

MANAGING RISK THROUGH CONTRACT PROVISIONS

Jason Siems, JD

Washington State Risk Manager

OVERVIEW

- State Office of Risk Management
Intro
- What is Risk—is it all that bad?
- What Could Go Wrong
- Methods of Mitigation
- Insurance Specifications
- Contract Provisions
- Contract Management

STATE OFFICE OF RISK MANAGEMENT

The Office of Risk Management (ORM) administers the Self-Insurance Liability Program (SILP) and manages the Self-Insurance Liability Account (SILA).

ORM receives, processes, and manages the assignment and adjudication of all tort claims filed against Washington state agencies.

ORM also manages risk financing (including purchasing commercial insurance), provides loss prevention services, and administers the loss prevention review team program.

ORM is a division of the Department of Enterprise Services (DES).

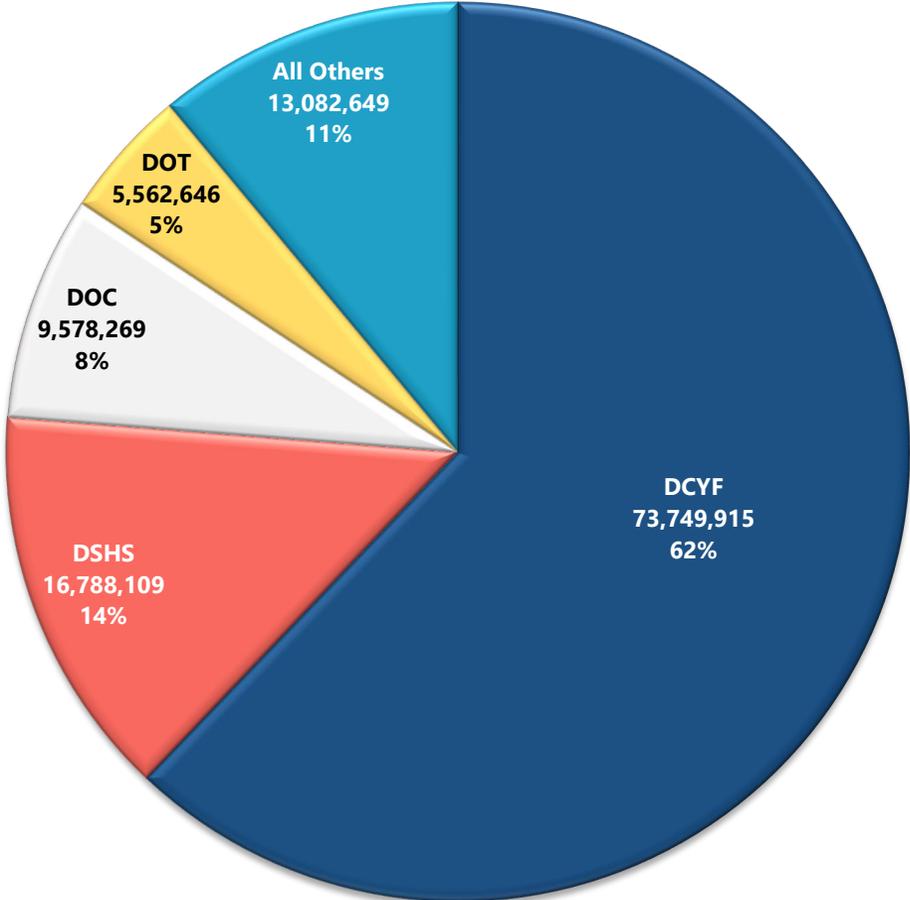
SELF INSURANCE LIABILITY PROGRAM

- The state's Self Insurance Liability Program (SILP) is used to finance the legal defense and indemnity costs of tort claims arising from negligent actions by state agencies, its officers, employees and volunteers.
- The program is funded by premiums paid by each agency.
- Premiums are set, in part, with the intent of incentivizing good loss prevention and risk management.
- Excess Insurance policies to protect the fund.

