quality- work together to determine what we would need to do to take this on. HR: Is training on the processes easily available? Should we add/change employees?	1 week	
	Regulatory bodies (local, state, federal), management	New process	Regulatory changes	Mgmt: work with Ops and Quality to examine any regulatory changesdue to the new process	No - Similar to existing process regulations Yes - additional regulations exist			

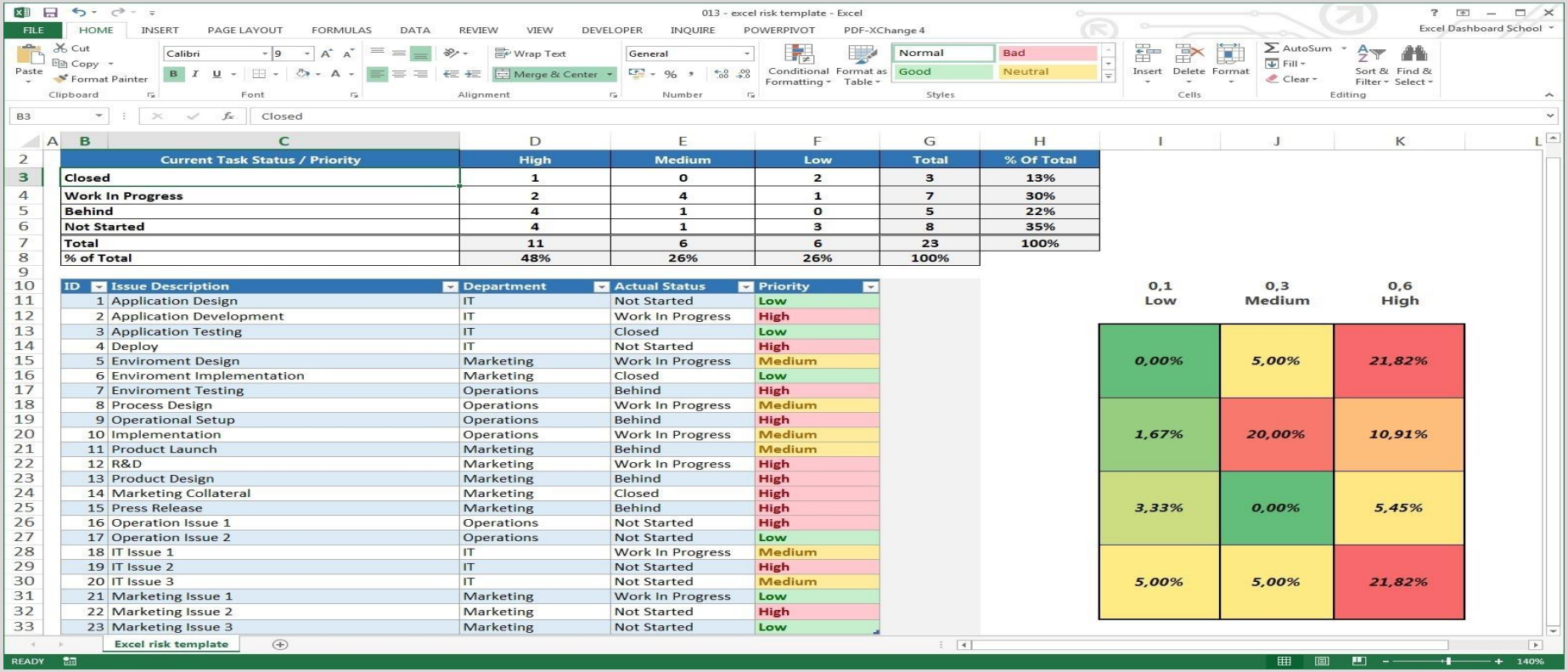
DEKRA

Example – Spreadsheet with Rating

Risk Management Analysis												
Context	**Interested Parties**	**What are the hazards**	**Who / What might be harmed**	**How severe could the harm be**	**Severity rating = S**	**What controls are already in place**	**How likely is it O**	**Risk rating: S x O**	**What extra controls are needed (if any)**	**Who will action the extra controls**	**When will they be in place**	**New risk rating**
Facility	Operations & personnel	Fire due to flammable chemicals	Anyone in the area	**Major**: Death **Serious**: time off work **Slight**: non reportable injury	3	Flammable cabinets, training, PPE	1	3				
Facility	Operations & personnel	Fire due to flammable chemicals	Loss of production	**Major:** 3: Down more than 1 shift **Serious**: 2: Up to one shift down **Slight**: 1: Less than 1 hour down	3	Flammable cabinets, training, PPE, fire alarms, fire extinguishers	1	3				
				Major=3 Serious=2 Slight=1			High=3 Med=2 Low=1	Stop=over 6 Review=3-5 OK=under 3				