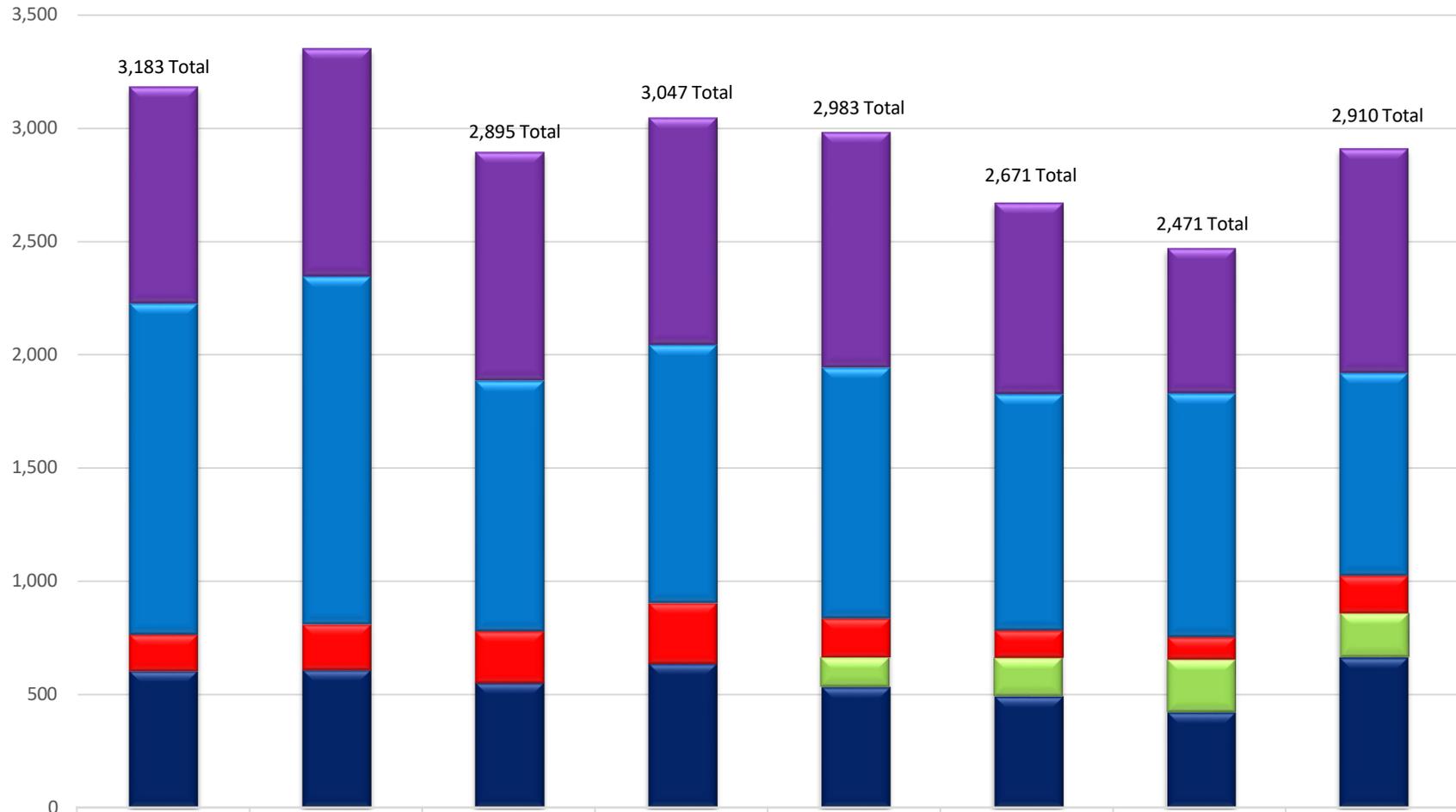
FY 22 STATEWIDE INDEMNITY PAYOUT DISTRIBUTION

(Includes WSDOT Marine Division Payouts and Excludes UW and Excess Insurance Refunds)

Total Dollars Paid
\$118,761,588



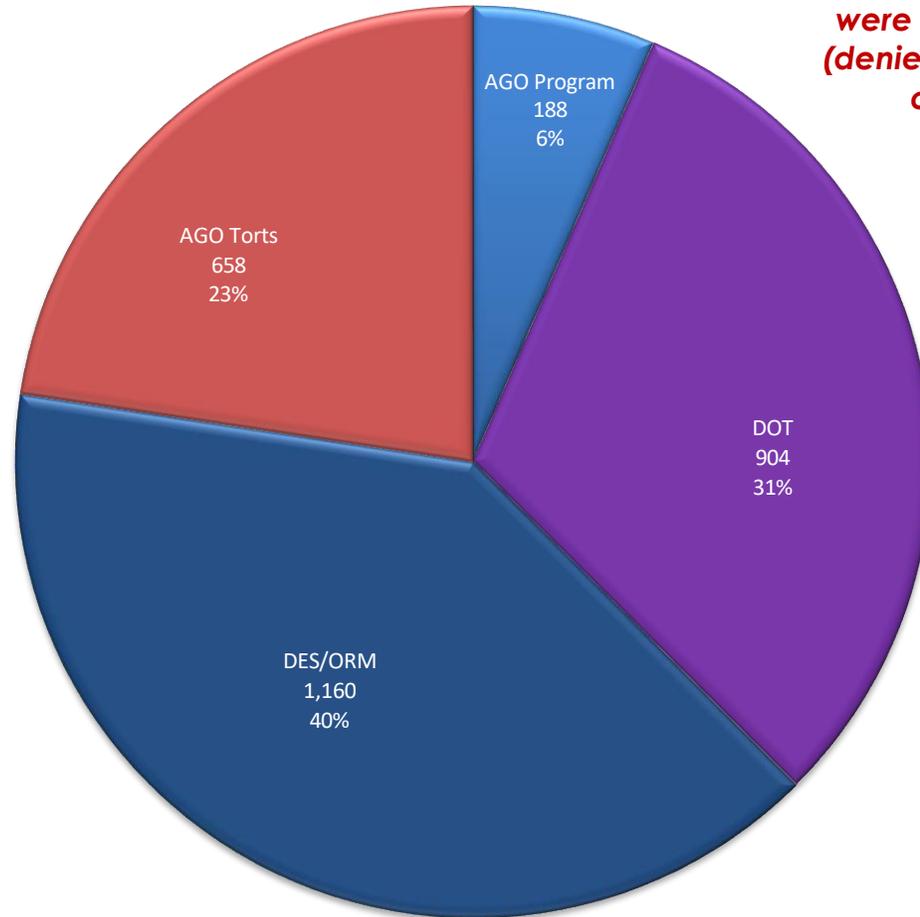
NUMBER OF CLAIMS



	FY2015	FY2016	FY2017	FY2018	FY2019	FY2020	FY2021	FY2022
■ DOT	958	1,008	1,010	1,004	1,040	845	642	992
■ DOC	1,459	1,533	1,104	1,138	1,106	1,042	1,073	892
■ DSHS	163	204	230	270	174	122	102	169
■ DCYF	0	0	0	0	132	172	233	196
■ All Others	603	607	551	635	531	490	421	661

NUMBER OF CLAIMS

40% of tort claims filed in FY-22 were administratively handled (denied or settled) by the Office of Risk Management



■ AGO Program ■ DOT ■ DES/ORM ■ AGO Torts

WHAT IS RISK?

“The effect of uncertainty on objectives.”

The level and types of risk vary among organizations, as well as within divisions of organizations.

Risks must be identified and managed to protect the organization's employees, resources, reputation and also to take best advantage of opportunities.

STRUTHIOUS

“Ostrich-like. Suggests a tendency to bury one’s head in the sand like an ostrich.” *Merriam-Webster*



MANAGING RISK HELPS ENSURE THAT



Goals are
completed
on time



Organization
is financially
healthy



Reputation
is
protected



Employees
&
Customers
are safe



Agency
innovates
and adapts
to change
while
managing
associated
risk

NEW OPPORTUNITIES

With effective risk management, risk managers can work across the organization to identify, measure and evaluate any type of risk.