DEKRA

Example – Spreadsheet with Rating and Status



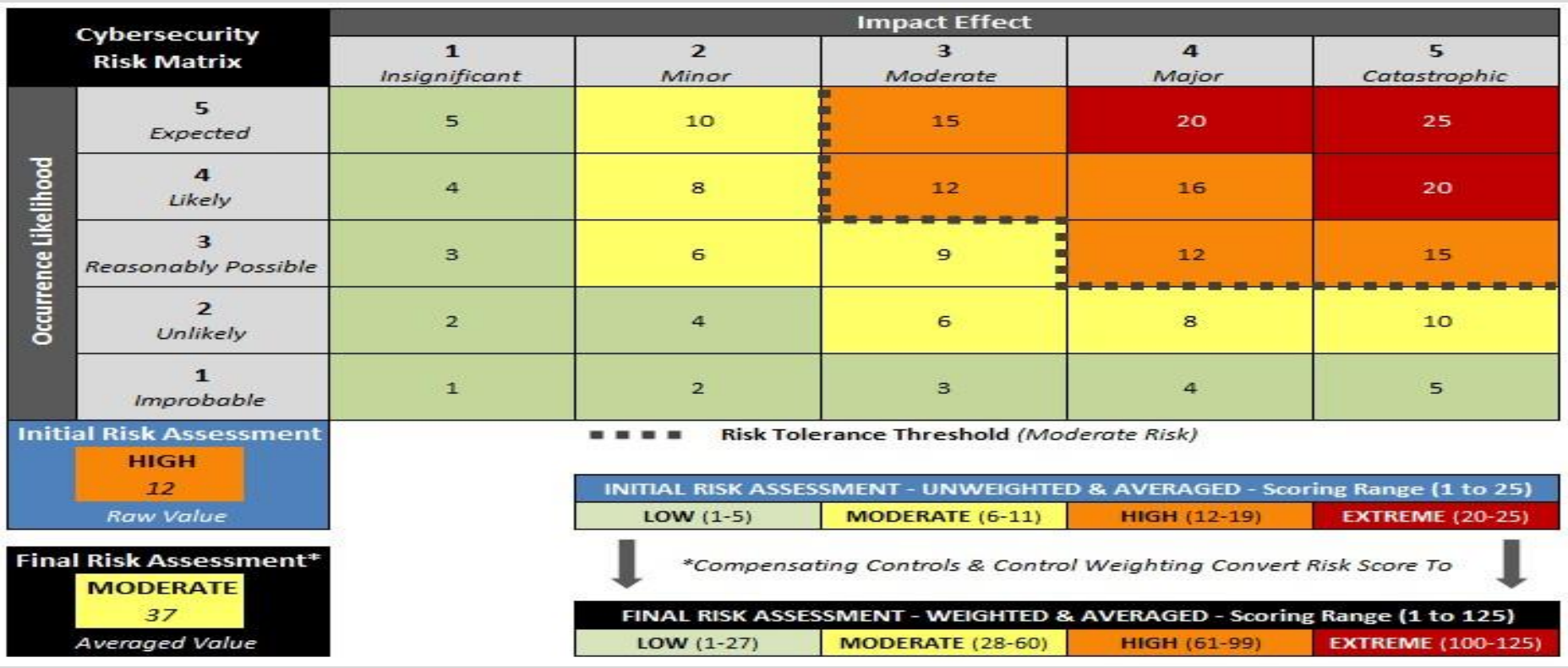
013 - excel risk template - Excel

Current Task Status / Priority	High	Medium	Low	Total	% Of Total
Closed	1	0	2	3	13%
Work In Progress	2	4	1	7	30%
Behind	4	1	0	5	22%
Not Started	4	1	3	8	35%
Total	11	6	6	23	100%
% of Total	48%	26%	26%	100%	

ID	Issue Description	Department	Actual Status	Priority
1	Application Design	IT	Not Started	Low
2	Application Development	IT	Work In Progress	High
3	Application Testing	IT	Closed	Low
4	Deploy	IT	Not Started	High
5	Enviroment Design	Marketing	Work In Progress	Medium
6	Enviroment Implementation	Marketing	Closed	Low
7	Enviroment Testing	Operations	Behind	High
8	Process Design	Operations	Work In Progress	Medium
9	Operational Setup	Operations	Behind	High
10	Implementation	Operations	Work In Progress	Medium
11	Product Launch	Marketing	Behind	Medium
12	R&D	Marketing	Work In Progress	High
13	Product Design	Marketing	Behind	High
14	Marketing Collateral	Marketing	Closed	High
15	Press Release	Marketing	Behind	High
16	Operation Issue 1	Operations	Not Started	High
17	Operation Issue 2	Operations	Not Started	Low
18	IT Issue 1	IT	Work In Progress	Medium
19	IT Issue 2	IT	Not Started	High
20	IT Issue 3	IT	Not Started	Medium
21	Marketing Issue 1	Marketing	Work In Progress	Low
22	Marketing Issue 2	Marketing	Not Started	High
23	Marketing Issue 3	Marketing	Not Started	Low

0,1 Low	0,3 Medium	0,6 High
0,00%	5,00%	21,82%
1,67%	20,00%	10,91%
3,33%	0,00%	5,45%
5,00%	5,00%	21,82%

Example – Risk and Impact Matrix



Cybersecurity Risk Matrix		Impact Effect				
		1 *Insignificant*	2 *Minor*	3 *Moderate*	4 *Major*	5 *Catastrophic*
Occurrence Likelihood	5 *Expected*	5	10	15	20	25
	4 *Likely*	4	8	12	16	20
	3 *Reasonably Possible*	3	6	9	12	15
	2 *Unlikely*	2	4	6	8	10
	1 *Improbable*	1	2	3	4	5

Initial Risk Assessment

HIGH

12

Raw Value

Final Risk Assessment*

MODERATE

37

Averaged Value

▪ ▪ ▪ ▪ **Risk Tolerance Threshold** *(Moderate Risk)*

INITIAL RISK ASSESSMENT - UNWEIGHTED & AVERAGED - Scoring Range (1 to 25)			
LOW (1-5)	MODERATE (6-11)	HIGH (12-19)	EXTREME (20-25)

**Compensating Controls & Control Weighting Convert Risk Score To*

FINAL RISK ASSESSMENT - WEIGHTED & AVERAGED - Scoring Range (1 to 125)			
LOW (1-27)	MODERATE (28-60)	HIGH (61-99)	EXTREME (100-125)

DEKRA

Thank You

If you need anything please contact us at

1-800-768-5362

or go to

www.dekra-certification.us

Sales.us@dekra.com