Leaders can now get a clear “big picture” of their most serious exposures and make informed decisions about how to deploy resources to mitigate risks that threaten success.

Risk Management should play a prominent role in the strategic efforts of the organization.

WHAT COULD GO WRONG



TAYLOR BRIDGE FIRE



TAYLOR BRIDGE FIRE

2012 Wildfire in Kittitas County

Started by a contractor of WSDOT, welding on the “Taylor Bridge” on State Route 10 near Cle Elum.

Contract for work on the bridge required contractor to have \$1 Mil in liability coverage.

300 people lost property—23,500 acres burned—61 homes and 100 outbuildings destroyed.

\$60 Million Settlement—largest wildfire settlement in state’s history.

OSO LANDSLIDE



OSO LANDSLIDE

March 2014 landslide blocks Stillaguamish River, destroys rural neighborhood

Forty-three fatalities, 49 homes destroyed.

State contract with Stillaguamish Tribe to restore Salmon habitat along river.

Contract required tribe to indemnify state, have \$5 Mil insurance coverage--invalidated.

\$60 Million Settlement.

RCW 4.92.270

Risk management—Standard indemnification agreements.

The risk manager shall develop procedures for standard indemnification agreements for state agencies to use whenever the agency agrees to indemnify, or be indemnified by, any person or party. The risk manager shall also develop guidelines for the use of indemnification agreements by state agencies. On request of the risk manager, an agency shall forward to the office of risk management for review and approval any contract or agreement containing an indemnification agreement.

RCW 4.92.130(2)

Tortious conduct of state—Liability Account—Purpose.

(3) No money shall be paid from the liability account, except for defense costs, unless all proceeds available to the claimant from any valid and collectible liability insurance shall have been exhausted . . .

CONTRACTS TRAINING



SELF ▾

MY TEAM ▾

Learning ▾

Search



Home



Timeline



Library



Training Transcript



Training Schedule

[Home](#) / [Back to Search Results](#)



WA STATE CURRICULUM

DES - WA-STATE PURCHASING AND PROCUREMENT 101 MODULE 1



Completion Status

REGISTER

DES - WA-State Purchasing and procurem...

1. WA-State Purchasing and procureme...

DETAILS

ACTIVITIES

SIMILAR ACTIVITIES



WA STATE CURRICULUM

DES - WA-State Contract Management 101 Module 4

Welcome to WA-State Contract Management - Module 4. Included in the module are knowledge checks and the final assessment.

DES_WA-State Contract_Management_101_Module_4_4/30/2015



WA STATE CURRICULUM

DES - WA-State Contract Management 101 Module 2

Welcome to WA-State Contract Management - Module 2. Included in the module are knowledge checks and the assessment.On...

DES_WA-State Contract_Management_101_Module_2_5/30/2015



WA STATE CURRICULUM

DES - WA-State Contract Management 101 Module 3

Welcome to WA-State Contract Management - Module 3. Included in the module are knowledge checks and the assessment.On...

DES_WA-State Contract_Management_101_Module_3_5/30/2015



WA STATE CURRICULUM

DES - WA-State Contract Management 101 Module 1

Welcome to WA-State Contract Management - Module 1. Included in the module are knowledge checks and the assessment.On...

DES_WA-State Contract_Management_101_Module_1_5/30/2015



ALASKAN WAY VIADUCT



ALASKAN WAY VIADUCT

Tunnel boring project resulted in \$80 Mil in claims—paid \$10 Mil.

Maximum probable loss study prior to procurement for vendor to tear down viaduct—informed on what types of insurance to require, and how much.

Demolition completed in 2019.

No claims—no payouts.

AMTRAK DERAILMENT



AMTRAK DERAILMENT

December 2017—Amtrak Cascades passenger train derails near Dupont.

Three deaths, many more injured, significant property damage.

Contract with Amtrak required indemnification.

Thirty-five people sued Amtrak, over \$45 Mil in payouts.

Contract provisions kept the state protected legally.

FISH AND WILDLIFE CYBER BREACH



FISH AND WILDLIFE CYBER BREACH

- Summer 2016 hack of electronic licensing vendor system.
- Private vendor under contract to provide service.
- Four states impacted—WA, OR, ID and KY.
- Individual financial/payment information accessed—2 Mil WA customers.
- Contract required vendor to cover costs/have insurance.

AND WE LEARNED. . . .

- Require vendors to indemnify your organization.
- Require vendors to have insurance to pay claims arising from their activity.
- Require the type of insurance that addresses the risk of the activity.
- The insurance needs to be sufficient to cover the whole risk.
- Do a risk assessment early on.

BUT,,,AREN'T WE JUST PASSING THE BUCK!?



WHY BOTHER?

- Your entity can be held liable for damages caused by your contractors.
- You should be able to rely on the contractor's expertise to do the job safely, and if it doesn't, it should pay for the consequences.
- Responsibility encourages safety on the part of the contractor.
- Risk is placed upon those best able to control the work.
- You have a source for payment of claims against your entity
- Maintaining your own project or entity budget .
- Maintaining your own good loss history and lower insurance costs.

CONTRACT RISK MANAGEMENT METHODS OF MITIGATION



CONTRACT RISK TRANSFER

- Analyze the Risks and Relationships
- Use Hold Harmless (Indemnity) Agreement
- Require the Appropriate Insurance Specifications
- Verify Insurance Coverage
- Report Claims Properly
- Remember the Records

ANALYZE THE RISKS AND RELATIONSHIPS

- Start early—first meeting of the procurement team.
- Conduct a risk assessment—many methods/tools available.
- Review the scope of work.
- Ask, “What Could Go Wrong?”
- Small contracts have risks too.
- Prioritize risks using magnitude and likelihood.

USE HOLD HARMLESS (INDEMNITY) AGREEMENT

- Hold Harmless (indemnity) should include an obligation to defend your entity (including employees, officials, agents, etc.).
- Shifts responsibility for loss or damage arising from the activities of the contract from your entity to the contractor.
- Hold harmless language allows you to tender the claim of the damaged third party to the contractor for defense or indemnity by the contractor or their insurer.

SAMPLE HOLD HARMLESS LANGUAGE

- **Hold harmless**: to the fullest extent permitted by law, Contractor shall **hold harmless, defend** at its own expense, **and indemnify Entity** its officers, employees, agents, and volunteers, **against any and all** liability, **claims**, losses, damages, or expenses, including reasonable attorney's fees, **arising from all acts or omissions to act of contractor or its** officers, **agents**, or employees in rendering services under this contract; **excluding**, however, such liability, **claims**, losses, damages, or expenses **arising from Entity's sole negligence or willful acts**.

REQUIRE THE APPROPRIATE INSURANCE SPECIFICATIONS

- Requiring insurance helps to ensure the contractor will have the money to deliver on their promise to hold harmless or indemnify you.
- Inform contractors/bidders early in the process (RFP phase):
 - Allows for more accurate bid pricing
 - Allows time to contact insurers
- Consider a specific appendix to the contract for insurance specifications with reference in the contract.

BASIC INSURANCE REQUIREMENTS FOR MOST CONTRACTS

- Commercial General Liability
- Automobile Liability
- Worker's Compensation
- Professional Liability
- Cyber Breach Insurance

COMMERCIAL GENERAL LIABILITY (CGL)

- Fundamental coverage for bodily injury, property damage and personal injury arising from the contractor's activities.
- Should cover most perils identified in risk assessment of the project (watch for exclusions).
- Choose an amount per occurrence sufficient to cover probably perils
- Choose an aggregate limit at least twice the occurrence limit, even in the smallest contracts.
- E.G. Minimum \$1 Mil per occurrence; \$2 Mil aggregate—allows for two separate claims in policy period.

AUTOMOBILE LIABILITY COVERAGE

- Require for any work or service that will involve the use of motor vehicles.
- If contractor does no own autos, cover hired and non-owned autos used by contractor.
- No less than \$1 Mil per accident for bodily injury and property damage.

WORKERS COMPENSATION

- All employers must provide this insurance.
- Requirements vary by state.
- Require compliance with Washington State Worker's Compensation laws:
"Contractor shall comply with the Washington State Industrial Insurance Act and, if applicable, the Federal Longshoremen's and Harbor Worker's Act and the Jones Act."

PROFESSIONAL LIABILITY

- For technology and professional services contracts, particularly with licensed professionals such as architects, engineers, attorneys, accountants, medical professionals.
- Provides coverage for errors in professional judgment that lead to damages to your entity or third parties.
- Amount per occurrence and aggregate amounts should reflect risk

CYBER AND DATA USE RISKS

- Be alert for any contract that allows a vendor access to your data. These may include:
 - Portals that allow access to obtain, submit, use or store data;
 - Cloud hosting and data storage services;
 - Any IT software or hardware;
 - Programming, configuration, data migration services;
 - Any IT service.

SPECIFIC CYBER RISKS

- Any time a vendor has access to, or provides customer access to, your data, there are risks of:
 - Loss of stored data
 - Theft of data;
 - Disruption of network capabilities;
 - Disclosure of private information;
 - Hijacking of network for malicious purposes.

SPECIFIC PROVISIONS TO ADDRESS CYBER RISKS

- Confidentiality agreements:

Include specific language that requires the vendor to acknowledge that they will receive or have access to private information; that private information is not owned by the vendor, that they have not ability to sell of otherwise misuse that private information and that they will have safeguards in place to protect that information.

--Be specific about what data the vendor might have access to, how it may be used and the safeguards that must be in place.

SPECIFIC PROVISIONS TO ADDRESS CYBER RISKS

- Think about what happens to the data when the contract ends:

At some point in the future, your contract with a data system vendor will likely end and you will want access to all of your data in a usable format within a reasonable period of time. Returned data should include tables and indexes, number of records and any other useful information so that you can utilize the data or transfer it to a new vendor. Include specific language that requires the vendor to acknowledge that they will receive or have access to private information; that private information is not owned by the vendor, that they have not ability to sell or otherwise misuse that private information and that they will have safeguards in place to protect that information.

--Add specific language to allow return of data without regard to other disputes that may be pending with the vendor.

SPECIFIC PROVISIONS TO ADDRESS CYBER RISKS

- Require that the vendor notify the entity of a breach even if no data was lost.
- Require that data be backed up in a secure fashion and that entity have access to backups.
- Require specific minimum response and recovery time.
- Require independent audits of operations.

SPECIFIC PROVISIONS TO ADDRESS CYBER RISKS

- For vendors providing hardware, pre-packaged software or portal access, add a requirement for IT Professional Liability or Cyber Liability insurance that includes:
 - Security and privacy liability, including privacy breach response costs, regulatory fines and penalties;
 - Media liability, including infringement of copyright and trademark;
 - Cyber extortion;
 - Privacy.

CYBER INSURANCE REQUIREMENTS

- Determination of Exposure:
 - The type of protected data involved;
 - The number of protected data records stored or processed by the vendor;
 - The cost of breach notification, response and investigation;
 - The potential for credit monitoring costs;
 - The cost of legal support and defense;
 - The cost of regulatory fines;
 - The potential for tort claims or lawsuits;
 - The potential that other clients of the vendor are experiencing the same incident.

SAMPLE CYBER INSURANCE LANGUAGE

Cyber Liability Insurance, with limits not less than **\$2,000,000** per occurrence or claim, **\$4,000,000** aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by Vendor in this agreement and shall include, but not be limited to, claims involving infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, alteration of electronic information, extortion and network security. The policy shall provide coverage for breach response costs as well as regulatory fines and penalties as well as credit monitoring expenses with limits sufficient to respond to these obligations.

VERIFY INSURANCE COVERAGE

- Require that Certificates of Insurance for required coverages be submitted with bid.
 - Require that actual insurance policies and all endorsements be submitted/approved prior to signing contract.
 - Periodically review insurance during the term of the contract.
- Beware of endorsements and exclusions

REPORT CLAIMS PROPERLY

- Most insurers impose specific requirements and timelines for reporting claims and may deny coverage for failure to comply.
- Spell out who does the reporting, of what and when.
- Avoid terms like “reasonable time” or “promptly”. Use specific number of days instead.

OTHER RISK MITIGATING CONTRACT PROVISIONS

- *Additional Insured Status*—allows you entity the same standing as the insured vendor:

“The Entity, its officers, officials, employees, and volunteers are to be covered as additional insureds on the CGL policy with respect to liability arising out of work or operations performed by or on behalf of the Vendor including materials, parts, or equipment furnished in connection with such work or operations. ”

****Difficult to obtain on professional liability coverage*

OTHER RISK MITIGATING CONTRACT PROVISIONS

- *Primary Coverage*—requires that the vendor's insurance pay first:

“For any claims related to this contract, the **Consultant's insurance coverage shall be primary**. Any insurance or self-insurance maintained by the Entity, its officers, officials, employees, or volunteers shall be excess of the Consultant's insurance and shall not contribute with it.”

OTHER RISK MITIGATING CONTRACT PROVISIONS

- *Notice of Cancellation*—requires that the vendor's insurer notify you if the insurance lapses:

"Each insurance policy required above shall state that **coverage shall not be canceled, except with notice to the Entity.**"

OTHER RISK MITIGATING CONTRACT PROVISIONS

- *Waiver of Subrogation*—protects your organization from claims made by vendor's insurer to recover for a loss:

“Vendor hereby grants to Entity a waiver of any right to subrogation which any insurer of said Vendor may acquire against the Entity by virtue of the payment of any loss under such insurance. Vendor agrees to obtain any endorsement that may be necessary to affect this waiver of subrogation, but this provision applies regardless of whether or not the Entity has received a waiver of subrogation endorsement from the insurer.”

OTHER RISK MITIGATING CONTRACT PROVISIONS

- *Self-Insured Retentions*—allows your organization to know about and approve self-insured portion of the required coverages:

“Self-insured retentions must be declared to and approved by the Entity. The Entity may require the Vendor to provide proof of ability to pay losses and related investigations, claim administration, and defense expenses within the retention. The policy language shall provide, or be endorsed to provide, that the self-insured retention may be satisfied by either the named insured or Entity.”

OTHER RISK MITIGATING CONTRACT PROVISIONS

- *Acceptability of Insurers*—allows your organization to limit insurance coverage to only highly rated insurance companies:

“Insurance is to be placed with insurers with a current A.M. Best’s rating of no less than A:VII, unless otherwise acceptable to the Entity.”

OTHER RISK MITIGATING CONTRACT PROVISIONS

- *Subcontractors*—extends insurance requirements to any subcontractors of your vendor:

“Vendor shall require and verify that all subcontractors maintain insurance meeting all the requirements stated herein, and Vendor shall ensure that Entity is an additional insured on insurance required from subcontractors.”

OTHER RISK MITIGATING CONTRACT PROVISIONS

- *Special Risks or Circumstances*—allows your organization to change the insurance requirements as circumstances warrant:

“Entity reserves the right to modify these requirements, including limits, based on the nature of the risk, prior experience, insurer, coverage, or other special circumstances.”

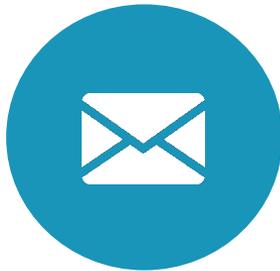
REMEMBER THE RECORDS

- Depending on the type of contract, the vendor will be creating records that could create legal obligations for your organization.
- Washington state has some of the most expansive open government laws.
- Records created by vendors may be pertinent to legal defenses long after the contract has ended.
- Discovery and public records disclosure penalties can be severe.
- Spell out in the contract how records created by the vendor are to be preserved and/or returned to your organization after the contract ends.

QUESTIONS, COMMENTS, ANSWERS?



THANK YOU FOR ATTENDING



Jason.Siems@des.wa.gov



360-742-6348



des.wa.gov